



**RAILTEL CORPORATION OF INDIA LIMITED**

(A Govt. of India Undertaking, Ministry of Railways)

**Expression of Interest for Selection of Partner from Empaneled Business Associates / OEMs /  
OEM's authorized partner / distributor(s)**

**for the work of**

**“Master System Integrator (MSI) for CGSDC2.0 Project in  
the State of Chhattisgarh”**

**EoI No: RailTel/WR/BPL/CHiPS/EOI/2024-25/23**

**Dated: 29<sup>th</sup> November 2024**

**Plot No. 17, 1<sup>st</sup> Floor, Raghunath Nagar, Near Shahpura Police station,  
Bhopal MP-462039**

## EOI NOTICE

**RailTel Corporation of India Limited,  
Plot No. 17, 1<sup>st</sup> Floor, Raghunath Nagar, Near Shahpura Police Station, Bhopal MP - 462039**

**EOI No: RailTel/WR/BPL/CHIPS/EOI/2024-25/23**

**dated: 29<sup>th</sup> November 2024**

RailTel Corporation of India Ltd., (here after referred to as “RailTel”), publishes EOI to select suitable partner among RailTel’s Empaneled BA / OEMs / OEM’s authorized partner / distributor(s) for work of “**Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh**”.

The DATA SHEET is as under:

1	Last date for submission of EOI response.	05 <sup>th</sup> December 2024 at 16:00 Hours
2	Opening of EOI response	05 <sup>th</sup> December 2024 at 16:30 Hours
3	Number of copies to be submitted for scope of work	One
4	EMD Amount	<p>Rs. 3,00,00,000/- (Rupees Three Crores Only) (in form of BG) (Refer Annexure-7)</p> <p>Empaneled BA may submit the EMD in two parts. Detailed as under –</p> <p>1. Token EMD – Rs. 5 Lakhs in form of BG or cash transfer in account of RailTel (Bank details given at Annexure – 6)</p> <p>2. The balance amount of advertised EMD by BA will be submitted one day before final submission of bid to customer.</p> <p>Remaining EMD value Rs. 2.95 Crore in form of BG or cash transfer in account of RailTel (Bank details given at Annexure – 6)</p>
5	Tender Fees & Processing Fees	Rs. 5000/- (Rupees Five Thousand Only) (to be deposited online as per Annexure - 6)

The EMD in form of BG should be in the favor of RailTel Corporation of India Limited payable at Mumbai.

Partner needs to submit BG with all details as per Annexure – 7.

Against Tender fee and processing fee deposition, online payment details like UTR No. date and Bank detail to be submitted along with the technical proposal.

### **RailTel Bank Details:**

- 1. Name of the Bank - Union Bank of India**
- 2. Account No. - 317801010036605**
- 3. IFSC Code - UBIN0531782**

#### 4. Branch name – Mahalaxmi Branch

Eligible Business Associates / OEMs / authorized partner or distributor(s) of OEM are directed to do all communications related to this Invitation for EoI document / documentation, through the following officials:

##### **Level:1**

Name: Sh. Anand Kumar

Position: Jt. General Manager/Marketing

Email: [anandnkn@railtelindia.com](mailto:anandnkn@railtelindia.com)

Contact: +91-9004444107

##### **Level:2**

Name: Sh. Pavan Kumar Bhargava

Position: ED/TM/Bhopal

Email: [pavan@railtelindia.com](mailto:pavan@railtelindia.com)

Note:

1. Empaneled BA's / OEMs / authorized partner or distributor(s) of OEMs are required to submit soft copy (password protected PDF) against EOI response separately for Technical and Financial response through an e-mail at [bploffice@railtelindia.com](mailto:bploffice@railtelindia.com) duly signed by Authorized Signatory with Company seal and stamp. **The size of both the files should not exceed 20 Mb.**
2. **The OEMs need not be prior empaneled Business Associates, given their proven technical prowess. However, The EOI response is invited from eligible Empaneled BA's / Partners of RailTel only in case of participation by Business Associates.**
3. The password will be sought at the time of opening of the bid response packet.
4. All the documents must be submitted with proper indexing and page no.
5. This is an **exclusive arrangement with empaneled business associate/OEMs/authorized partner or distributor(s) of OEM of RailTel for fulfilling the end customer requirements.**
6. Selected partner's authorized signatory has to give an undertaking that, they will not submit directly or indirectly their bids and techno-commercial solution / association with any other organization once selected through this EOI (before and after submission of bid to prospective organization by RailTel). This undertaking has to be given with this EOI Response.
7. **Transfer and Sub-letting.** The Business Associate/OEMs/authorized partner or distributor of OEM has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contract or any part thereof.  
As well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.

## 1. Introduction about RailTel

**RailTel Corporation of India Limited (RailTel)**, an ISO-9001:2000 organization is a “**Navratna**” company under Ministry of Railways, Government of India. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

RailTel has approximately 70000 kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon and Secunderabad hosting / collocating critical applications. RailTel is also providing Telepresence as a Service (TPaaS), where a High- Definition Video Conference facility bundled with required BW is provided as a Service.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Executive Director and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. These regions are further divided into territories for efficient working. RailTel has territorial offices at Guwahati, & Bhubaneswar in East, Chandigarh, Jaipur, Lucknow in North, Chennai & Bangalore in South, Bhopal, and Pune & Ahmedabad in West. Various other territorial offices across the country are proposed to be created shortly.

RailTel’s business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers):

Licenses & Service portfolio:

Presently, RailTel holds Infrastructure Provider -1, National Long-Distance Operator, International Long-Distance Operator and Internet Service Provider (Class-A) licenses under which the following services are being offered to various customers:



**a) Carrier Services**

- National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
- Lease Line Services: Available for granularities from E1 to multiple of Gigabit bandwidth & above
- Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
- Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

**b) Enterprise Services**

- Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
- MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 2 Mbps & above
- Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2 Mbps to several Gbps

**c) DATA CENTER** Infrastructure as a service (IaaS), Hosting as Services, Security operation Centre as a Service (SOCaaS): RailTel has MeitY empaneled two Tier-III data centres in Gurgaon & Secunderabad. Presently RailTel is hosting critical applications of Indian Railways, Central & State government/ PSUs applications. RailTel will facilitate Government's applications / Hosting services including smooth transition to secured state owned RailTel's Data Centers and Disaster Recovery Centres. RailTel also offers SOC as a Service 'SOCaaS'. In addition, RailTel offers VPN client services so that employees can seamlessly access government's intranet, applications securely from anywhere without compromising security.

- National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
- Lease Line Services: Available for granularities from E1 to multiple of Gigabit bandwidth & above
- Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
- Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

**d) High-Definition Video Conference:** RailTel has unique service model of providing high-definition video conference bundled with Video Conference equipment, bandwidth and FMS services to provide end to end seamless services on OPEX model connecting HQ with other critical offices. RailTel also offers application-based video conference solution for employees to be productive specially during this pandemic situation.

**e) Retail Services – RailWire**

RailWire: Triple Play Broadband Services for the Masses. RailTel has unique model of delivering broadband services, wherein local entrepreneurs are engaged in delivering &

maintaining broadband services and upto 66% of the total revenues earned are shared to these local entrepreneurs in the state, generating jobs and revitalizing local economies. On date RailTel is serving approx. 4,00,000 subscribers on PAN Indian basis. RailTel can provide broadband service across– Government PSU or any organization’s officers colonies and residences.

## **2. Project Background and Objective of EOI**

RailTel intends to participate in the work for “Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh”

RailTel Corporation of India Ltd., publishes EOI to select suitable partner among RailTel’s Empaneled BA / OEMs / OEM’s authorized partner / distributor(s) for work of “**Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh**”. The empaneled partner/OEMs/authorized partner or distributor of OEMs is expected to have excellent execution capability and good understanding about customer’s local environment.

## **3. Scope of Work**

The scope of work is to execute all end to end work comes under RFP Ref. 160662 Dated: 28.10.2024, titled as “Select Empaneled BA / OEMs / OEM’s authorized partner / distributor(s) for Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh” as per there requirement.

The above scope of work is indicative, and the detailed scope of work will be shared after the completion of the EOI process.

In case of any discrepancy or ambiguity in any clause / specification pertaining to the scope of work area, the decision of the end customer organization shall supersede and will be considered sacrosanct. (All clarifications, response to queries, revisions, addendum and corrigendum, associated prime service agreement (PSA)/MSA/SLA also included.)

**Special Note: RailTel may retain some portion of the work mentioned in the end organization RFP, where RailTel has competence so that overall proposal becomes most winnable proposal. Scope of Work and payment terms shall be on a back-to-back basis as per the end customer RFP.**

## 4. Response to EOI guidelines

### 4.1 Language of Proposals

The proposal and all correspondence and documents shall be written in English in password protected PDF file through an email (size of email should not exceed 20Mb) to [bpltooffice@railtelindia.com](mailto:bpltooffice@railtelindia.com).

### 4.2 RailTel's Right to Accept/Reject responses

RailTel reserves the right to accept or reject any response and annul the bidding process or even reject all responses at any time prior to selecting the partner, without thereby incurring any liability to the affected bidder or Business Associate/OEM/authorized partner or distributor of OEM or without any obligation to inform the affected bidder or bidders about the grounds for RailTel's action.

### 4.3 EOI response Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder's risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed by the bidder including the closing page in token of his having studied the EOI document and should be submitted along with the bid.

### 4.4 Period of Validity of bids and Bid Currency

Bids shall remain valid for 180 days from the date of submission.

### 4.5 Bidding Process

The bidding process as defined in EOI.

### 4.6 Bid Earnest Money (EMD)

4.6.1 The Business Associate shall furnish the EMD as described in DATA SHEET (Page-2 of EOI).

4.6.2 Offers not accompanied with valid Earnest Money Deposit and tender fee, processing fee deposition details shall be summarily rejected.

4.6.3 The validity of such EMD shall be maintained till the finalization of end Customer RFP/Tender i.e. award of order and till submission of Performance Guarantee of requisite value required by end customer on back-to-back basis.

4.6.4 **Return of EMD for unsuccessful Business Associates:** Final EMD of the unsuccessful Business Associate shall be returned without interest after completion of EOI process (i.e. after pre-bid agreement is signed with the selected partner)

4.6.5 **Return of EMD for successful Business Associate:** Final Earnest Money Deposit of the successful bidder will be discharged / returned as promptly as possible after the receipt of RailTel's EMD/BG from the Customer and or on receipt of Security Deposit Performance Bank Guarantee as applicable from Business Associate whichever is later.

#### 4.6.6 Forfeiture of EMD and or Penal action as per EMD Declaration:

4.6.6.1 The EOI EMD may be forfeited and or penal action shall be initiated, if a Business Associate withdraws his offer or modifies the terms and conditions of the offer during validity period.

#### 4.7 Security Deposit / Performance Bank Guarantee (PBG)

4.7.1 In case the bid is successful, the PBG / SD of full amount as asked by end customer will be submitted / deposited by selected BA in favour of RailTel Corporation of India Limited.

#### 4.8 Last date & time for Submission of EOI response

EOI response must be submitted to RailTel at the email address specified in the DATA SHEET not later than the specified date and time mentioned in the DATA SHEET.

#### 4.9 Modification and/or Withdrawal of EOI response

EOI response once submitted will be treated, as final and no modification will be permitted except with the consent of the RailTel. No Business Associate shall be allowed to withdraw the response after the last date and time for submission.

The successful Business Associate will not be allowed to withdraw or back out from the response commitments. In case of withdrawal or back out by the successful business associate, the Earnest Money Deposit shall be forfeited, and all interests/claims of such Business Associate shall be deemed as foreclosed.

#### 4.10 Clarification of EOI Response

To assist in the examination, evaluation and comparison of bids, the purchaser may, at its discretion, ask the Business Associate for clarification. The response should be in writing and no change in the price or substance of the EOI response shall be sought, offered or permitted.

#### 4.11 Period of Association / Validity of Agreement

RailTel will enter into agreement with selected bidder with detailed Terms and conditions.

### 5. Pre-Qualification Criteria for Bidding Business Partner of RailTel

S No.	Particulars	Criteria for Tender Package
		(Mandatory Compliance & Document Submission)
1	The MSI Bidder must be incorporated and registered in India under the Indian Companies Act 1956 or 2013, or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for a minimum of five years as on 31.03.2024. The MSI Bidder must be registered with appropriate authorities for all applicable statutory duties/taxes.	1. Copy of certificate of Incorporation / Registration under Companies Act 1956/2013 (for Indian companies) 2. Copy of GST certificate 3. Copy of PAN Card 4. Valid Empanelment letter (LOI) issued by RailTel (* BA with expired LOI will not be considered)



2.	MSI Bidder must have average annual turnover of INR 150 crores from IT/ITES business for last three audited financial years (i.e. FY 2021-22, 2022-23, 2023-24) And MSI Bidder should have a positive net worth as on bid submission date.	1. Copy of audited profit and loss account and balance sheet for latest three financial years (FY 2021-22, 2022-23, 2023-24) 2. Certificate from Statutory Auditor with UDIN and stamp for both average annual turnover and positive net worth.
3.	MSI Bidder should have established/implemented Data Centre projects for Central / State Governments, PSUs, PSEs in India in the last five (5) years: a. One project of value INR 80 Crores or more; OR b. Two projects each having minimum value of INR 60 Crores or more; OR c. Three projects each having minimum value of INR 40 Crores or more The Data Centre project consisting of Supply, Installation, Testing and Commissioning (SITC) of IT components such as server, storage, backup system, network, cyber security equipment for the Data Centre; Non-IT components including installation, commissioning of any of these Electrical Distribution & Lighting, DG sets, Precision AC/ Chiller Plant, UPS System, Fire Detection & suppression system, Access Control and CCTV, BMS System. Note: Bidder's in-house projects setup will not be considered.  Note: Bidder's in-house projects setup will not be considered	1. Work orders & Completion certificate 2. Datacentre Completion certificates on the client letter head for the completed project also signed by the authorized signatory.
5.	MSI Bidder should have experience of setting up and managing NOC operations, Service Desk for Central / State Governments / PSUs /PSEs in India in last 5 years Note: Bidder's in-house projects setup will not be considered	For on-going projects: 1. Work orders & Agreement highlighting scope of work. 2. In progress certificates on the client letter head of the projects For completed projects: 1. Work orders & Agreement highlighting scope of work. 2. Completion certificates on the client letter head of the projects/Self-Certificate by the authorised signatory
6.	The MSI Bidder shall provide all the three Certifications valid at the time of bidding: • ISO 9001:2015 or latest certification • ISO 20000:2018 or latest certification • ISO 27001:2013 or latest certification	Copies of the valid certificates in the name of the MSI.
7.	As on date of submission of the proposal, the MSI Bidder, shall not be blacklisted / debarred by any State / Central Government Department or Central /State PSUs / PSEs.	The MSI Bidder Undertaking as per the format on company letter head.

8.	Furnishing of the Power of Attorney	Power of Attorney executed by the MSI Bidder in favor of the duly Authorized signatory, certifying him/her as an authorized signatory for the purpose of this Tender.
9.	<p>The MSI Bidder should submit valid letter from all the OEMs confirming the following:</p> <p>a. Authorization for MSI Bidder Confirm that the products quoted are not “end of life” or “end of sale products”.</p> <p>b. Undertake that the support including spares, patches for the quoted products shall be available for defined project duration</p>	<p>Documentary evidence</p> <p>1. Authorization letters on OEM Letter Head and</p> <p>2. Manufacturer’s Authorization Form (MAF) from all OEMs’ in their Letterhead whose products are being quoted by the MSI</p>
10.	OEM for Server, Storage, Networking, Backup, Security must have direct or registered service partner presence in India.	An undertaking from each OEM on the direct or registered service partner presence in India.

<b>S No.</b>	<b>Annexures</b>	<b>Description</b>
1	<b>Annexure 1</b>	<b>Covering Letter:</b> Self-certification duly signed by authorized signatory on company letter head.
2	<b>Annexure 2</b>	The Bidder should agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted.
		Self-certification duly signed by authorized signatory on company letter head.
3	<b>Annexure 3</b>	An undertaking signed by the Authorized Signatory of the company to be provided on letter head. The Bidder should not have been blacklisted / debarred by any Governmental / Non-Governmental Organization in India as on bid submission date.
4	<b>Annexure-4</b>	Format for Affidavit to be uploaded by BA along with the tender documents.
5	<b>Annexure-5</b>	Non-disclosure agreement with RailTel.
6	<b>Annexure-6</b>	Bank Mandate
7	<b>Annexure-7</b>	Bank Guarantee Format
8	<b>Annexure-8</b>	Tender Document
9	<b>Annexure - 9</b>	Power of Attorney and Board Resolution in favor of one of its employees who will sign the Bid Documents.
10	<b>Additional Documents to be Submitted</b>	Technical Proposal with overview of the project with strength of the Partner.
11	<b>Annexure-10</b>	BOQ of the RFP document. Price Bid Format to be submitted in separate password protected pdf.

## 6. Bidder's Profile

The bidder shall provide the information in the below table:

S. No.	ITEM	Details
1.	Full name of bidder's firm	
2.	Full address, telephone numbers, fax numbers, and email address of the primary office of the organization / main / head / corporate office	
3.	Name, designation and full address of the Chief Executive Officer of the bidder's organization as a whole, including contact numbers and email Address	
4.	Full address, telephone and fax numbers, and email addresses of the office of the organization dealing with this tender	
5.	Name, designation and full address of the person dealing with the tender to whom all reference shall be made regarding the tender enquiry. His/her telephone, mobile, Fax and email address	
6.	Bank Details (Bank Branch Name, IFSC Code, Account number)	
7.	GST Registration number	

## 7. Evaluation Criteria

- 7.1 The Business Associates are first evaluated on the basis of the Pre-Qualification Criteria as per clause 5 above.
- 7.2 The Business Associate who meets all the Pre-qualification criteria, their price bid will be evaluated. The Lowest (L1) price bidder will be selected and entered into agreement with for delivery of the work on back-to-back basis for the agreed scope of work.
- 7.3 RailTel reserves the right to further re-negotiate the prices with eligible L1 bidder. Selected bidder must ensure the best commercial offer to RailTel to offer the most winnable cost to customer.
- 7.4 RailTel also reserves the right to accept or reject the response against this EOI, without assigning any reasons. The decision of RailTel is final and binding on the participants. The RailTel evaluation committee will determine whether the proposal/ information is complete in all respects and the decision of the evaluation committee shall be final. RailTel may at its discretion assign lead factor to the Business associate as per RailTel policy for shortlisting partner against this EOI. RailTel also reserves the right to negotiate the price with the selected bidder.
- 7.5 All General requirement mentioned in the Technical Specifications are required to be complied. The solution proposed should be robust and scalable.

## 8. Payment terms

- 8.1 RailTel shall make payment to selected Business Associate after receiving payment from Customer for the agreed scope of work. In case of any penalty or deduction made by customer for the portion of work to be done by BA, same shall be passed on to Business Associate.
- 8.2 All payments by RailTel to the Partner will be made after the receipt of payment by RailTel from end Customer organization.

## 9. SLA

The selected bidder will be required to adhere the SLA matrix if as defined by the end Customer. SLA breach penalty will be applicable proportionately on the selected bidder, as specified by the end Customer. The SLA scoring and penalty deduction mechanism for in-scope of work area shall be followed as specified by the customer. All clarifications, responses to queries, revisions, addendum and corrigendum, associated Prime Services Agreement (PSA)/ MSA/ SLA also included. Any deduction by Customer from RailTel payments on account of SLA breach which is attributable to Partner will be passed on to the Partner proportionately based on its scope of work.

## 10. Other Terms and Conditions

Any other terms and conditions in relation to SLA, Payments, PBG etc. will be as per the PO/agreement/Work Order/RFP of the end customer.

**Note: Depending on RailTel's business strategy RailTel may choose to work with Partner who is most likely to support in submitting a winning bid.**

**Annexure 1**

**COVERING LETTER**  
(To be submitted on company letter head)

EoI Reference No:

Date :

To,

RailTel Corporation of India Ltd.  
Plot No. 17, First Floor,  
Raghunath Nagar,  
Near Shahpura Thana,  
Bhopal, M.P. - 462039

Dear Sir,

SUB: Participation in the EoI process

Having examined the Invitation for EoI document bearing the ref. no. \_\_\_\_\_ released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document.

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

We hereby Submit EMD amount of Rs. \_\_\_\_\_ issued vide \_\_\_\_\_ from Bank \_\_\_\_\_.

Authorized Signatory

Name

Designation

Self-Certificate  
(To be submitted on company letter head)

EoI Reference No:

Date:

To,

RailTel Corporation of India Ltd.  
Plot No. 17, First Floor,  
Raghunath Nagar,  
Near Shahpura Thana,  
Bhopal, M.P. - 462039

Dear Sir,

**Sub: Self Certificate for Tender, Technical & other compliances**

- 1) Having examined the Technical specifications mentioned in this EOI & end customer tender, we hereby confirm that we meet all specification.
- 2) We agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted (except pricing, termination & risk purchase rights of the RailTel). We understand and agree that RailTel shall release the payment to selected BA after the receipt of corresponding payment from end customer by RailTel. Further we understand that in case selected BA fails to execute assigned portion of work, then the same shall be executed by RailTel through third party or departmentally at the risk and cost of selected BA.
- 3) We agree to abide by all the technical, commercial & financial conditions of the end customer's RFP for the agreed scope of work for which this EOI is submitted.
- 4) We hereby agree to comply with all OEM technical & Financial documentation including MAF, Technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP. We are hereby enclosing the arrangement of OEMs against each of the BOQ item quoted as mentioned end customer's RFP. We also undertake to submit MAF and other documents required in the end Customer organization tender in favour of RailTel against the proposed products.
- 5) We hereby undertake to work with RailTel as per end customer's RFP terms and conditions. We confirm to submit all the supporting documents constituting/ in compliance with the Criteria as required in the end customer's RFP terms and conditions like technical certificates, OEM compliance documents.
- 6) We understand and agree that RailTel is intending to select a BA who is willing to accept all terms & conditions of end customer organization's RFP for the agreed scope of work. RailTel will strategies to retain scope of work where RailTel has competence.



- 7) We hereby agree to submit that in case of being selected by RailTel as BA for the proposed project (for which EOI is submitted), we will submit all the forms, appendix, relevant documents etc. to RailTel that is required and desired by end Customer well before the bid submission date by end customer and as and when required.
- 8) We hereby undertake to sign Pre-Bid Agreement and Non-Disclosure Agreement with RailTel on a non-judicial stamp paper of Rs. 100/- in the prescribed Format.

Authorized Signatory

Name & Designation

**Annexure 3:**

**Undertaking for not Being Blacklisted/Debarred**  
(To be submitted on Company Letter Head)

To,

RailTel Corporation of India Ltd.  
Plot No. 17, First Floor,  
Raghunath Nagar,  
Near Shahpura Thana,  
Bhopal, M.P. - 462039

Subject: Undertaking for not Being Blacklisted/Debarred

We, \_\_\_\_\_ Company Name \_\_\_\_\_, having its registered office at  
\_\_\_\_\_ address \_\_\_\_\_ hereby declares that that the Company  
has not been blacklisted/debarred by any Governmental / Non-Governmental organization in India  
for past 3 Years as on bid submission date.

Date and Place

Authorized Signatory's Signature:

Authorized Signatory's Name and Designation:

Bidder's Company Seal:

**Annexure 4:**

**Format of Affidavit**  
**FORMAT FOR AFFIDAVIT TO BE UPLOADED BY BA ALONGWITH THE EOI**  
**DOCUMENTS**

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 100/-.  
The paper has to be in the name of the BA) \*\*

I..... (Name and designation) \*\* appointed as the attorney/authorized  
signatory of the BA (including its constituents),

M/s.....(hereinafter called the BA) for the purpose of the EOI  
documents for the work of ..... as per the EOI No.  
..... of (RailTel Corporation of India Ltd.), do hereby solemnly affirm and state on the  
behalf of the BA including its constituents as under:

1. I/we the BA (s), am/are signing this document after carefully reading the contents.
2. I/we the BA(s) also accept all the conditions of the EOI and have signed all the pages in confirmation thereof.
3. I/we hereby declare that I/we have downloaded the EOI documents from RailTel website [www.railtelindia.com](http://www.railtelindia.com). I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the EOI document. In case of any discrepancy noticed at any stage i.e. evaluation of EOI, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.
4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.
5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.
6. I/we declare that the information and documents submitted along with the EOI by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.
7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of EOI, it shall lead to forfeiture of the EOI EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the BA) \*\* ..... and all my/our constituents understand that my/our constituents understand that my/our offer shall be summarily rejected.

8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

DEPONENT SEAL AND SIGNATURE  
OF THE BA

#### VERIFICATION

I/We above named EOI do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT SEAL AND SIGNATURE  
OF THE BA

Place:  
Dated:

**\*\*The contents in Italics are only for guidance purpose. Details as appropriate, are to be filled in suitably by BA. Attestation before Magistrate/Notary Public.**

### **NON-DISCLOSURE AGREEMENT**

This Non-Disclosure Agreement (this “**Agreement**”) is made and entered into on this \_\_\_\_ day of \_\_\_\_, 2024 (the “**Effective Date**”) at \_\_\_\_\_. By and between

**RailTel Corporation of India Limited, (CIN: L64202DL2000GOI107905)**, a Public Sector Undertaking under Ministry of Railways, Govt. of India, having its registered and corporate office at Plate-A, 6th Floor, Office Block, Tower -2, East Kidwai Nagar, New Delhi-110023, (hereinafter referred to as '**RailTel**'), which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of the ONE PART,

And

\_\_\_\_\_) (CIN: \_\_\_\_\_), a company duly incorporated under the provisions of Companies Act, \_\_\_\_\_ having its registered office at \_\_\_\_\_, (hereinafter referred to as '**\_\_\_\_\_**'),

which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of OTHER PART

RailTel and \_\_\_\_\_ shall be individually referred to as “Party” and jointly as “Parties”

WHEREAS, RailTel and \_\_\_\_\_, each possesses confidential and proprietary information related to its business activities, including, but not limited to, that information designated as confidential or proprietary under Section 2 of this Agreement, as well as technical and non-technical information, patents, copyrights, trade secrets, know-how, financial data, design details and specifications, engineering, business and marketing strategies and plans, forecasts or plans, pricing strategies, formulas, procurement requirements, vendor and customer lists, inventions, techniques, sketches, drawings, models, processes, apparatus, equipment, algorithms, software programs, software source documents, product designs and the like, and third party confidential information (collectively, the “**Information**”);

WHEREAS, the Parties have initiated discussions regarding a possible business relationship for \_\_\_\_\_.

WHEREAS, each Party accordingly desires to disclose certain Information (each Party, in such disclosing capacity, the “**Disclosing Party**”) to the other Party (each Party, in such receiving capacity, the “**Receiving Party**”) subject to the terms and conditions of this Agreement.

NOW THEREFORE, in consideration of the receipt of certain Information, and the mutual promises made in this Agreement, the Parties, intending to be legally bound, hereby agree as follows:

**Permitted Use.**

Receiving Party shall:

hold all Information received from Disclosing Party in confidence; use such Information for the purpose of evaluating the possibility of entering into a commercial arrangement between the Parties concerning such Information; and restrict disclosure of such Information to those of Receiving Party’s officers, directors, employees, affiliates, advisors, agents and consultants (collectively, the “**Representatives**”) who the Receiving Party, in its reasonable discretion, deems need to know such Information, and are bound by the terms and conditions of (1) this Agreement, or (2) an agreement with terms and conditions substantially similar to those set forth in this Agreement.

The restrictions on Receiving Party's use and disclosure of Information as set forth above shall not apply to any Information that Receiving Party can demonstrate: is wholly and independently developed by Receiving Party without the use of Information of Disclosing Party; at the time of disclosure to Receiving Party, was either (A) in the public domain, or (B) known to Receiving Party; is approved for release by written authorization of Disclosing Party; or is disclosed in response to a valid order of a court or other governmental body in the India or any political subdivision thereof, but only to the extent of, and for the purposes set forth in, such order; provided, however, that Receiving Party shall first and immediately notify Disclosing Party in writing of the order and permit Disclosing Party to seek an appropriate protective order.

(c) Both parties further agree to exercise the same degree of care that it exercises to protect its own Confidential Information of a like nature from unauthorised disclosure, but in no event shall a less than reasonable degree of care be exercised by either party.

**Designation.**

Information shall be deemed confidential and proprietary and subject to the restrictions of this Agreement if, when provided in:

written or other tangible form, such Information is clearly marked as proprietary or confidential when disclosed to Receiving Party; or oral or other intangible form, such Information is identified as confidential or proprietary at the time of disclosure.

**Cooperation.** Receiving Party will immediately give notice to Disclosing Party of any unauthorized use or disclosure of the Information of Disclosing Party.

**Ownership of Information.** All Information remains the property of Disclosing Party and no license or other rights to such Information is granted or implied hereby. Notwithstanding the foregoing, Disclosing Party understands that Receiving Party may currently or in the future be developing information internally, or receiving information from other parties that may be similar to Information of the Disclosing Party. Notwithstanding anything to the contrary, nothing in this Agreement will be construed as a representation or inference that Receiving Party will not develop products, or have products developed for it, that, without violation of this Agreement, compete with the products or systems contemplated by Disclosing Party's Information.

**No Obligation.** Neither this Agreement nor the disclosure or receipt of Information hereunder shall be construed as creating any obligation of a Party to furnish Information to the other Party or to enter into any agreement, venture or relationship with the other Party.

**Return or Destruction of Information.**

All Information shall remain the sole property of Disclosing Party and all materials containing any such Information (including all copies made by Receiving Party) and its Representatives shall be returned or destroyed by Receiving Party immediately upon the earlier of:

termination of this Agreement; expiration of this Agreement; or  
Receiving Party's determination that it no longer has a need for such Information.

Upon request of Disclosing Party, Receiving Party shall certify in writing that all Information received by Receiving Party (including all copies thereof) and all materials containing such Information (including all copies thereof) have been destroyed.

**Injunctive Relief:** Without prejudice to any other rights or remedies that a party may have, each party acknowledges and agrees that damages alone may not be an adequate remedy for any breach of this Agreement, and that a party shall be entitled to seek the remedies of injunction, specific performance and/or any other equitable relief for any threatened or actual breach of this Agreement

**Notice.**

Any notice required or permitted by this Agreement shall be in writing and shall be delivered as follows, with notice deemed given as indicated:

by personal delivery, when delivered personally; by overnight courier, upon written verification of receipt; or by certified or registered mail with return receipt requested, upon verification of receipt.

Notice shall be sent to the following addresses or such other address as either Party specifies in writing.

Attn: \_\_\_\_\_

Address: \_\_\_\_\_

Phone:

Email.:

Attn: \_\_\_\_\_

Address: \_\_\_\_\_

Phone:

Email:

### **Term, Termination and Survivability.**

Unless terminated earlier in accordance with the provisions of this agreement, this Agreement shall be in full force and effect for a period of \_\_\_\_years from the effective date hereof.

Each party reserves the right in its sole and absolute discretion to terminate this Agreement by giving the other party not less than 30 days' written notice of such termination.

Notwithstanding the foregoing clause 9(a) and 9 (b), Receiving Party agrees that its obligations, shall:

In respect to Information provided to it during the Term of this agreement, shall survive and continue even after the expiry of the term or termination of this agreement; and not apply to any materials or information disclosed to it thereafter.

**Governing Law and Jurisdiction.** This Agreement shall be governed in all respects solely and exclusively by the laws of India without regard to its conflicts of law principles. The Parties hereto expressly consent and submit themselves to the jurisdiction of the courts of New Delhi.

**Counterparts.** This agreement is executed in duplicate, each of which shall be deemed to be the original and both when taken together shall be deemed to form a single agreement

**No Definitive Transaction.** The Parties hereto understand and agree that no contract or agreement with respect to any aspect of a potential transaction between the Parties shall be deemed to exist unless and until a definitive written agreement providing for such aspect of the transaction has been executed by a duly authorized representative of each Party and duly delivered to the other Party (a "**Final Agreement**"), and the Parties hereby waive, in advance, any claims in connection with a possible transaction unless and until the Parties have entered into a Final Agreement.

### **Settlement of Disputes:**

The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation or consultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.

In the event of any dispute, difference, conflict or question arising between the parties hereto, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator.

The sole arbitrator shall be appointed by CMD/RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the parties.

### **CONFIDENTIALITY OF NEGOTIATIONS**

Without the Disclosing Party's prior written consent, the Receiving Party shall not disclose to any Person who is not a Representative of the Receiving Party the fact that Confidential Information has been made available to the Receiving Party or that it has inspected any portion of the Confidential Information or that discussions between the Parties may be taking place.



## **REPRESENTATION**

The Receiving Party acknowledges that the Disclosing Party makes no representation or warranty as to the accuracy or completeness of any of the Confidential Information furnished by or on its behalf. Nothing in this clause operates to limit or exclude any liability for fraudulent misrepresentation.

## **ASSIGNMENT**

Neither this Agreement nor any of the rights, interests or obligations under this Agreement shall be assigned, in whole or in part, by operation of law or otherwise by any of the Parties without the prior written consent of each of the other Parties. Any purported assignment without such consent shall be void. Subject to the preceding sentences, this Agreement will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns. its Affiliates to advise their Representatives, contractors, subcontractors and licensees, of the obligations of confidentiality and non-use under this Agreement, and shall be responsible for ensuring compliance by its and its Affiliates' Representatives, contractors, subcontractors and licensees with such obligations. In addition, each Party shall require all persons and entities who are not employees of a Party and who are provided access to the Confidential Information, to execute confidentiality or non-disclosure agreements containing provisions no less stringent than those set forth in this Agreement. Each Party shall promptly notify the other Party in writing upon learning of any unauthorized disclosure or use of the Confidential Information by such persons or entities.

## **NO LICENSE**

Nothing in this Agreement is intended to grant any rights to under any patent, copyright, or other intellectual property right of the Disclosing Party, nor will this Agreement grant the Receiving Party any rights in or to the Confidential Information of the Disclosing Party, except as expressly set forth in this Agreement.

## **RELATIONSHIP BETWEEN PARTIES:**

Nothing in this Agreement or in any matter or any arrangement contemplated by it is intended to constitute a partnership, association, joint venture, fiduciary relationship or other cooperative entity between the parties for any purpose whatsoever. Neither party has any power or authority to bind the other party or impose any obligations on it and neither party shall purport to do so or hold itself out as capable of doing so.

## **20: UNPULISHED PRICE SENSITIVE INFORMATION (UPSI)**

\_\_\_\_\_ agrees and acknowledges that \_\_\_\_\_, its Partners, employees, representatives etc., by virtue of being associated with RailTel and being in frequent communication with RailTel and its employees, shall be deemed to be "Connected Persons" within the meaning of SEBI (Prohibition of Insider Trading) Regulations, 2015 and shall be bound by the said regulations while dealing with any confidential and/ or price sensitive information of RailTel. \_\_\_\_\_ shall always and at all times comply with the obligations and restrictions contained in the said regulations. In terms of the said regulations, \_\_\_\_\_ shall abide by the restriction on communication, providing or allowing access to any Unpublished Price Sensitive Information (UPSI) relating to RailTel as well as restriction on trading of its stock while holding such Unpublished Price Sensitive Information relating to RailTel

**MISCELLANEOUS.** This Agreement constitutes the entire understanding among the Parties as to the Information and supersedes all prior discussions between them relating thereto. No amendment or modification of this Agreement shall be valid or binding on the Parties unless made in writing and signed on behalf of each Party by its authorized representative. The failure or delay of any Party to enforce at any time any provision of this Agreement shall not constitute a waiver of such Party's right thereafter to enforce each and every provision of this Agreement. In the event that any of the terms, conditions or provisions of this Agreement are held to be illegal, unenforceable or invalid by any court of competent jurisdiction, the remaining terms, conditions or provisions hereof shall remain in full force and effect. The rights, remedies and obligations set forth herein are in addition to, and not in substitution of, any rights, remedies or obligations which may be granted or imposed under law or in equity.

IN WITNESS WHEREOF, the Parties have executed this Agreement on the date set forth above.

\_\_\_\_\_:

RailTel Corporation of India Limited:

By\_\_\_\_\_

By\_\_\_\_\_

Name:

Name:

Title:

Title:

Witnesses

## Annexure-6 – Bank Mandate



**Mahalaxmi Branch  
Mahalaxmi Chambers  
22, Bhulabhai Desai Road  
MUMBAI: 400 026**

**Tel. No. No.23512895 / 23517234 Fax No.23516948**

**LT No:MAH/RCIL/2010**

**Date: 21/10/2010**

To,  
The Sr. Manager (Finance)  
Railtel Corporation Of India Limited  
Mahalaxmi, Mumbai

Dear Sir,

Sub-: Bank Details For your collection account.

We are in receipt of your letter no. RCIL/WR/Fin/Bank Matters dated 20.10.2010  
Requesting bank details for your collection account no. 317801010036605. Details are below:-

Account No.- 317801010036605

A/c Name- Railtel WR collection A/c

Bank Name- UNION BANK OF INDIA

Branch name- Mahalaxmi, branch

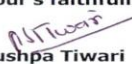
Branch address- 22, bhulabhai desai Road, Mahalaxmi chambers,  
Mahalaxmi, Mumbai-400026

IFSC Code- UBIN0531782

Swift Code- UBININBBLOP

Thanking You

Your's faithfully

  
Pushpa Tiwari  
Manager



**Bank Guarantee for Earnest Money Deposit**

(To be stamped in accordance with stamp act)

Ref: Bank Guarantee #

Date -

Principle Executive Director,  
Western Region  
RailTel Corporation of India Limited,  
Mahalaxmi, Mumbai.

Dear Sir,

In accordance with your bid reference no. \_\_\_\_\_ Dated  
\_\_\_\_\_ M/s \_\_\_\_\_ (Bidder's Name ) \_\_\_\_\_

herein after (Called 'bidder') wish to participate in the said EOI to select suitable partner among RailTel's Empaneled BA / OEMs / OEM's authorized partner / distributor(s) for work of "**Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh**".

An irrevocable Financial Bank Guarantee (issued by a nationalized / scheduled commercial Bank) against Earnest Money Deposit amounting to Rs. 30000000/- Rupees (Rupees Three Crore only) Valid up to (270 days since EOI submission last date) is required to be submitted by the bidder, as a condition for participation in the said EOI, in which amount is liable to be forfeited on happening of any contingencies mentioned in the EOI document.

M/s \_\_\_\_\_ (Bidder's Name) \_\_\_\_\_, has undertaken in pursuance of their offer to RailTel Corporation of India Limited (hereinafter called as the beneficiary) dated \_\_\_\_\_ has expressed its intention to participate in the said EOI and in terms thereof has approached us and requested us ..... (Name of Bank) ..... (Address of Bank) to issue an irrevocable financial Bank Guarantee against Earnest Money Deposit (EMD) amounting to Rs 30000000 /- Rupees (Rupees Three crore only) valid up to .....

We, the \_\_\_\_\_ (Name of Bank) \_\_\_\_\_ (Address of Bank) having our Head office at \_\_\_\_\_ therefore Guarantee and undertake to pay immediately on first written demand by RailTel Corporation of India Limited, the amount Rs. \_\_\_\_\_ Rupees (in words) without any reservation, protest, demur and recourse in case the bidder fails to Comply with any condition of the bid or any violation against the terms of the bid, Without the beneficiary needing to prove or demonstrate reasons for its such demand. Any Such demand made by said beneficiary shall be conclusive and binding on us irrespective of any dispute or difference raised by the bidder.

This guarantee shall be irrevocable and shall remain valid up to \_\_\_\_\_. If any further extension of this Guarantee is required, the same shall be extended to such required period on receiving instructions in writing, from RailTel Corporation of India Limited, on whose behalf guarantee is issued.

This Bank guarantee shall be valid up to \_\_\_\_\_. We are liable to pay the guaranteed amount or any part thereof under this Bank guarantee only if you serve upon us a written claim or demand, on or before hours (Indian Standard Time) where after it ceases to be in effect in all respects whether or not the original Bank guarantee is returned to us."

In witness whereof the Bank, through its authorized officer has set its hand stamped on this \_\_\_\_\_ Day of \_\_\_\_\_ 2024 at \_\_\_\_\_.

**Beneficiary Bank Detail as below –**

1. Name of the Bank - Union Bank of India
2. IFSC Code - UBIN0531782
3. Branch name – Mahalaxmi Branch

**Name of signatory:**

**Designation:**

**Email ID:**

**Contact No.:**

**Bank Common Seal:**

**Tender Document**

**Annexure- 8**

# Request for Proposal for Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh

**Issued By:  
Chhattisgarh Infotech Promotion Society  
(CHIPS)**



SDC Building,  
02nd floor, Near Police Control Room, Civil Lines  
Raipur, Chhattisgarh– 492001  
Fax:- 0771-4066205, Ph No. 0771-4014158  
E-mail: ceochips@nic.com, Website: [www.chips.gov.in](http://www.chips.gov.in)

## Disclaimer

Chhattisgarh Infotech Promotion Society (CHiPS) is the nodal agency and prime mover for propelling IT growth & implementation of the IT & e-Governance projects in the State of Chhattisgarh. CHiPS has prepared this **Request for Proposal (RFP) for the Selection of Master System Integrator (MSI) for CGSDC2.0 in the State of Chhattisgarh**. This RFP is a detailed document that specifies the terms and conditions on which the MSI is expected to work. These terms and conditions are designed keeping in view the overall aims and objectives of the Chhattisgarh State Data Centre (CGSDC).

CHiPS has taken due care in the preparation of the information contained herein and believes it to be accurate. However, neither CHiPS nor any of its authorities or agencies nor any of the irrespective officers, employees, agents, or advisors gives any lit warranty or makes any representations, express, or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it. This Tender may not be appropriate for all persons, and it is not possible for the CHiPS, its employees, or advisers to consider the objectives, technical expertise and particular needs of each party who reads or uses this tender.

This Tender is not an agreement and is neither an offer nor invitation by the CHiPS to the prospective MSIs or any other person. The information provided in this document is to assist the MSI(s) in preparing their proposals. However, this information is not intended to be exhaustive, and interested parties are expected to make their own inquiries to supplement the information in this document. The information is provided on the basis that it is non-binding on CHiPS any of its authorities or agencies, or any of their respective officers, employees, agents, or advisors. Each MSI is advised to consider the RFP as per its understanding and capacity. The MSIs are also advised to do appropriate examination, enquiry, and scrutiny of all aspects mentioned in the RFP before bidding. MSIs are encouraged to take the professional help of experts on financial, legal, technical, taxation, and any other matters/sectors appearing in the document or specified work. The MSIs should go through the RFP in details and bring to notice of CHiPS any kind of error, misprint, inaccuracy or omission. The CHiPS also accept no liability of any nature whether resulting from negligence or otherwise however caused arising from reliance of any MSI upon the statements contained in this Tender.

The MSI should bear all its costs associated with or relating to the preparation and submission of its Proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the CHiPS or any other costs incurred in connection with or relating to its Proposal. All such costs and expenses will remain with the MSI, and the CHiPS should not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a MSI in preparation or submission of the Bid, regardless of the conduct or outcome of the Selection Process.

CHiPS reserve the right not to proceed with the project, to alter the timetable reflected in this document, or to change the process or procedure to be applied. It also reserves the right to decline to discuss the Project further with any party submitting a proposal, nor reimbursement of cost of any type will be paid to persons, entities submitting a Proposal. CHiPS may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumption contained in this Tender. The issue of this Tender does not imply that CHiPS is bound to select an MSI or MSIs, as the case may be, for the State Data Centre Project and CHiPS reserves the right to reject all or any of the Proposals without assigning any reasons whatsoever.



## Glossary of Terms

Abbreviation	Description
AMC	Annual Maintenance Contract
PBG/BG	Performance Bank Guarantee / Bank Guarantee
MSI	Master Systems Integrator
BMS	Building Management System
BoM	Bill of Material
BoQ	Bill of Quantity
CAPEX/OPEX	Capital Expenditures / Operational Expenses
CGSDC	Chhattisgarh State Data Centre
CHiPS	Chhattisgarh infotech Promotion Society
CSP	Cloud Service Provider
DC/DR	Data Centre/ Disaster Recovery
DD	Demand Draft
EMD	Earnest Money Deposit
EMS	Enterprise Monitoring System
FAT	Final Acceptance Test
GoI	Government of India
IIS	Internet Information Services
LoA	Letter of Authorization
LoI	Letter of Intent
MAF	Manufacturer Authorization Form
MoU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
NDA	Non-Disclosure Agreement
NIT	Notice Inviting Tender
NIPS	Network Intrusion Protection System
NMS	Network Management Services
NOC	Network Operation Centre
O&M	Operations & Maintenance
OEM	Original Equipment Manufacturer
PBH	Primary Business Hour
RFP	Request for Proposal
RTO/RPO	Recovery Point Objective / Recovery Time Objective
SLA	Service Level Agreement
Wi-Fi	Wireless Fidelity
NDR	Network Detection & Response
EDR	Endpoint Detection & Response
HSM	Hardware Security Module
HIPS	Host Intrusion Prevention System
NGFW	Next generation Firewall
WLD	Water Leakage Detection
UPS	Universal Power Supply
NAC	Network Access Control
IDAM	Identity Access Manager
PTZ	Pan Tilt Zoom

## Table of Contents

1. Notice Inviting Tender .....	9
2. Fact Sheet .....	10
3. General .....	12
3.1 About CHiPS .....	12
3.2 About Chhattisgarh .....	12
3.3 About the project .....	12
4. Instructions to MSIs .....	13
4.1 General .....	13
4.2 Compliant Tenders/Completeness of Response .....	13
4.3 Procedure for Submission of Bids .....	14
4.4 Other Conditions of Bid Submission .....	14
4.5 Cost to bid .....	14
4.6 Contents of RFP .....	14
4.7 Clarification on RFP .....	14
4.8 Responses to Pre-Bid Queries and Issue of Corrigendum .....	15
4.9 Amendment of RFP .....	15
4.10 Language of Bids .....	15
4.11 Documents Comprising the Bids .....	15
4.12 Procedure for Submission of Bids .....	16
4.13 Bid Prices .....	17
4.14 Firm Prices .....	17
4.15 Discount .....	17
4.16 MSI Qualification .....	17
4.17 Earnest Money Deposit (EMD) .....	18
4.18 Period of Validity of Bids .....	19
4.19 Format and Signing of Bid .....	19
4.20 Revelation of Prices .....	19
4.21 Terms and Conditions of MSIs .....	19
4.22 Consortium .....	19
4.23 Local Conditions .....	19
4.24 Last Date for Receipt of Bids .....	20
4.25 Late Bids .....	20
4.26 Modification and Withdrawal of Bids .....	20
4.27 Contacting the Purchaser .....	20
4.28 Opening of Technical Bids by Purchaser .....	21

4.29	Purchaser's Right to Vary Scope of Contract.....	21
4.30	Purchaser's Right to Accept Any Bid & to Reject Any or All Bids .....	21
4.31	Notification of Award .....	21
4.32	Award of Contract.....	21
4.33	Annulment & Re-award .....	22
4.34	Placing of Work Order .....	22
4.35	Tender Related Conditions .....	22
4.36	Rejection Criteria.....	23
4.37	Performance Bank Guarantee and Advance Bank Guarantee .....	23
4.38	Fraud and Corrupt Practices.....	24
4.39	Disqualification of the MSI.....	25
4.40	Verification and Disqualification .....	25
5.	General Conditions of the Contract.....	26
5.1	Definitions.....	26
5.2	Interpretations.....	28
5.3	Expected To Examine All Instructions .....	29
5.4	All Costs.....	29
5.5	Professional Excellence and Ethics .....	29
5.6	Failure of Successful MSI .....	29
5.7	Amendment/Cancellation .....	29
5.8	Right to accept or reject any or all Bids .....	29
5.9	Conditional Bids .....	29
5.10	Acceptance Testing .....	29
5.11	Proprietary Rights .....	29
5.12	Delays in performance of supplier's obligation .....	30
5.13	Damages.....	30
5.14	Applicable Law .....	30
5.15	Notices .....	30
5.16	Taxes & Duties .....	30
5.17	Defence of Suits .....	30
5.18	Conditions Precedent .....	30
5.19	Representations & Warranties .....	31
5.20	Scope of Work .....	32
5.21	Key Performance Measurements .....	33
5.22	Commencement and progress .....	33
5.23	Standards of Performance.....	33

5.24	Sub-contract .....	33
5.25	MSI's Obligations.....	34
5.26	MSI's Personnel.....	38
5.27	Contract Administration.....	39
5.28	Purchaser's Right of Monitoring, Inspection and Periodic Audit.....	39
5.29	Purchaser's Obligations .....	39
5.30	Intellectual Property Rights .....	40
5.31	Record of Contract Documents .....	40
5.32	Ownership and Retention of Documents .....	40
5.33	Ownership of Equipment.....	40
5.34	Indemnity.....	41
5.35	Confidentiality.....	41
5.36	Taxes .....	42
5.37	Warranty .....	42
5.38	Term and Extension of the Contract .....	43
5.39	Prices.....	43
5.40	Change Orders/ Alteration/ Variation .....	43
5.41	Suspension of Work .....	46
5.42	Time is of Essence .....	46
5.43	Completion of Contract .....	46
5.44	Special Conditions of Contract.....	46
5.45	Event of Default by the MSI .....	46
5.46	Consequences of Event of Default .....	47
5.47	Termination .....	48
5.48	Consequences of Termination.....	48
5.49	Penalty.....	49
5.50	Liquidated Damages .....	49
5.51	Dispute Resolution .....	49
5.52	Insurance.....	50
5.53	Transfer of Ownership.....	50
5.54	Limitation of the MSI's (MSI) Liability towards the Purchaser .....	51
5.55	Conflict of Interest .....	51
5.56	Severance .....	52
5.57	Governing Language .....	52
5.58	"No Claim" Certificate .....	52
5.59	Publicity.....	52

5.60	Force Majeure .....	53
5.61	General .....	53
5.62	Exit Management Plan .....	55
5.63	IT Act 2008 .....	56
5.64	Pre-Contract Integrity Pact .....	57
6.	Bid Evaluation .....	57
6.1	Evaluation Process of Bids .....	57
6.2	Eligibility Criteria & Evaluation .....	58
6.3	Evaluation of Commercial Bids .....	60
6.4	Final Bid Evaluation .....	60
7.	Scope of Work .....	61
7.1	Project Background & Objectives .....	61
7.2	Details of Existing Setup at CGSDC 1.0 .....	61
7.3	CGSDC 2.0 Project Overview .....	68
7.4	Design Considerations for CGSDC 2.0 .....	71
7.5	Schedule I - Hand Over and Take Over of the Existing IT Infrastructure at the CGSDC .....	74
7.6	Schedule II - Supply, Installation, Configuration, Testing and Commissioning of new hardware, software at CGSDC, Setup of DR on Cloud and Migration to new environment .....	75
7.7	Schedule III – Operations & Maintenance for contract period for IT and Non-IT Infrastructure. ..	90
7.8	Data Centre Certifications .....	98
7.9	OEM Obligations .....	99
7.10	Manpower Deployment .....	99
7.11	Responsibilities of CHIPS .....	103
8.	Implementation Plan, Deliverables, Payment Milestones and Penalties .....	104
9.	Service Level Agreement .....	106
9.1	Data Centre Availability .....	107
9.2	SLA for Availability of IT Infrastructure .....	108
9.3	SLA for Non-IT Infrastructure .....	108
9.4	SLA for Help Desk .....	111
9.5	SLA for Cloud Services .....	112
9.6	SLA for Security and Incident Management .....	115
9.7	Change Management .....	118
9.8	Scheduled Maintenance .....	118
9.9	DC Certifications .....	119
9.10	SLA for Compliance and Reporting: .....	119
9.11	Manpower SLA .....	120

9.12	Service Level Monitoring.....	120
9.13	SLA Change Process .....	121
10.	Annexures .....	122
	Annexure-1: Request for Clarifications/ Pre-bid queries .....	122
	Annexure-2: Proforma for Bank Guarantee for Earnest Money Deposit .....	123
	Annexure-3: Guidelines for E-Procurement.....	124
	Annexure-4: Eligibility Bid Cover Letter (Company Letter head) .....	127
	Annexure-5: Eligibility Bid Compliance Checklist .....	128
	Annexure-6: Certificate for No Conflict-of-Interest Certificate (Company Letter head) .....	131
	Annexure-7: Format for Power of Attorney for Sole MSI.....	132
	Annexure-8: Undertaking on Blacklisting .....	133
	Annexure-9: CV Format .....	134
	Annexure-10: Pre-Contract Integrity Pact .....	135
	Annexure-11: Commercial Bid Cover Letter .....	139
	Annexure-12: Commercial Bid Format.....	141
	Annexure-13: Format for Performance Bank Guarantee.....	156
	Annexure-14: Format for Manufacturer Authorization Letter (on OEM's Letterhead) .....	157
	Annexure-15: Non-Disclosure Agreement (NDA) .....	158
	Annexure -16: Compliance to Technical Specifications on OEM Letterhead.....	161
	Annexure-17: Technical Specifications.....	162
	Annexure-18: Unpriced Bill of Material .....	338
	Annexure-19: Existing Asset Details of Current Infrastructure at CGSDC .....	341

## 1. Notice Inviting Tender

Chhattisgarh infotech Promotion Society (CHiPS), having its Registered Office at SDC Building, 02<sup>nd</sup> Floor, Near Civil Lines Police Control Room, Raipur, Chhattisgarh– 492001, invites responses (“Proposals”/ “Bids”) to this Selection of Master System Integrator (MSI) for CGSDC2.0 in the State of Chhattisgarh.

Interested MSIs are advised to study this RFP carefully before submitting their proposals in response to the RFP. CHiPS shall bear no responsibility and will not accept any justification from MSI post-bid submission on the grounds of misunderstanding or failure to review the RFP.

Submission of a proposal in response to this RFP shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.

Interested MSIs may download the RFP from the website URL mentioned in the Fact Sheet. Any subsequent corrigenda/ clarifications shall also be made available on the website URL mentioned in the fact sheet.

Proposals must be received not later than time and date mentioned in the Fact Sheet. Proposals that are received after the deadline **WILL NOT** be considered in this procurement process.

To obtain first-hand information on the assignment, MSIs are encouraged to attend a pre-bid meeting, carry out site visits. Attending the pre-bid meeting and carrying out site visits are not mandatory.

## 2. Fact Sheet

Tender Issued By	Chhattisgarh infotech Promotion Society (CHIPS)
Name of the Project Work	Selection of Master System Integrator (MSI) for CGSDC2.0 in the State of Chhattisgarh
Tender Reference No./System Tender No.	160662
Place of availability of Tender Documents (RFP)	<a href="https://eproc.cgstate.gov.in">https://eproc.cgstate.gov.in</a> <a href="https://www.chips.gov.in">https://www.chips.gov.in</a>
Tender Document	Request for Proposal
Date of Issue of Tender	28/10/2024
Tender Type (Open/ Limited/ EOI/ Auction/ Single)	Open
Is Offline Submission Allowed (Yes/No)	No
Withdrawal Allowed (Yes/ No)	Yes (on or before the last date and time of bid submission)
Bid Validity days	180 days
Cost of Tender Document	Rupees Five Thousand only (INR 5000/-) To be paid by online through e-Procurement portal ( <a href="https://eproc.cgstate.gov.in">https://eproc.cgstate.gov.in</a> )
Earnest Money Deposit (EMD)	INR 3 Crore/- (Rupees Three Crore only)  EMD may be submitted in the form of Bank Guarantee (BG) in the Name of CEO, CHIPS as per format mentioned in the RFP (Annexure – 02) on stamp paper of value required under law duly signed by authorized representative of Bank:  1) Scan copy of BG should be uploaded in e-Procurement portal along with actual online bid submission. 2) <b>Original copy of BG should be submitted to CHIPS office between 03:00 PM to 05:00 PM on the last date of bid submission</b>
Address to send Pre-bid Queries	The Chief Executive Officer Office of CHIPS, SDC Building, 02nd floor, Near Police Control Room, Civil Lines, Raipur, Chhattisgarh-492001 Phone: 0771-4014158 FAX No: 0771-4066205 Website: <a href="http://www.chips.gov.in">www.chips.gov.in</a> Email: <a href="mailto:ceochips@nic.in">ceochips@nic.in</a>
Nature of Bid Process	Two stage bidding in three envelopes <b>Envelope A</b> 1.1 EMD <b>Envelope B</b> 2.1 Technical Bid <b>Envelope C</b> 3.1 Commercial Bid
Method of Selection	<b>Lowest Cost (L1)</b>
Last Date for Submission of written queries by MSIs	08/11/2024 by 03:00PM (Queries received in writing or email in the format as per Annexure-1, by last date for submission of queries shall be discussed during the pre-bid meeting)
Date of Pre-Bid Meeting	12/11/2024 at 03:00 PM
Place for Pre-bid Meeting	CHIPS, SDC Building, 02nd floor, Near Police Control Room, Civil Lines, Raipur, Chhattisgarh-492001



Last date and time for Submission of Bids	27/11/2024 until 03:00 PM
Last date and time for Submission of Original copy of BG for EMD	Original copy of BG should be submitted to CHiPS office between 03:00 PM to 05:00 PM on the last date of bid submission
Opening of Technical Bids	27/11/2024 at 05:00 PM
Opening of Commercial Bids	To be informed later through e-Procurement Portal or mail and telephone (MSI should furnish the mobile number and e-mail of one authorized representative)
Address for Communication	<p>The Chief Executive Officer  CHiPS, SDC Building, 02nd floor, Near Police Control Room, Civil Lines, Raipur, Chhattisgarh-492001</p> <p>Phone: 0771-4014158  FAX No: 0771-4066205  Website: <a href="http://www.chips.gov.in">www.chips.gov.in</a>  Email: <a href="mailto:ceochips@nic.in">ceochips@nic.in</a></p>

### 3. General

#### 3.1 About CHiPS

CHiPS, a Registered Society promoted by the Government of Chhattisgarh, is the nodal agency and prime mover for propelling IT growth and implementation of IT plans in the State. The Hon'ble Chief Minister heads the High-Powered Governing Council of CHiPS. It involves the Minister for Education, Minister for Panchayat and Rural Development, Minister for Commerce and Industry, Minister for Finance and Commercial Taxes, Chief Secretary, well-known members of IT sectors and a spokesperson from the Ministry of Information Technology of the Government of India.

CHiPS is involved as State Designated Agency (SDA) in NeGP MMP's implementation of some mega IT Projects like CHOICE, Digital Secretariat, GyanVinimay (e-classroom), e-Procurement, SWAN, SSDG, e-District, Bhuiyan, SLCM, Wi-Fi enablement in Government offices, CM Dashboard and advisory services to CM Secretariat and GIS, CSC'S. A professional approach is being adopted for the implementation of IT Projects using the services of e-governance experts and consultants from corporate and academia.

#### 3.2 About Chhattisgarh

Chhattisgarh, a 21st century State, came into being on November 1, 2000. Good Governance is the highest priority in this Fast Track State. There is both policy stability as well as political stability. The government has been kept small and the State is in excellent fiscal health.

Chhattisgarh is truly a land of opportunities. With all major minerals such as coal, iron ore, bauxite in abundance, it is the richest State in mineral resources. There are mega industries in Steel, Aluminium, and Cement.

Chhattisgarh contributes substantially to the Human Resources of India. Female literacy has doubled in the last decade, and male literacy is higher than India's average which is next only to Kerala. Several hundred students from the State qualify for admissions in prestigious academic institutions every year. Bhilai, the knowledge capital of the State, alone sends over 50 students to the elite Indian Institutes of Technology every year.

Large power surplus of Chhattisgarh attracts power-intensive industries, and the State is poised to become the power-hub of the nation. Its central location helps easy power transmission to any part of the country. 12% of India's forests are in Chhattisgarh, and 44% of the State's land area is under forests. Identified as one of the richest biodiversity habitats, the Green State of Chhattisgarh has the densest forests in India, rich wildlife, and above all, over 200 non-timber forest produces, with tremendous potential for value addition.

One-third of Chhattisgarh's population is of tribes, mostly in the thickly forested areas in the North and South. Bastar has known the world over for its unique and distinctive tribal heritage. The Bastar Dussehra is the traditional celebration of the gaiety of tribals. While the central plains of Chhattisgarh are known as the "Rice Bowl" of Central India. Many, unexplored tourism destinations are there in all the parts of Chhattisgarh

#### 3.3 About the project

Chhattisgarh infotech Promotion Society (CHiPS), the nodal agency of Department of Electronics & Information Technology, Government of Chhattisgarh invites technical and financial proposals from reputed MSIs for Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh along with the Operations & Maintenance of CGSDC2.0 as detailed in the Scope of Work in this RFP. The successful MSI will be selected to provide services under this RFP for 5 years period

as per the scope mentioned in this RFP document and may be extended for another 2 years subject to the terms and conditions of this RFP.

## 4. Instructions to MSIs

### 4.1 General

- 4.1.1 While every effort has been made to provide comprehensive and accurate background Information, requirements and specifications, MSIs must form their own conclusions about the services required. MSIs and recipients of this TENDER may wish to consult their own legal advisers in relation to this TENDER.
- 4.1.2 All information supplied by MSIs may be treated as contractually binding on the MSIs, on successful award of the assignment by the CHiPS on the basis of this TENDER.
- 4.1.3 No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the CHiPS. Any notification of preferred MSI status by the CHiPS shall not give rise to any enforceable rights by the MSI. CHiPS may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the CHiPS.
- 4.1.4 This TENDER supersedes and replaces any previous public documentation & Communications, and MSIs should place no reliance on such communications.
- 4.1.5 Please refer Annexure-3 for e-procurement guidelines.

### 4.2 Compliant Tenders/Completeness of Response

- 4.2.1 MSIs are advised to study all instructions, forms, terms, requirements, appendices and other information in the TENDER documents carefully. Online submission of the bid/proposal shall be deemed to have been done after careful study and examination of the TENDER document with full understanding of its implications
- 4.2.2 Prior to evaluation of Bids, CHiPS shall determine whether each Bid is responsive to the requirements of this RFP. A Bid shall be considered responsive if:
  - a) It is received as per the relevant format set out under this RFP;
  - b) It is received by the Bid Due Date including any extension thereof pursuant to the terms of this RFP;
  - c) It is accompanied by the EMD as specified in Clause 4.17;
  - d) It is accompanied by the power(s) of attorney or board resolution
  - e) Consortium of firms are not allowed
  - f) It contains all the information (complete in all respects) as requested in this RFP and/or Bidding Documents (in formats same as those specified);
  - g) It does not contain any condition or qualification limiting or affecting the manner or substance of performance of obligations of the MSI under this RFP, unless specifically required as per the terms of this RFP;
  - h) If a MSI imposes conditions, which is in addition to or in conflict with the conditions mentioned herein, its Bid shall be liable to be summarily rejected. In any case none of such conditions will be deemed to have been accepted unless specifically mentioned in the LOA of the Bid issued by CHiPS;
  - i) It does not contain any suppression of information or facts as required to be furnished by the MSI under this RFP or as may be relevant to be furnished by the MSI in relation to the Project;
  - j) It does not comprise any incomplete information subjective/conditional/contingent/partial offers;
  - k) Is valid for a period of 180 (one hundred and eighty days); and
  - l) It is not non-responsive as per any other terms of this RFP.
- 4.2.3 CHiPS reserves the right to reject any Bid which is non-responsive and no request for alteration, modification, substitution or withdrawal shall be entertained by CHiPS in respect

of such Bid. Provided, however, that CHiPS may, in its discretion, allow the MSI to rectify any infirmities or omissions if the same do not constitute a material modification of the Bid, subject to its written approval and confirmation in this regard.

- 4.2.4 Failure to comply with the requirements of this paragraph may render the Proposal non-compliant and the Proposal may be rejected. MSIs must:
- a. Comply with all requirements asset out within this TENDER.
  - b. Include all supporting documentations specified in this TENDER

#### 4.3 Procedure for Submission of Bids

- 4.3.1 Bids (Technical bid & Commercial bid) shall be submitted online on website <https://eproc.cgstate.gov.in>
- 4.3.2 The participating MSIs in the tender should register themselves on e-procurement portal.
- 4.3.3 The MSIs should scan and upload the respective documentary evidence as mentioned in Eligibility Criteria.
- 4.3.4 The MSIs shall sign on all the statements, documents, certificates uploaded by them, owning responsibility for their correctness/authenticity.
- 4.3.5 The rates should be filled online as well as share as per the commercial bid format (Annexure – 12)

#### 4.4 Other Conditions of Bid Submission

- 4.4.1 After uploading the documents online, Bank Guarantee in original towards the EMD shall be submitted by the MSI in sealed envelope to the CHiPS office as per date & time mentioned in the Section 2 – Fact Sheet. The cover thus prepared should also clearly indicate the name, address, telephone number, E-mail ID and fax number of the MSI to enable the Bid to be returned unopened in case it is declared "Late".
- 4.4.2 Failure to furnish original copy of Bank Guarantee in respect of EMD shall result in rejection of the bid. CHiPS shall not be liable for postal delay. Similarly, if any of the certificates, documents, etc., uploaded by the MSI online are found to be false/fabricated/bogus, the MSI shall be disqualified, blacklisted and action shall be initiated as deemed fit and the Bid Security shall be forfeited.
- 4.4.3 CHiPS shall not hold any risk and responsibility regarding non-clarity / non-legibility of the scanned and uploaded documents.
- 4.4.4 The documents that are uploaded online on the portal shall only be considered for Evaluation of bids.

#### 4.5 Cost to bid

- 4.5.1 The MSI shall bear all costs associated with the preparation and submission of its bid, including cost of presentation for the purposes of clarification of the bid, if so desired by the CHiPS
- 4.5.2 CHiPS shall in no case be responsible or liable for any costs whatsoever, regardless of the conduct or outcome of the Tendering process.

#### 4.6 Contents of RFP

- 4.6.1 The MSI is expected to examine all Sections, Annexures & Corrigenda in the RFP and furnish all information as stipulated therein.

#### 4.7 Clarification on RFP

- 4.7.1 A prospective MSI requiring any clarification on the RFP may submit queries, in writing, at the Purchaser's mailing address and email ID mentioned in Section 2 – Fact Sheet. Queries must be submitted in the format mentioned in Annexure-1.

- 4.7.2 The Purchaser shall not respond to any queries not adhering as per the format mentioned in Annexure-1.
- 4.7.3 All queries on the RFP should be received in Spreadsheet format (.xls) only on or before the last date as mentioned by the Purchaser in Section 2 – Fact Sheet.

#### 4.8 Responses to Pre-Bid Queries and Issue of Corrigendum

- 4.8.1 CHIPS at its sole discretion may provide response to the queries. However, CHIPS makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does CHIPS undertake to answer all the queries that have been posed by the MSIs.
- 4.8.2 At any time prior to the last date for receipt of bids, CHIPS may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective MSI, modify the TENDER Document by a corrigendum.
- 4.8.3 The Corrigendum (if any) & clarifications to the queries from all MSIs will be posted on the CHIPS website [www.chips.gov.in](http://www.chips.gov.in) and CG-e-procurement portal <https://eproc.cgstate.gov.in>.
- 4.8.4 Any such corrigendum shall be deemed to be incorporated into this tender.
- 4.8.5 In order to provide prospective MSIs reasonable time for taking the corrigendum into account, CHIPS may, at its discretion, extend the last date for the receipt of bids.
- 4.8.6 Verbal clarifications and information given by CHIPS or its employees or representatives shall not in any way or manner be binding on CHIPS.

#### 4.9 Amendment of RFP

- 4.9.1 At any time prior to the last date for receipt of bids, the purchaser, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective MSI, modify the RFP by an amendment. The amendment shall be notified on CHIPS website [www.chips.gov.in](http://www.chips.gov.in) and CG-e-procurement portal <https://eproc.cgstate.gov.in> and should be taken into consideration by the prospective agencies while preparing their bids.
- 4.9.2 In order to provide prospective MSIs reasonable time to take the amendment into account to prepare their bids, the Purchaser may, at its discretion, extend the last date for the receipt of bids

#### 4.10 Language of Bids

- 4.10.1 The Bids prepared by the MSI, all correspondence and documents relating to the bids exchanged by the MSI and the Purchaser, shall be written in English language, provided that any printed literature furnished by the MSI may be written in another language so long the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall only govern.

#### 4.11 Documents Comprising the Bids

- 4.11.1 The bid prepared by the MSI shall comprise of the following components:  
Eligibility Bid - The bid shall comprise of the following:
- Annexure-2: Proforma for Bank Guarantee for Earnest Money Deposit
- 4.11.2 Technical Bid - shall comprise of the following:
- Annexure-4: Eligibility Bid Cover Letter (Company Letter head)
  - Annexure-5: Eligibility Bid Compliance Checklist with all supporting documents required for eligibility
  - Annexure-6: Certificate for No Conflict of Interest

- d. Annexure-7: Power of Attorney executed in favour of the Authorized Signatory OR Board Resolution in granting the requisite authority in favour of the person granting power of attorney to the authorized signatory
- e. Annexure-8: Undertaking on Blacklisting
- f. Annexure-9: CV Formats
- g. Annexure-10: Pre-Contract Integrity Pact
- h. Annexure 14: MAF Undertaking on OEM Letterhead
- i. Annexure 15: Non-Disclosure Agreement
- j. Annexure 16: Compliance to Technical Specifications on Respective OEM Letterhead
- k. Annexure 17: Technical Specifications
- l. Annexure 18: Unpriced BOM

- 4.11.3 Commercial Bid - The Commercial Bid shall comprise of the following:
- a. Annexure-11: Commercial Bid Cover Letter (Company Letter head)
  - b. Annexure-12: Commercial Bid Format

#### 4.12 Procedure for Submission of Bids

- 4.12.1 The bid prepared by the MSI shall comprise of the following cover (to be uploaded at e-procurement portal as individual files):

4.12.2 **Envelope A (EMD Bid)**

- a. Envelope / File – I: shall comprise of all the documents (in PDF format):
  - i. Scanned copy of EMD in the form of ‘Refundable & Irrevocable Bank Guarantee’
  - ii. Documents mentioned in Clause 4.11.1
- b. MSI shall upload these documents on or before the last date of bid submission as mentioned in Section 2 – Fact Sheet
- c. MSI shall submit original copy of EMD in the form of Refundable & Irrevocable Bank Guarantee’, on or before the last date of bid submission as mentioned in Section 2 – Fact Sheet. The address of CHiPS, name and address of the MSI and the Tender Reference Number shall be marked on the envelope. The envelope shall also be marked with a sentence “NOT TO BE OPENED BEFORE the Date and Time of Bid Opening”. If the envelope is not marked as specified above, CHiPS shall not assume any responsibility for its misplacement, pre-mature opening etc.

4.12.3 **Envelope B (Technical Bid)**

- a. Envelope B shall comprise of all the documents (in PDF format) mentioned in Clause 4.11.2 and uploaded on the e-proc portal

4.12.4 **Envelope C (Commercial Bid)**

- a. **Envelope / File - III** shall comprise of all the documents (in PDF format) mentioned in Clause 4.11.3 and uploaded on the e-proc portal
- b. All prices under the Commercial Bid should be in Indian National Rupee (INR) and should comply with all the rules and regulation of RBI, and the relevant Government instrumentality at their own cost. In the event of any discrepancy between the Commercial Bid quoted in words and in figures, words shall prevail.
- c. CHiPS may at its sole discretion and in accordance with the terms of this RFP, declare the MSI quoting the lowest Price Bid as the lowest MSI (“L1 MSI”). CHiPS shall not be responsible for any erroneous calculation of Taxes. Any upward/downward revision of GST shall be applicable at the time of invoicing. However, to arrive at the bid value of the respective Bid, MSI has to quote the charges inclusive of all taxes, duties, levies etc. excluding GST. The Commercial Bid shall be inclusive of all freight, forwarding, transit insurance and installation charges.

- d. The price quoted by the MSI inclusive of all taxes, duties, levies etc. as per the commercial format shall be considered for deciding the L1 price
- e. In the event of any difference between figures and words, the amount indicated in words in the Price Bid shall be taken into account.

***Note: Prices should not be indicated/ mentioned in the Technical Bid but should only be mentioned in the Commercial Bid. Any bids received with the prices / commercial details in any form apart from the Commercial bid shall be rejected***

The MSI shall submit only one (1) bid in response to the RFP. If the MSI submits more than one bid, it shall lead to disqualification of MSI and shall also cause the rejection of all the bids which such MSI has submitted.

#### 4.13 Bid Prices

- 4.13.1 The MSI shall indicate in the format prescribed, the unit rates and total Bid Price of the equipment / services, it proposes to provide under the Contract. Prices shall be filled online as per template provided on e-procurement portal (indicative BOM and relative calculations are in Annexure-12: Commercial Bid Format)
- 4.13.2 In absence of information requested in above Clause, a bid may be considered incomplete and be summarily rejected
- 4.13.3 The MSI shall prepare the bid based on details provided in the RFP. It must be clearly understood that the Scope of Work is intended to give the MSI an idea about the order and magnitude of the work and is not in any way exhaustive and guaranteed by the Purchaser. The MSI shall carry out all the tasks in accordance with the requirement of the RFP and it shall be the responsibility of the MSI to fully meet all the requirements of the RFP.

#### 4.14 Firm Prices

- 4.14.1 Prices quoted in the bid must be firm and final and shall not be subject to any upward modifications, on any account whatsoever. However, the Purchaser reserves the right to negotiate the prices quoted by the MSI to effect downward modification. The Bid Prices shall be indicated in Indian Rupees (INR) only.
- 4.14.2 The Commercial bid should clearly indicate the price to be charged and the applicable Taxes as per actuals. It is mandatory that such charges wherever applicable/ payable should be indicated separately. However, should there be a change in the upward or downward revision in GST, the same shall apply.

#### 4.15 Discount

- 4.15.1 The MSIs are advised not to indicate any separate discount in the Commercial Bid. Discount, if any, should be merged with the quoted prices. Discount of any type, indicated separately, shall not be taken into account for evaluation purpose. However, in the event of such an offer is found to be the lowest without taking into account the discount, the Purchaser shall avail such discount at the time of award of Contract.

#### 4.16 MSI Qualification

- 4.16.1 The "MSI" as used in the RFP shall mean the one who has signed the Tender Form. The MSI may be either the Principal Officer or his duly Authorized Representative, in either case, he/ she shall submit a certificate of authority. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall be furnished and signed by the authorized representative and the Principal Officer.
- 4.16.2 It is further clarified that the individual signing the tender or other documents in connection with the tender must certify whether he/ she signs as the Constituted attorney of the firm, or a company



- 4.16.3 The authorization shall be indicated by written Power-of-Attorney accompanying the bid
- 4.16.4 The power or authorization and any other document consisting of adequate proof of the ability of the signatory to bind the MSI shall be annexed to the bid
- 4.16.5 Any change in the Principal Officer or his duly Authorized Representative shall be intimated to CHiPS in advance

#### 4.17 Earnest Money Deposit (EMD)

- 4.17.1 The MSI shall furnish, as part of its bid, an Earnest Money Deposit (EMD) of the amount mentioned in the Section 2 – Fact Sheet
- 4.17.2 The EMD is required to protect the Purchaser against the risk of MSI's conduct which would warrant the security's forfeiture, pursuant to Section 7 – Scope of Work
- 4.17.3 The EMD must be submitted, by Bank Guarantee of any Scheduled Commercial Bank/ Nationalized Bank drawn in favour of CHiPS, payable at Raipur.
- 4.17.4 The EMD of unsuccessful MSIs shall be discharged/ returned within 60 days of award of Contract to the successful MSI.
- 4.17.5 The EMD of successful MSI shall be discharged/returned upon the MSI executing the Contract, pursuant to Clause 4.32: Award of Contract and furnishing the Bank Guarantee/Security Deposit, pursuant to Clause 4.37: Performance Bank Guarantee and Advance Bank Guarantee.
- 4.17.6 CHiPS may, in its sole discretion and at the Successful MSI's option, adjust the amount of EMD in the amount of PBG to be provided by him in accordance with the provisions of the Agreement.
- 4.17.7 CHiPS shall be entitled to forfeit and appropriate the EMD as damages inter alia in any of the events specified in Clause 4.17.8 and Clause 4.17.10 herein. The MSI, by submitting its Bid pursuant to this RFP, shall be deemed to have acknowledged and confirmed that CHiPS will suffer loss and Damages on account of withdrawal of its Bid or for any other default by the MSI during the period of validity of the Bid as specified in this RFP. No relaxation of any kind on EMD shall be given to any MSI.
- 4.17.8 The EMD shall be forfeited as Damages without prejudice to any other right or remedy that may be available to CHiPS under the Bidding Documents and/ or under the Agreement, or otherwise, if:
  - a. MSI submits a non-responsive Bid;
  - b. MSI engages in a corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice as specified in Clause 4.39 of this RFP;
  - c. MSI withdraws its Bid during the period of Bid validity as specified in this RFP and as extended by mutual consent of the respective MSI(s) and CHiPS; and
  - d. the Successful MSI fails within the specified time limit:
    - i. to sign and return the duplicate copy of LOA; or
    - ii. to execute the Agreement; or
    - iii. to furnish the PBG within the period prescribed therefore in the Agreement.
    - iv. the Successful MSI, having executed the Agreement, commits any breach thereof prior to furnishing the PBG.
- 4.17.9 No interest shall be paid by the Purchaser on the EMD
- 4.17.10 The EMD may be forfeited:
  - a. if a MSI withdraws its bid during the period of bid validity specified by the MSI in the Bid; or
  - b. In case the successful MSI fails;



- i. to sign the Contract in accordance with Clause 4.32 : Award of Contract;  
or
- ii. to furnish Performance Bank Guarantee in accordance with Clause 4.37: Performance Bank Guarantee

#### 4.18 Period of Validity of Bids

- 4.18.1 Bids shall have validity period as mentioned in Section 2 - Fact Sheet after the date of opening of Technical Bid. A bid valid for a shorter period may be summarily rejected by the Purchaser as non-responsive.
- 4.18.2 Prior to the expiry of the validity of the period of validity of the bids, the Purchaser may request the MSI(s) for an extension of the period of validity up to 180 days or more. The request and the responses thereto shall be made in writing (or through e-mail). The period of validity of their Bids shall require extension in the period of validity of EMD submitted by the MSIs or submission of new EMD to cover the extended period of validity of their Bids. A MSI whose EMD is not extended, or that has not submitted a new EMD, shall be considered to have refused the request to extend the period of validity of its Bid.

#### 4.19 Format and Signing of Bid

- 4.19.1 The original bid documents shall be typed or written in indelible ink and signed by the MSI or an authorized representative empowered to bind the MSI to the Contract. Every page of the bid, except for un-amended printed literature, must be initialled and stamped by the MSI or the authorised representative of the MSI signing the bid.
- 4.19.2 The response to the bid should be submitted along with legible, appropriately indexed, duly filled Information sheets and sufficient documentary evidence as per Checklist. Responses with illegible, incomplete Information sheets or insufficient documentary evidence shall be rejected.
- 4.19.3 The bid shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the MSI, in which case such corrections shall be initialled by the person(s) signing the bid
- 4.19.4 The MSI shall duly sign and seal its bid with the exact name of the firm/company to whom the contract is to be issued.

#### 4.20 Revelation of Prices

- 4.20.1 Prices in any form or by any reason before opening the Commercial Bid should not be revealed, failing which the offer shall be liable to be rejected

#### 4.21 Terms and Conditions of MSIs

- 4.21.1 Any terms and conditions of the MSIs shall not be considered as forming part of their Bids

#### 4.22 Consortium

- 4.22.1 Consortium is not allowed for this assignment

#### 4.23 Local Conditions

- 4.23.1 It shall be incumbent upon each MSI to fully acquaint himself with the local conditions and other relevant factors at the proposed site which would have any effect on the performance of the contract and / or the cost.
- 4.23.2 The MSI is expected to make a site visit to obtain for himself on his own responsibility, all information that may be necessary for preparing the bid and entering into contract. Obtaining such information shall be at MSI's own cost.

- 4.23.3 Failure to obtain the information necessary for preparing the bids and/or failure to perform the activities that may be necessary for the providing services before entering into contract shall in no way relieve the MSI from performing any work in accordance with the RFP
- 4.23.4 It shall be imperative for each MSI to fully inform themselves of all legal conditions and factors which may have any effect on the execution of the contract as described in the bidding documents.
- 4.23.5 It is the responsibility of the MSI that such factors have properly been investigated and considered while submitting the bid proposals and that no claim whatsoever including those for financial adjustment to the contract awarded under the bidding documents shall be entertained by the Purchaser and that neither any change in the time schedule of the contract nor any financial adjustments arising thereof shall be permitted by the Purchaser on account of failure of the MSI to appraise themselves of local laws and site conditions
- 4.23.6 It shall be deemed that by submitting a Bid, the MSI has:
  - a. made a complete and careful examination of the Bidding Documents;
  - b. received all relevant information requested from CHiPS;
  - c. accepted the risk of inadequacy, error or mistake in the information provided in the Bidding Documents or furnished by or on behalf of CHiPS relating to any of the matters

#### 4.24 Last Date for Receipt of Bids

- 4.24.1 Bids shall be submitted by the MSI no later than the time and date specified in Section 2 – Fact Sheet
- 4.24.2 The Purchaser may, at its discretion, extend the last date for submission of bids by amending the RFP, in which case all rights and obligations of the Purchaser and MSIs previously subject to the last date shall thereafter be subject to the last date as extended

#### 4.25 Late Bids

- 4.25.1 Any bid submitted by the MSI after the last date and time for submission of bids pursuant to Section 2 – Fact Sheet, shall be rejected

#### 4.26 Modification and Withdrawal of Bids

- 4.26.1 No bid may be altered/ modified subsequent to the closing time and date for receipt of bids. Unsolicited correspondences from MSIs shall not be considered.
- 4.26.2 No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified by the MSI in the Bid. Withdrawal of a bid during this interval may result in the MSI's forfeiture of its EMD and shall be declared a "defaulting MSI". In such situation the tendering process shall be continued with the remaining MSIs as per their ranking.
- 4.26.3 If the MSI relents after being declared as selected MSI, it shall be declared as defaulting MSI and EMD of such defaulting MSI shall be forfeited and CHiPS reserves right to blacklist/ debarred such MSI for next 3 years from participating in any CHiPS tender. In such situation, L2 MSI shall be invited to match the prices of L1 MSI. However, in-case of refusal of acceptance by the L2 MSI to match the price of L1 MSI, CHiPS would carry out discussions with the subsequent MSIs

#### 4.27 Contacting the Purchaser

- 4.27.1 No MSI shall contact the Purchaser on any matter relating to its bid, from the time of the bid submission to the time the Contract is awarded
- 4.27.2 Any effort by a MSI to influence the Purchaser's bid evaluation, bid comparison or Contract award decisions may result in the rejection of the MSI's bid

#### 4.28 Opening of Technical Bids by Purchaser

- 4.28.1 The Bids received from the MSIs shall be opened online. The opening of the Bids shall be carried out online in the physical presence of the designated representatives of CHiPS and the MSIs. However, this RFP does not mandate the physical presence of the MSIs. The absence of the physical presence of the MSIs shall in no way affect the outcome of the evaluation of the Bids.
- 4.28.2 CHiPS shall subsequently examine and evaluate the Bids in accordance with the provisions set out in this RFP.
- 4.28.3 To facilitate evaluation of Bids, CHiPS may, at its sole discretion, seek clarifications in writing from any MSI regarding its Bid.

#### 4.29 Purchaser's Right to Vary Scope of Contract

- 4.29.1 The quantity of goods works or services originally specified in the bidding documents is indicative, actual quantity will depend upon the design, solution proposed by the MSI.
- 4.29.2 If the Purchaser does not procure any subject matter of procurement or procures less than the quantity specified in the bidding documents due to change in circumstances, the bidder shall not be entitled for any claim or compensation except otherwise provided in the bidding document.
- 4.29.3 The purchaser may at any time increase or decrease the quantity through a written communication to the MSI and MSI is bound to honour the same.

#### 4.30 Purchaser's Right to Accept Any Bid & to Reject Any or All Bids

- 4.30.1 The Purchaser reserves the right to accept any or all bid, and to annul the Tendering process or reject all bids at any time prior to award of Contract or if the bidder fails to comply with any of the conditions as per Clause 4.2.2 and 4.36 of this RFP, without thereby incurring any liability to the affected MSI or MSIs or any obligation to inform the affected MSI or MSIs of the grounds for the Purchaser's action
- 4.30.2 Further, in the event that the RFP has been terminated on account of any default of the MSI/Successful MSI, CHiPS reserves the right to encash the EMD and/or PBG to the extent required to make good the losses suffered by it on account of such default having been committed by the MSI.
- 4.30.3 This RFP does not constitute an offer by CHiPS. The MSI's participation in the Bidding Process may result CHiPS selecting the MSI to engage towards execution of the Scope of Work of the Project.

#### 4.31 Notification of Award

- 4.31.1 Prior to the expiry of the period of bid validity, pursuant to Section 2- Fact Sheet and Clause 4.18: Period of Validity of Bid, the Purchaser shall notify the successful MSI in writing by registered letter/ courier, that its bid has been accepted
- 4.31.2 The notification of award shall constitute the formation of the Contract
- 4.31.3 Upon furnishing of Performance Bank Guarantee of 10% of the CAPEX value by MSI, the Purchaser may notify successful MSI and shall discharge/return its EMD.

#### 4.32 Award of Contract

- 4.32.1 There shall be only one successful MSI
- 4.32.2 At the same time as the Purchaser notifies the MSI that its bid has been accepted, the Purchaser shall send the MSI the pro forma for Contract, incorporating all agreements between the parties

- 4.32.3 Within 7 days of receipt of the Contract, the MSI shall sign and date the Contract and return it to the Purchaser
- 4.32.4 Contract duration will be of 5 years of which implementation period is 9 months and O&M period is 4.3 years (i.e. 17 Quarters). The MSI whose bids is accepted shall be required to submit Performance Bank Guarantee as mentioned in the Clause: 4.37 along with acceptance of work order, within 15 days of the receipt of notification of award from the Purchaser. PBG shall be in the form of Bank Guarantee (BG) from any nationalized or scheduled bank as per Annexure-13.
- 4.32.5 MSI has to agree for honouring all RFP conditions and adherence to all aspects of fair-trade practices in executing the work orders placed by CHiPS
- 4.32.6 If the name of the system/ service/ process is changed for describing substantially the same in a renamed form; then all techno-fiscal benefits agreed with respect to the original product, shall be passed on to CHiPS and the obligations with CHiPS taken by the Vendor with respect to the product with the old name shall be passed on along with the product so renamed
- 4.32.7 CHiPS may, at any time, terminate the contract by giving written notice to the MSI without any compensation, if the MSI becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to CHiPS.
- 4.32.8 If at any point during the Contract, the MSI fails to deliver as per the RFP terms and conditions or any other reason amounting to disruption in service, the Termination and Exit Management clause shall be invoked.

#### 4.33 Annulment & Re-award

- 4.33.1 Failure of the Successful MSI to comply with all the requirements shall constitute sufficient grounds for the annulment of the award of the Agreement, in which event CHiPS may make the award to the next lowest evaluated MSI or call for new bids.

#### 4.34 Placing of Work Order

- 4.34.1 Quantities mentioned in **Annexure-12: Commercial Bid Format** are indicative, and CHiPS reserves the right at the time of issuance of work order to increase or decrease the quantity of goods and / or services from the original requirements as specified in the terms & conditions of the RFP
- 4.34.2 For procurement of Hardware/service, Work Order shall be placed to MSI
- 4.34.3 Objection, if any, to the Work Order must be reported to CHiPS by the MSI within five (5) working days counted from the Date of issuance of work Order for modifications, otherwise it is assumed that the MSI has accepted the Work Order
- 4.34.4 If the MSI is not able to do the complete work as mentioned in the scope of work within the specified period, the penalty clause shall be invoked
- 4.34.5 The decision of CHiPS shall be final and binding on the MSI. CHiPS reserve the right to accept or reject an offer without assigning any reason whatsoever

#### 4.35 Tender Related Conditions

- 4.35.1 The MSI shall confirm unconditional acceptance of full responsibility of completion of job and for executing the 'Scope of Work' of this RFP. This confirmation should be submitted as part of the Technical Bid. The MSI shall also be the sole point of contact for all purposes of the Contract.
- 4.35.2 The MSI should not be involved in any litigation that may have an impact of affecting or compromising the delivery of services as required under this Contract. If at any stage of Tendering process or during the term of the contract, any suppression/ falsification of such information is brought to the knowledge of the Purchaser, the Purchaser shall have

the right to reject the bid or terminate the Contract, as the case may be, without any compensation to the MSI.

#### 4.36 Rejection Criteria

4.36.1 Besides other conditions and terms highlighted in the RFP, bids may be rejected under following circumstances:

- a. Technical Rejection Criteria
  - i. Bids submitted without or improper EMD
  - ii. Technical Bid containing commercial details
  - iii. Bids received through Telex/ Telegraphic/ Fax/ E-Mail/ post etc. except, wherever required, shall not be considered for evaluation
  - iv. Bids which do not confirm unconditional validity of the bid as prescribed in the RFP
  - v. If the information provided by the MSI is found to be incorrect/ misleading at any stage/ time during the Tendering Process
  - vi. Any effort on the part of a MSI to influence the Purchaser's bid evaluation, bid comparison or Contract award decisions
  - vii. Bids submitted by the MSI after the last date and time of bid submission prescribed by the Purchaser, pursuant to Section 2 – Fact Sheet
  - viii. Bids without power of authorization and any other document consisting of adequate proof of the ability of the signatory to bind the MSI
  - ix. Failure to furnish all information required by the RFP or submission of a bid not substantially responsive to the RFP in every respect
  - x. MSIs not quoting for the complete Scope of Work as indicated in the RFP, addendum (if any) and any subsequent information given to the MSIs
  - xi. MSIs not complying with the functionality, specifications and other Terms and Conditions as stated in the RFP
  - xii. The MSI not conforming unconditional acceptance of full responsibility of providing Goods and Services in accordance with the Section 5: General Conditions of Contract and Section 7: Scope of Work
  - xiii. If the bid does not conform to the timelines indicated in this RFP
- xiv. Commercial Rejection Criteria
  - xv. Incomplete Commercial Bid
  - xvi. Commercial Bids that do not conform to this RFP's Commercial Bid format
  - xvii. If there is an arithmetic discrepancy in the commercial bid calculations, the Purchaser shall rectify the same. If the MSI does not accept the correction of the errors, bid may be rejected.

4.36.2 If MSI quotes NIL charges/ consideration, the bid shall be treated as unresponsive and shall not be considered

#### 4.37 Performance Bank Guarantee and Advance Bank Guarantee

4.37.1 Within 15 days of the receipt of notification of award from the Purchaser, the successful MSI shall be required to submit a **CAPEX Performance Bank Guarantee (PBG)** of 10% of the CAPEX value of the contract and should be valid up to 60 days after successful Project Go-Live. PBG shall be in the form of Bank Guarantee (BG) from any nationalized or scheduled bank.

4.37.2 If required, MSI may request Mobilisation advance of 10% of the CAPEX cost after signing the contract and submission of CAPEX PBG as per Clause 4.37.1 above. In such case, MSI shall submit an Advance Bank Guarantee of 110% of the value of mobilisation advance and which should be kept valid up to 60 days after successful Project Go-Live.

4.37.3 The PBG of the CAPEX and Advance Bank Guarantee shall be returned to MSI upon Successful Project Go-live and against the submission of **O&M PBG** amounting to 10% of the OPEX value of the contract and should be valid up to 60 days beyond completion of O&M period, which is 4.3 years, i.e.~17 quarters. The PBG of OPEX shall be returned

to MSI upon successful completion of Hand Over-Take Over (HOTO) to the New MSI / CHiPS.

- 4.37.4 The above PBG should be in accordance to General Conditions of the Contract, in the prescribed contract format as per the Annexure-13: Format for Performance Bank Guarantee.
- 4.37.5 Failure of the MSI to comply with the requirement of Clause 4.33 shall constitute sufficient grounds for the annulment of the contract and forfeiture of the EMD.

#### 4.38 Fraud and Corrupt Practices

- 4.38.1 The MSI and their respective officers, employees, agents and advisers shall observe the highest standards of ethics during the Bidding Process and subsequent to the issue of the Award of Work and during the subsistence of the Contract. Notwithstanding anything to the contrary contained herein, or in the Award of Work or the Contract, the Purchaser shall reject a Bid, withdraw the Award of Work, or terminate the Contract, as the case may be, without being liable in any manner whatsoever to the MSI as the case may be, if it determines that the MSI, as the case may be, has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice in the Bidding Process. In such an event, the Purchaser shall forfeit and appropriate the Bid Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the Purchaser towards, inter alia, time, cost and effort of the Purchaser, without prejudice to any other right or remedy that may be available to the Authority hereunder or otherwise.
- 4.38.2 Without prejudice to the rights of the Purchaser under Clause 4.35.1 hereinabove and the rights and remedies which the Purchaser may have under the Award of Work or the Contract, if a MSI, as the case may be, is found by the Authority to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Bidding Process, or after the issue of the Award of Work or the execution of the Contract, such MSI shall not be eligible to participate in any RFP issued by the Purchaser during a period of 2 (two) years from the date such MSI, as the case may be, is found by the Purchaser to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practices, as the case may be.
- 4.38.3 For the purposes of the Clause 4.39.1, the following terms shall have the meaning hereinafter respectively assigned to them:
  - a. "corrupt practice" means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the actions of any person connected with the Bidding Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the Authority who is or has been associated in any manner, directly or indirectly, with the Bidding Process or the Work Order or has dealt with matters concerning the Contract or arising therefrom, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the Authority, shall be deemed to constitute influencing the actions of a person connected with the Bidding Process); or (ii) save, engaging in any manner whatsoever, whether during the Bidding Process or after the issue of the Work Order or after the execution of the Contract, as the case may be, any person in respect of any matter relating to the Project or the Work Order



- or the Contract, who at any time has been or is a legal, financial or technical adviser of the Purchaser in relation to any matter concerning the Project;
- b. "Fraudulent practice" means a misrepresentation or omission of facts or suppression of facts or disclosure of incomplete facts, in order to influence the Bidding Process.
  - c. "Coercive practice" means impairing or harming, or threatening to impair or harm, directly or indirectly, any person or property to influence any person's participation or action in the Bidding Process.
  - d. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by the Authority with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Bidding Process; or (ii) having a Conflict of Interest; and
  - e. "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among MSI with the objective of restricting or manipulating a full and fair competition in the Bidding Process

#### 4.39 Disqualification of the MSI

- 4.39.1 MSI shall be liable for disqualification and forfeiture of the EMD submitted by it, if any legal, financial or technical adviser of CHiPS in relation to the Project is engaged by the MSI, its members or any Associate thereof, as the case may be, in any manner for matters related to or incidental to such Project during the Bidding Process or subsequent to the (i) issuance of the LOA or (ii) execution of the Agreement.
- 4.39.2 In the event any such adviser is engaged by the Successful MSI or the Contractor, as the case may be, after issuance of the LOA or execution of the Agreement for matters related or incidental to the Project, then notwithstanding anything to the contrary contained herein or in the LOA or the Agreement and without prejudice to any other right or remedy of CHiPS, including the forfeiture and appropriation of the EMD or PBG, as the case may be, the LOA and/or the Agreement shall be liable to be terminated without CHiPS being liable in any manner whatsoever to the Successful MSI or Contractor for the same.
- 4.39.3 For the avoidance of doubt, this disqualification shall not apply where such adviser was engaged by the MSI, its member or Associate in the past but its assignment expired or was terminated prior to the Bid Due Date. Nor will this disqualification apply where such adviser is engaged after a period of 3 (three) years from the date of completion of Scope of Work of the Project.

#### 4.40 Verification and Disqualification

- 4.40.1 CHiPS reserve the right to verify all statements, information and documents submitted by the MSI in response to the Bidding Documents and the MSI shall, when so required by CHiPS, make available all such information, evidence and documents as may be necessary for such verification. Any such verification, or lack of such verification, by CHiPS shall not relieve the MSI of its obligations or liabilities hereunder nor will it affect any rights of CHiPS hereunder.
- 4.40.2 CHiPS reserve the right to reject any Bid and appropriate the EMD if:
  - a. at any time, a material misrepresentation is made or uncovered, or
  - b. L1 expresses its desire to or does withdraw its Bid, or
  - c. The MSI does not provide, within the time specified by CHiPS, the supplemental information sought by CHiPS for evaluation of the Bid within a reasonable time as determined by CHiPS in its sole discretion.
- 4.40.3 Such misrepresentation/ improper response/intent to withdraw shall lead to the disqualification of the MSI. If such disqualification/rejection occurs after the Bids have been opened and the L1 MSI gets disqualified/rejected, then CHiPS reserve the right to:
  - a. invite the remaining MSIs to submit fresh Bids in accordance with this RFP; or
  - approach the next lowest MSI (L2) for matching the price of L1. Should L2 choose

to match the price bid of L1, CHiPS may issue the LOA to L2. However, in-case of refusal of acceptance by the L2 MSI to match the price of L1 MSI, CHiPS would carry out discussions with the subsequent MSIs take any such measure as may be deemed fit in the sole discretion of CHiPS, including annulment of the Bidding Process.

- 4.40.4 In case it is found during the evaluation or at any time before signing of the Agreement or after its execution and during the period of subsistence thereof, that one or more of the qualification conditions have not been met by the Successful MSI/Bidder (as may be the case), or the MSI has made material misrepresentation or has given any materially incorrect or false information, the Successful MSI/Bidder may be, without CHiPS being liable in any manner whatsoever to the Successful MSI or Contractor - In such an event, CHiPS shall be entitled to forfeit and appropriate the EMD or PBG, as the case may be as Damages, without prejudice to any other right or remedy that may be available to CHiPS under the Bidding Documents and/ or the Agreement, or otherwise.
- 4.40.5 MSIs are advised to study all instructions, forms, terms, requirements, appendices and other information in the RFP carefully. Online submission of the Bid shall be deemed to have been done after careful study and examination of the RFP with full understanding of its implications and failure to comply with the requirements of the RFP, in addition to submission of all the documents as required hereunder, may render the Bid non-compliant and the same may be rejected

## 5. General Conditions of the Contract

### 5.1 Definitions

#### 5.1.1 In this RFP, unless the context otherwise requires

- a. "Applicable Laws" includes all applicable statutes, enactments, acts of legislature or laws, ordinances, rules, by-laws, regulations, notifications, guidelines, policies, directions, directives, requirement or other governmental restriction and orders or judgements of any Governmental authority, tribunal, board, court or other quasi-judicial authority or other governmental restriction or any similar form of decision applicable to the relevant Party and as may be in effect on the date of execution of Agreement and during the subsistence thereof, applicable to the Project
- b. Bid Validity Period: The period during which a bidder is required to maintain the validity of their proposal without any changes. During this time, the bidder is expected to honour the terms, conditions, and prices proposed in their bid.
- c. "Confidential Information" means all information as defined in Section 5 - General Conditions of the Contract
- d. "Contract" means the Agreement entered between the MSI and the Purchaser as recorded in the Contract form signed by the Purchaser and the MSI including all attachments and Annexes thereto, the RFP and all Annexes thereto and the agreed terms as set out in the bid, all documents incorporated by reference therein and amendments and modifications to the above from time to time.
- e. "Contract Value" means the price payable to the MSI under this Contract for the full and proper performance of its contractual obligations
- f. "Deliverables" means the products, infrastructure, licenses and services agreed to be delivered by the MSI in pursuance of the Contract as elaborated in the RFP and includes all documents related to the user manual, technical manual, designs, process documentations, the artefacts, the training materials, process and operating manuals, service mechanisms, policies and guidelines, inter alia payment and/or process related etc. and all their respective modifications.
- g. "Effective Date" means the date on which the Contract is executed by both the Parties



- h. "End-to-End Solution" means Complete upgradation, Installation, Integration, Commissioning and Testing of the equipment of SDC.
- i. "OEM" or "Original Equipment Manufacturer" means the original manufacturer and owner of the Intellectual Property Rights of any Software or Equipment to be used in the Project and to which CHiPS has been granted license to use
- j. "Contract Performance Guarantee" or "Performance Bank Guarantee" shall mean the guarantee provided by a Scheduled Commercial Bank/ Nationalized Bank to CHiPS by the successful MSI
- k. "Project" means Upgrade of CGSDC Project for Design, Supply, Installation, Integration, Testing, Commissioning of entire setup.
- l. "Project Go-Live" shall refer to the successful commissioning of the project, following the completion of all Data Centre components, encompassing IT, Non-IT and Civil works, as delineated in the Scope of Work outlined in the Request for Proposal (RFP). This milestone signifies that all upgraded or replaced systems, hardware, and infrastructure are fully operational, integrated, and seamlessly functioning within the existing environment, including the successful migration of data and services to the new systems and successful setup and operations of Network Operations Centre and Helpdesk. Go-Live is considered successful once Go-Live certificate is issued by CHiPS or their appointed Third-Party Agency.
- m. "Purchaser" means Chhattisgarh infotech Promotion Society (CHiPS)
- n. "Purchaser's Representative" or "Purchaser's Technical Representative" means the person or the persons appointed by the Purchaser from time to time to act on its behalf for overall co-ordination, supervision, and project management
- o. "Project Implementing Agency is also termed as Master System Integrator (MSI)" means the successful MSI whose bid has been accepted by the Purchaser and with whom the order for "Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh" has been placed as per requirements and terms & conditions specified in this RFP and shall be deemed to include the MSI's successors, representatives (approved by the Purchaser), heirs, executors, administrators and permitted assigns, as the case may be, unless excluded by the terms of the contract
- p. "MSIs' Team" means the MSI along with all its partners / OEMs, who have to provide goods & services to the Purchaser under the scope of this RFP / Contract. This definition shall also include any authorized service providers/partners/agents and representatives, or other personnel employed or engaged either directly or indirectly by the MSI for the purposes of this MSI / Contract
- q. Non-responsive Bid: A bid that does not comply with the mandatory requirements outlined in the Request for Proposal (RFP). A non-responsive bid may be missing required information, fail to meet the specifications, or not adhere to the submission guidelines, leading to its disqualification from the evaluation process.
- r. "Request for Proposal/ (RFP)" means the documents containing the general, technical, functional, commercial and legal specifications for the implementation of this Project including different Annexures and includes the clarifications, explanations, minutes of the meetings, corrigendum(s) and amendment(s) issued from time to time during the bidding process and on the basis of which MSI has submitted its Proposal
- s. "Schedule of Requirements" or "SoR" means the requirement regarding the Project provided by MSI in its bid, stating the prices and the quantity of the materials to be procured by the MSI (on behalf of CHiPS)
- t. "State Level Committee" means a committee involving representatives of the Purchaser and senior officials of the MSI shall be formed for the purpose of this Contract. This committee shall meet at intervals, as decided by the Purchaser later, to oversee the progress of the Project

- u. "Successful MSI" means MSI that is selected as the winning bidder after a competitive bidding process. This entity has satisfactorily met all the specified requirements and evaluation criteria set forth in the RFP documentation and is selected for CGSDC2.0 Project in the State of Chhattisgarh
- v. "Tender" or "Tender Document" means RFP
- w. "Timelines" means the duration of the contract as described in the RFP
- x. "Working Day" means any day on which any of the office of CHiPS shall be functioning, including gazetted holidays, restricted holidays or other holidays, Saturdays and Sundays

## 5.2 Interpretations

### 5.2.1 In this RFP, unless otherwise specified:

- a. Unless otherwise specified, a reference to clauses, sub-clauses, or Section is a reference to clauses, sub-clauses, or Section of this RFP including any amendments or modifications to the same from time to time
- b. Words denoting the singular include the plural and vice versa and use of any gender includes the other genders
- c. References to a "company" shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established
- d. Words denoting to a "person" shall be construed to include any individual, partnerships, firms, companies, public sector units, corporations, joint ventures, trusts, associations, organizations, executors, administrators, successors, agents, substitutes and any permitted assignees or other entities (whether or not having a separate legal entity). A reference to a group of persons is a reference to all of them collectively, to any two or more of them collectively and to each of them individually
- e. A reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted
- f. Any reference to a "day" (including within the phrase "business day") shall mean a period of 24 hours running from midnight to midnight
- g. References to a "business day" shall be construed as a reference to a day (other than a Sunday) on which CHiPS office is generally open for business
- h. References to times are to Indian Standard Time
- i. Reference to any other document referred to in this RFP is a reference to that other document as amended, varied, novated or supplemented at any time
- j. All headings and titles are inserted for convenience only, they are to be ignored in the interpretation of this Contract
- k. Unless otherwise expressly stated, the words "herein", "hereof", "hereunder" and similar words refer to this RFP as a whole and not to any particular Section or Annexure and the words "include" and "including" shall not be construed as terms of limitation
- l. The words "in writing" and "written" mean "in documented form", whether electronic or hard copy, unless otherwise stated
- m. Any reference at any time to any agreement, deed, instrument, license or document of any description shall be construed as reference to that agreement, deed, instrument, license or other document as amended, varied, supplemented, modified or novated at the time of such reference
- n. Unless otherwise stated, any reference to any period commencing "from" a specified day or date and "till" or "until" a specified day or date shall include either such days or date

**Note: MSIs must read these conditions carefully and comply strictly while submitting their bids.**

### 5.3 Expected To Examine All Instructions

- 5.3.1 The MSI is expected to examine all instructions, forms, terms, and specifications in the bidding documents. Failure to furnish all information required in the bidding documents or submitting a Bid not substantially responsive to the bidding documents in any respect may result in the rejection of the Bid.

### 5.4 All Costs

- 5.4.1 The MSI shall bear all the costs associated with the preparation and submission of its bid, and CHiPS in no case will be responsible or liable for these costs, regardless of conduct or outcome of Bidding Process.

### 5.5 Professional Excellence and Ethics

- 5.5.1 CHiPS requires that all MSIs participating in this Bid adhere to the highest ethical standards, both during the selection process and throughout the execution of the contract.

### 5.6 Failure of Successful MSI

- 5.6.1 Failure of the successful MSI to comply with all the requirements shall constitute sufficient grounds for the annulment of the award, in which event CHiPS may, make the award to the next lowest evaluated MSI or call for new bids.

### 5.7 Amendment/Cancellation

- 5.7.1 The CHiPS reserve the right to cancel this Tender at any time without any obligation to the MSIs. The CHiPS at any time, prior to the deadline for submission of Proposals, may amend the Tender by issuing an addendum in writing or by standard electronic means. The addendum will be binding on all the MSIs. MSIs shall acknowledge receipt of all amendments. To give MSIs reasonable time to take an amendment into account in their Proposals, the CHiPS may, if the amendment is substantial, extend the deadline for the submission of Proposals.

### 5.8 Right to accept or reject any or all Bids

- 5.8.1 The CHiPS reserve the right to accept any bid, and to annul the bid process and reject all bids at any time prior to award of contract, without assigning any reason & without thereby incurring any liability to the affected MSI or MSIs or any obligation to inform the affected MSI or MSIs of the grounds for the action.

### 5.9 Conditional Bids

- 5.9.1 If a MSI imposes conditions, which is in addition to or in conflict with the conditions mentioned herein, his bid is liable to be summarily rejected. In any case none of such conditions will be deemed to have been accepted unless specifically mentioned in the letter of acceptance of bid issued by the CHiPS.

### 5.10 Acceptance Testing

- 5.10.1 The equipment will be tested by CHiPS or its nominated agency.

### 5.11 Proprietary Rights

- 5.11.1 The MSI shall indemnify CHiPS against all third-party claims of infringement of patent, copy right, trademark, license or industrial design rights, software piracy arising from use of goods or any part thereof within India.

## 5.12 Delays in performance of supplier's obligation

- 5.12.1 Any delay by the Successful MSI in the performance of its delivery obligations shall render the Successful MSI liable to any or all of the following sanctions – forfeiture of its performance Bank Guarantee, imposition of Damages and / or termination of the work order for default.

## 5.13 Damages

- 5.13.1 CHiPS reserve the right to terminate the contract if total Damage in this regard exceeds 10% of the Project value. The provisions pertaining to Damages under the RFP shall be in addition, and without prejudice, to the provisions pertaining to the same under the Agreement.

## 5.14 Applicable Law

- 5.14.1 The work order issued under the Agreement shall be interpreted in accordance with the laws of India, irrespective of the place of delivery, the place of performance or place of payment under the Agreement. The Agreement shall deem to have made at the place in India from where the contract has been issued.

## 5.15 Notices

- 5.15.1 Any notice given by one party to the other pursuant to this contract shall be sent in writing or by telegram or Telefax and confirmed in writing to CEO, CHiPS, SDC Building, Civil Lines, 02nd floor, Near Civil Lines Police Station, Raipur, Chhattisgarh–492001, Fax:- 0771-4066205, Ph. No. 0771-4014158.
- 5.15.2 A notice shall be effective when delivered or on the notice's effective date whichever is later.

## 5.16 Taxes & Duties

- 5.16.1 The MSI shall be entirely responsible for all taxes, duties, license fee etc.
- 5.16.2 Any upward/downward revision of GST shall be applicable at the time of invoicing. However, to arrive at the bid value of the respective MSI, MSI has to quote the charges inclusive of all taxes, duties, levies etc. excluding GST.

## 5.17 Defence of Suits

- 5.17.1 If any action in court is brought against the CHiPS/ Consignee for failure or neglect on the part of the MSI to perform any acts, matters, covenants or things under the contract or for the damage or injury caused by the alleged omission of neglect on the part of the contractor, his agents, representatives or sub-contractors, workmen supplier or employees, the contractor in all such cases shall indemnify and keep CHiPS harmless from all costs, Damages, expenses or decrees arising out of such action.

## 5.18 Conditions Precedent

- 5.18.1 This Contract is subject to the fulfilment of the following conditions precedent by the MSI
- Furnishing by the MSI, an unconditional, irrevocable and continuing Performance Bank Guarantee, which shall be as per Clause 4.38, in a form and manner acceptable to the Purchaser
  - Execution of a Deed of Indemnity in terms of Clause 5.34 - Indemnity
  - Obtaining of all statutory and other approvals required for the performance of the Services under this Contract
  - Furnishing of such other documents as the Purchaser may specify

- e. The Purchaser reserves the right to waive any or all of the conditions specified above in writing and no such waiver shall affect or impair any right, power or remedy that the Purchaser may otherwise have

## 5.19 Representations & Warranties

- 5.19.1 In order to induce the Purchaser to enter into this Contract, the MSI hereby represents and warrants as of the date hereof, the following:
  - a. That the MSI has the power and the authority that would be required to enter into this Contract and the requisite experience, the technical know-how and the financial wherewithal required to successfully execute the terms of this Contract and to provide Services sought by the Purchaser under this Contract
  - b. That the MSI is not involved in any litigation or legal proceedings, pending, existing, potential or threatened, that may have an impact of affecting or compromising the performance or delivery of Services under this Contract
  - c. That the representations and warranties made by the MSI in its Bid, RFP and Contract are and shall continue to remain true and fulfil all the requirements as are necessary for executing the obligations and responsibilities as laid down in the Contract and the RFP and unless the Purchaser specifies to the contrary, the MSI shall be bound by all the terms of the Bid and the Contract through the term of the Contract.
  - d. That the MSI has the professional skills, personnel, infrastructure and resources/ authorizations that are necessary for providing all such Services as are necessary to fulfil the Scope of Work stipulated in the RFP and the Contract.
  - e. That the MSI shall ensure that all assets/ components including but not limited to equipment, documents, etc. installed, procured and created during the term of this Contract are duly maintained and suitably updated, upgraded, replaced with regard to contemporary requirements
  - f. That the MSI shall use such assets of the Purchaser as the Purchaser may permit for the sole purpose of execution of its obligations under the terms of the Bid, RFP or this Contract. The MSI shall however, have no claim to any right, title, lien or other interest in any such property, and any possession of property for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof
  - g. That there shall not be any privilege, claim or assertion made by a third party with respect to right or interest in, ownership, mortgage or disposal of any asset, property, movable or immovable as mentioned in any Intellectual Property Rights, licenses and permits.
  - h. That the execution of the scope of work and the Services herein is and shall be in accordance and in compliance with all applicable laws.
  - i. That all conditions precedent under the Contract have been satisfied.
  - j. That neither the execution and delivery by the MSI of the Contract nor the MSIs' compliance with or performance of the terms and provisions of the Contract (i) shall contravene any provision of any Applicable Laws or any order, writ, injunction or decree of any court or Governmental Authority binding on the MSI, (ii) shall conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any Contract, Contract or instrument to which the MSI is a party or by which it or any of its property or assets is bound or to which it may be subject or (iii) shall violate any provision of the Memorandum and Articles of Association of the MSI .
  - k. That the MSI certifies that all registrations, recordings, filings and notarizations of the Contract and all payments of any tax or duty, including but not limited to stamp duty, registration charges or similar amounts which are required to be effected or made by

the MSI which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been made.

- l. That the MSI confirms that there has not and shall not occur any execution, amendment or modification of any agreement/ contract without the prior written consent of the Purchaser, which may directly or indirectly have a bearing on the Contract with the Purchaser.
- m. That the MSI owns or has good, legal or beneficial title, or other interest in, to the property, assets and revenues of the MSI on which it grants or purports to grant or create any interest pursuant to the Contract, in each case free and clear of any encumbrance and further confirms that such interests created or expressed to be created are valid and enforceable.
- n. That the MSI owns, has license to use or otherwise has the right to use, which are required or desirable for performance of its services under this contract. All Intellectual Property Rights (owned by the MSI or which the MSI is licensed to use) required by the MSI for the performance of the contract are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required to maintain the same in full force and effect have been taken thereon and shall keep the Purchaser indemnified in relation thereto.
- o. That the MSI shall at all times maintain sufficient manpower, resources, and facilities, to provide the Services in a workmanlike manner on a timely basis.
- p. That its security measures, policies and procedures are adequate to protect and maintain the confidentiality of the Confidential Information
- q. That in providing the Services or deliverables or materials, neither MSI or its agent, nor any of its employees, shall utilize information which may be considered confidential information of, or proprietary to, any prior employer or any other person or entity;
- r. That the MSI shall provide adequate and appropriate support and participation, on a continuous basis

## 5.20 Scope of Work

- 5.20.1 Scope of the Work shall be as defined in Section 7 - Scope of Work and Annexes thereto of this tender.
- 5.20.2 Purchaser shall engage the MSI for technology refresh of SDC, Chhattisgarh including Operations & Maintenance for a period of 5 years of which implementation period is 9 months and O&M period is 4.3 years (for 17 quarters). The MSI is required to provide such services, support and infrastructure as the Purchaser or Purchaser's representative may deem proper and necessary, during the term of this Contract, and includes all such processes and activities which are consistent with the proposals set forth in the Bid, the RFP and this Contract and are deemed necessary by the Purchaser, in order to meet its business requirements (hereinafter 'scope of work').
- 5.20.3 If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the Services or are required for proper performance or provision of the Services in accordance with this RFP, they shall be deemed to be included within the Scope of Work to be delivered for the Charges, as if such services, functions or responsibilities were specifically described in this RFP
- 5.20.4 The Purchaser or Purchaser's representative reserves the right to amend any of the terms & conditions with mutual agreement in relation to the Scope of Work and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the Scope of Work pursuant to Clause 5.40- Change Orders/ Alteration/ Variation

## 5.21 Key Performance Measurements

- 5.21.1 Unless specified by the Purchaser to the contrary, the MSI shall execute the services and carry out the scope of work in accordance with the terms & conditions of this Contract, Scope of Work and the service specifications as laid down in this RFP.
- 5.21.2 If the Contract, Scope of Work, or Service Specification includes more than one documents, and unless the Purchaser specifies otherwise, the document issued later in time shall take precedence over an earlier one in the event of any inconsistency.
- 5.21.3 The Purchaser reserves the right to amend any of the terms & conditions in relation to the Contract and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the scope of work.

## 5.22 Commencement and progress

- 5.22.1 The MSI shall be subject to the fulfilment of the conditions precedent set out in Clause 5.18 - Conditions Precedent of this Section, commence the performance of its obligations in a manner as specified in the Scope of Work
- 5.22.2 The MSI shall proceed to carry out the activities / services with diligence and expedition in accordance with the stipulation as to the time, manner, mode, and method of execution contained in this RFP.
- 5.22.3 The MSI shall be responsible for and shall ensure that all Services are performed in accordance with the Contract, Scope of Work & Specifications. MSI shall comply with such Specifications and all other standards, terms and other stipulations/conditions set out hereunder.
- 5.22.4 The MSI shall perform the activities/ Services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional engineering. It shall employ safe and effective equipment, machinery, material and methods. The MSI shall always act, in respect of any matter relating to this RFP, as faithful advisors to the Purchaser and shall, at all times, support and safeguard the Purchaser's legitimate interests in any dealings with Third Parties.
- 5.22.5 The items supplied under this Contract shall conform to the standards mentioned in Annexure-16 & 17. In other cases where no applicable standard is available such standards which are issued by the relevant authorized agencies shall be applicable. Delivery of the items shall be made by the MSI in accordance with the terms specified by the Purchaser in its Notification of Award / Work Order.

## 5.23 Standards of Performance

- 5.23.1 The MSI shall perform the activities/ Services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional engineering. It shall employ safe and effective equipment, machinery, material and methods. The MSI shall always act, in respect of any matter relating to this RFP, as faithful advisors to the Purchaser and shall, at all times, support and safeguard the Purchaser's legitimate interests in any dealings with Third Parties.

## 5.24 Sub-contract

- 5.24.1 MSI shall not subcontract any core work without CHiPS authorities' prior written consent which may be withheld or denied by CHiPS authorities without assigning any reasons.
- 5.24.2 MSI may, with prior written consent of the CHiPS authority, subcontract only the Civil work and supply of Non-IT components mentioned under the Agreement. MSI shall be responsible for the performance of its subcontractors and ensure that they comply with all the terms and conditions of the Agreement.



## 5.25 MSI's Obligations

- 5.25.1 The MSI's obligations shall include Technology Refresh of the CGSDC for Government of Chhattisgarh, Raipur including Operations & Maintenance for a period of 5 years of which implementation period is 9 months and O&M period is 4.3 years (for 17 quarters) as specified by the Purchaser in the Scope of Work and other sections of the RFP and Contract and changes thereof to enable the Purchaser to meet their objectives and operational requirements. It shall be the MSI's responsibility to ensure the proper and successful implementation, performance and continued operations of the project in accordance with and in strict adherence to the terms of the Bid, the RFP and this Contract
- 5.25.2 In addition to the aforementioned, the MSI shall perform the Services specified by the 'Scope of Work' requirements as specified in the RFP and changes thereof
- 5.25.3 The MSI shall ensure that the MSI's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. The MSI shall ensure that the Services are performed through the efforts of the MSI's Team, in accordance with the terms hereof and to the satisfaction of the Purchaser. Nothing in this Contract relieves the MSI from its liabilities or obligations under this Contract to provide the Services in accordance with the Contract and the Bid to the extent accepted by the Purchaser
- 5.25.4 The MSI shall be responsible on an ongoing basis for coordination with other vendors and agencies of the Purchaser in order to resolve issues and oversee implementation of the same.

### 5.25.5 Obligations related to IT and Non-IT Infrastructure

- a. The MSI shall Design, supply equipment/ components including associated accessories as under this Contract and Configuration, Implementation, Testing, Commissioning, Operations & Maintenance of those components during the entire period of Contract
- b. In case of any dissatisfaction or default on part of the MSI in providing the level of support desired by the Purchaser or Purchaser's Technical Representative in relation to the infrastructure supplied by the MSI, the MSI shall extend the necessary support required to meet the commitments without any financial liability to the Purchaser
- c. It is expected that MSI and OEM shall ensure that the equipment/ components being supplied by them shall be supported for the entire contract period. If the same is de-supported by the OEM for any reason whatsoever, the MSI shall replace it with an equivalent or better substitute that is acceptable to Purchaser without any additional cost to the Purchaser and without impacting the performance of the Solution in any manner whatsoever.
- d. In case of any problems/ issues arising due to integration of the infrastructure supplied by the MSI with any other component(s)/ product(s) under the purview of the overall solution, the MSI shall replace the required component(s) with an equivalent or better substitute that is acceptable to Purchaser without any additional cost to the Purchaser and without impacting the performance of the solution in any manner whatsoever
- e. The MSI shall ensure that the preventive maintenance monthly and break-fix maintenance is conducted in accordance with the specifications of the components and the best practices followed in the industry without any additional costs to the Purchaser
- f. The MSI shall extend necessary assistance, consultancy and services to the Purchaser beyond the defined Scope of Work to resolve issues related to the components supplied by him, under critical and unforeseen situations
- g. The MSI shall provide required information to the Purchaser as and when the OEM comes out with the same
- h. The MSI shall ensure that it is in compliance with all Applicable Laws at all times while discharging its Scope of Work



- i. The MSI shall ensure that it has procured all necessary permits and consents that may be required to discharge its Scope of Work effectively
- 5.25.6 **MSI's (MSI) Representative:** The MSI's Representative shall have all the powers requisite for the performance of Services under this Contract. The MSI's Representative shall liaise with the Purchaser's Representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. He shall extend full co-operation to Purchaser's representative in the manner required by them for supervision/ inspection/ observation of the Infrastructure, procedures, performance, reports and records pertaining to the works. He shall also have complete charge of the MSI's personnel engaged in the performance of the works and to ensure internal discipline, compliance of rules, regulations and safety practice. He shall also co-ordinate and co-operate with the other service providers of the Purchaser working at the site/ offsite for activities related to planning, execution of Scope of Work and providing Services under this Contract

**5.25.7 Reporting Progress**

- a. The MSI shall monitor progress of all the activities related to the execution of this Contract and shall submit to the Purchaser, at no extra cost, progress reports with reference to all related work, milestones and their progress during the implementation phase at the end of each month or before the expiry of the last day of each month
- b. Periodic meetings shall be held between the representatives of the Purchaser and the MSI once in every 15 days during the implementation phase to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held on an ongoing basis, once in every 30 days to discuss the performance of the Contract.
- c. The MSI shall ensure that the respective teams involved in the execution of work are part of such meetings
- d. State Level Committee involving representatives of the Purchaser and senior officials of the MSI shall be formed for the purpose of this Contract. This committee shall meet at intervals, as decided by the Purchaser later, to oversee the progress of the Project
- e. The equipment, Services and manpower to be provided/ installed/deployed by the MSI under the Contract and the manner and speed of implementation & maintenance of the work and Services are to be conducted in a manner to the satisfaction of Purchaser's representative in accordance with the Contract
- f. The Purchaser reserves the right to inspect and monitor/ assess the progress/ performance of the work/ services at any time during the course of the Contract. The Purchaser may demand and upon such demand being made, the MSI shall provide documents, data, material or any other information which the Purchaser may require, to enable it to assess the progress/ performance of the Work/ Service
- g. At any time during the course of the Contract, the Purchaser shall also have the right to conduct, either itself or through an independent audit firm appointed by the Purchaser as it may deem fit, an audit to monitor the performance by the MSI of its obligations/ functions in accordance with the standards committed to or required by the Purchaser and the MSI undertakes to cooperate with and provide to the Purchaser/ any other MSI appointed by the Purchaser, all documents and other details as may be required by them for this purpose
- h. If the rate of progress of the works or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works by the stipulated time, or is in deviation to RFP requirements/ standards, the Purchaser's representative shall so notify the MSI in writing
- i. The MSI shall reply to the written notice giving details of the measures he proposes to take to expedite the progress so as to complete the works by the prescribed time or to ensure compliance to RFP requirements. The MSI shall not be entitled to any additional payment for taking such steps. If at any time it should appear to the Purchaser or Purchaser's Representative that the actual progress of work does not conform to the

approved programme the MSI shall produce at the request of the Purchaser's Representative a revised programme showing the modification to the approved programme necessary to ensure completion of the works within the time for completion or steps initiated to ensure compliance to the stipulated requirements

- j. The submission seeking approval by the Purchaser or Purchaser's Representative of such programme shall not relieve the MSI of any of his duties or responsibilities under the Contract
- k. In case during execution of works, the progress falls behind schedule or does not meet the RFP requirements, MSI shall deploy extra manpower/ resources to make up the progress or to meet the RFP requirements. Programme for deployment of extra manpower/ resources shall be submitted to the Purchaser for its review and approval, which approval shall not be unreasonably withheld. All time and cost effect in this respect shall be borne, by the MSI within the Contract value

#### **5.25.8 Knowledge of Site Conditions**

- a. The MSI shall be deemed to have understood the requirements and have satisfied himself with the Data contained in the Bidding Documents, the quantities and nature of the works and materials necessary for the completion of the works, etc., and in-general to have obtained himself all necessary information of all risks, contingencies and circumstances affecting his obligations and responsibilities therewith under the Contract and his ability to perform it. However, if during delivery or installation, MSI observes physical conditions and/or obstructions affecting the work, the MSI shall take all measures to overcome them.
- b. MSI shall be deemed to have satisfied himself as to the correctness and sufficiency of the Contract Price for the works. The consideration provided in the Contract for the MSI undertaking the works shall cover all the MSI's obligation and all matters and things necessary for proper execution and maintenance of the works in accordance with the Contract and for complying with any instructions which the Purchaser's Representative may issue in accordance with the connection therewith and of any proper and reasonable measures which the MSI takes in the absence of specific instructions from the Purchaser's Representative
- c. The MSI shall have conducted its own due diligence with regard to the information contained in the RFP. The Purchaser does not make any representation or warranty as to the accuracy, reliability or completeness of the information in this RFP and it is not possible for the Purchaser to consider particular needs of each MSI who reads or uses this RFP. Each prospective MSI should conduct its own investigations and analyses and check the accuracy, reliability and completeness of the information provided in this RFP and obtain independent advice from appropriate sources
- d. The Purchaser shall not have any liability to any prospective MSI or any other person under any laws (including without limitation the law of contract or tort), the principles of equity, restitution or unjust enrichment or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with anything contained in this RFP, any matter deemed to form part of this RFP, the declaration of the MSI, the information supplied by or on behalf of the Purchaser or its employees, any consultants, or otherwise arising in any way from the bidding process. The Purchaser shall also not be liable in any manner whether resulting from negligence or otherwise however caused arising from reliance of any MSI upon any statements contained in this RFP

#### **5.25.9 Program of Work**

- a. Within 07 days after the award of work under this Contract or as part of kick-off meeting whichever is earlier, the MSI shall submit to the Purchaser for its approval a detailed programme showing the sequence, procedure and method in which he proposes to carry out the works as stipulated in the Contract and shall, whenever reasonably required by the Purchaser's Representative furnish in writing the arrangements and

methods proposed to be made for carrying out the works. The programme so submitted by the MSI shall conform to the duties and periods specified in the Contract. The Purchaser and the MSI shall discuss and agree upon the work procedures to be followed for effective execution of the works, which the MSI intends to deploy and shall be clearly specified. Approval by the Purchaser's Representative of a programme shall not relieve the MSI of any of his duties or responsibilities under the Contract

- b. If the MSI's work plans necessitate a disruption/ shutdown in Purchaser's operation, the plan shall be mutually discussed and developed so as to keep such disruption/ shutdown to the barest unavoidable minimum. Any time and cost arising due to failure of the MSI to develop/ adhere such a work plan shall be to his account.

#### **5.25.10 MSI's (MSI) Organization**

- a. The MSI's Team shall be deployed for execution of work and provision of Services under this Contract as mentioned in Section 7 - Scope of Work
- b. The MSI shall supply to the Purchaser for its approval, within 10 calendar days after the release of Work Order under this Contract during the kick-off meeting whichever is earlier, an organization chart showing the proposed organization/ manpower to be deployed by the MSI for execution of the work including the identities and Curriculum-Vitae of the key personnel to be deployed
- c. The MSI should to the best of his efforts, avoid any change in the organization structure proposed for execution of this Contract or replacement of any manpower resource appointed for the project. If the same is however unavoidable, due to circumstances such as the resource leaving the MSI's organization, the outgoing resource shall be replaced with an equally competent resource or better on approval from the Purchaser. The MSI shall promptly inform the Purchaser in writing, if any such revision or change is necessary
- d. In case of replacement of any manpower resource, the MSI should ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service
- e. All manpower resources deployed by the MSI for execution of this Contract must strictly adhere to the attendance reporting procedures and make their Services available for the entire reporting time period
- f. The MSI shall provide necessary supervision during the execution of work and as long thereafter as the Purchaser may consider necessary for the proper fulfilment of the MSI's obligations under the Contract. The MSI or his competent and authorized representative(s) shall be constantly present at the site whole time for supervision. The MSI shall authorize his representative to receive directions and instructions from the Purchaser's Representative
- g. The MSI shall be responsible for the deployment, transportation, accommodation and other requirements of all its employees required for the execution of the work and provision of Services for all costs/ charges in connection thereof
- h. The MSI shall provide and deploy only those manpower resources who are qualified/ skilled and experienced in their respective trades and who are competent to deliver in a proper and timely manner the work they are required to perform or to manage/ supervise the work
- i. The Purchaser's Representative may at any time object to and require the MSI to remove forthwith from the Project any authorized representative or employee of the MSI or any person(s) of the MSI's Team, if, in the opinion of the Purchaser's Representative the person in question has misconducted or his/ her deployment is otherwise considered undesirable by the Purchaser's Representative. The MSI shall forthwith remove and shall not again deploy the person without the written consent of the Purchaser's Representative

- j. The Purchaser's Representative may at any time object to and request the MSI to remove from the Project any of MSI's authorized representative including any employee of the MSI or his team or any person(s) deployed by MSI or his team for professional incompetence or negligence or for being deployed for work for which he is not suited. The MSI shall consider the Purchaser's Representative request and may accede to or disregard it. The Purchaser's Representative, having made a request, as aforesaid in the case of any person, which the MSI has disregarded, may in the case of the same person at any time but on a different occasion, and for a different instance of one of the reasons referred to above in this clause object to and require the MSI to remove that person from deployment on the work, which the MSI shall then forthwith do and shall not again deploy any person so objected to on the work or on the sort of work in question (as the case may be) without the written consent of the Purchaser's Representative
- k. The Purchaser's Representative shall state to the MSI in writing his reasons for any request or requirement pursuant to this clause
- l. The MSI shall maintain backup personnel and shall promptly replace every person removed, pursuant to this section, with an equally competent substitute from the pool of backup personnel

#### **5.25.11 Adherence to safety procedures, rules regulations and restrictions**

- a. MSI shall comply with the provision of all laws including labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by Purchaser shall be applicable in the performance of this Contract and MSI shall abide by these laws
- b. MSI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. Purchaser's employee also shall comply with safety procedures/ policy
- c. The MSI shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations
- d. MSI shall also adhere to all security requirement/ regulations of the Purchaser during the execution of the work

#### **5.25.12 Statutory Requirements**

- a. During the tenure of this Contract nothing shall be done by the MSI in contravention of any law, act and/ or rules/ regulations, there under or any amendment thereof governing inter-alia customs, stowaways etc. and shall keep Purchaser indemnified in this regard
- b. The MSI and their personnel/ representative shall not alter/ change/ replace any hardware component proprietary to the Purchaser and/ or maintenance of Third Party without prior consent of the Purchaser
- c. The MSI and their personnel/ representative shall not without consent of the Purchaser install any hardware or software not purchased/ owned by the Purchaser

### **5.26 MSI's Personnel**

- 5.26.1 The MSI shall employ and provide such qualified and experienced personnel as are required to perform the Services under the Contract
- 5.26.2 All the personnel, also of the MSI's partners shall be deployed only after adequate background verification check. The MSI shall submit the background verification check report for the personnel if required by CHIPS, Any deviations, if observed, would lead to removal of the personnel from the Project.

## 5.27 Contract Administration

- 5.27.1 No variation or modification of the terms & conditions of the contract shall be made except by written amendment signed by the parties.
- 5.27.2 Either party may appoint any individual / organization as their authorized representative through a written notice to the other party. Each Representative shall have the authority to:
  - a. Exercise all of the powers and functions of his/her Party under this Contract other than the power to amend this Contract and ensure the proper administration and performance of the terms hereof; and
  - b. Bind his or her Party in relation to any matter arising out of or in connection with this Contract.
- 5.27.3 The MSI along with other members / third parties / OEMs shall be bound by all undertakings and representations made by the authorized representative of the MSI and any covenants stipulated hereunder, with respect to this Contract, for and on their behalf.
- 5.27.4 For the purpose of execution or performance of the obligations under this Contract, the Purchaser's representative would act as an interface with the nominated representative of the MSI. The MSI shall comply with all instructions that are given by the Purchaser's representative during the course of this Contract in relation to the performance of its obligations under the terms of this Contract and the RFP.

## 5.28 Purchaser's Right of Monitoring, Inspection and Periodic Audit

- 5.28.1 The Purchaser or Purchaser's Technical Representative reserves the right to inspect and monitor/ assess the progress/ performance/ maintenance of the project at any time during the course of the Contract, after providing due notice to the MSI. The Purchaser may demand and upon such demand being made, the purchaser shall be provided with any document, data, material or any other information which it may require, to enable it to assess the progress of the Project
- 5.28.2 The Purchaser or Purchaser's Technical Representative shall also have the right to conduct, through an independent audit firm appointed by the Purchaser as it may deem fit, an audit to monitor the performance by the MSI of its obligations/ functions in accordance with the standards committed to or required by the Purchaser and the MSI undertakes to cooperate with and provide to the Purchaser, all documents and other details as may be required by them for this purpose. Any deviations or contravention identified as a result of such audit/ assessment would need to be rectified by the MSI failing which the Purchaser may, without prejudice to any other rights that it may issue a notice of default
- 5.28.3 The MSI shall at all times provide to the Purchaser or the Purchaser's Representative access to the Site

## 5.29 Purchaser's Obligations

- 5.29.1 The Purchaser's Representative shall interface with the MSI, to provide the required information, clarifications and to resolve any issues as may arise during the execution of the Contract. Purchaser shall provide adequate cooperation in providing details, assisting with coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the Purchaser is proper and necessary.
- 5.29.2 Purchaser shall ensure that timely approval is provided to the MSI, where deemed necessary, which should include technical architecture diagrams and all the specifications related to IT and Non-IT infrastructure required to be provided as part of the Scope of Work. All such documents shall be approved as soon as possible of the receipt of the documents by the Purchaser.
- 5.29.3 The Purchaser shall approve all such documents as per above Clause

- 5.29.4 The Purchaser's Representative shall interface with the MSI, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract

### 5.30 Intellectual Property Rights

- 5.30.1 Purchaser shall own and have Intellectual Property Rights of all the deliverables which have been developed by the MSI during the performance of Services and for the purposes of inter-alia use of such Services under this Contract. The MSI undertakes to disclose all Intellectual Property Rights arising out of or in connection with the performance of the Services to the Purchaser and execute all such agreements/documents and file all relevant applications, effect transfers and obtain all permits and approvals that may be necessary in this regard to effectively conserve the Intellectual Property Rights of the Purchaser.
- 5.30.2 If Purchaser desires, Further, the MSI shall be obliged to ensure that all approvals, registrations which are inter-alia necessary for use of the infrastructure installed by the MSI, the same shall be acquired in the name of the Purchaser, prior to termination of this Contract and which shall be assigned by the Purchaser to the MSI for the purpose of execution of any of its obligations under the terms of the Bid, RFP or this Contract. However, subsequent to the term of this Contract, such approvals etc. Shall endure to the exclusive benefit of the Purchaser.
- 5.30.3 The MSI shall ensure that while it uses any hardware, processes or material in the course of performing the Services, it does not infringe the Intellectual Property Rights of any person and MSI shall keep the Purchaser indemnified against all costs, expenses and liabilities howsoever, arising out of any illegal or unauthorized use (piracy) or in connection with any claim or proceedings relating to any breach or violation of any permission/license terms or infringement of any Intellectual Property Rights by the MSI during the course of performance of the Services.

### 5.31 Record of Contract Documents

- 5.31.1 The MSIs' shall at all time make and keep sufficient copies of the specifications and Contract documents for him to fulfil his duties under the contract,
- 5.31.2 The MSI shall keep at least two copies of each and every specification and Contract document, in excess of his own requirement and those copies shall be available at all times for use by the Purchaser's Representative and by any other person authorized by the Purchaser's Representative.

### 5.32 Ownership and Retention of Documents

- 5.32.1 The Purchaser shall own the Documents, prepared by or for the MSI arising out of or in connection with this Contract
- 5.32.2 Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by the Purchaser, the MSI shall deliver to the Purchaser all Documents provided by or originating from the Purchaser and all Documents produced by or from or for the MSI in the course of performing the Services, unless otherwise directed in writing by the Purchaser at no additional cost. The MSI shall not, without the prior written consent of the Purchaser store, copy, distribute or retain any such Documents

### 5.33 Ownership of Equipment

- 5.33.1 The Purchaser shall own assets/ components / furnishings / interiors including but not limited to equipment, documents and items supplied by the MSI arising out of or in connection with this Contract.
- 5.33.2 However, all the risk and liability arising out of or in connection with the usage of the equipment, assets/ components during the term of the Contract shall be borne by the MSI

### 5.34 Indemnity

- 5.34.1 The MSI shall indemnify and defend CHiPS and its representatives & employees and hold CHiPS, its representatives, employees harmless from:
- 5.34.2 Damages and losses caused by its negligent or intentional act or omission or any damages and losses caused by the negligent act of any third party or sub-contractor or agency engaged by the MSI ;
- 5.34.3 Damages and losses resulting from the non-compliance with the established obligations Third Party claim against CHiPS or its nominated agency that any Deliverables/Services/Equipment provided by the MSI infringes a copyright, trade secret, patents or other intellectual property rights of any third party in which case the MSI shall defend such claim at its expense and shall pay any costs or damages that may be finally awarded against CHiPS or its nominated agency. The MSI shall not indemnify CHiPS, however, if the claim of infringement is caused by (a) misuse or modification of the Deliverables; or (b) CHiPS failure to use corrections or enhancements made available by the MSI; or (c) CHiPS/MSI use of the Deliverables in combination with any product or information not owned or developed or supplied by the MSI.
- 5.34.4 If any Deliverable is or likely to be held to be infringing, the MSI shall at its expense and option either (i) procure the right for CHiPS to continue using it, or (ii) replace it with a non- infringing equivalent, or (iii) modify it to make it non-infringing.
- 5.34.5 Any environmental damages caused by it and/or its representatives or employees or employees of any third party or sub-contractor or agency engaged by the MSI
- 5.34.6 Breach (either directly by it or through its representatives and/or employees) of any representation and guarantee declared herein by it;
- 5.34.7 From any and all claims, actions, suits, proceedings, taxes, duties, levies, costs, expenses, damages and liabilities, including attorneys' fees, arising out of, connected with, or resulting from or arising in connections with the services provided due to neglect, omission or intentional act.

### 5.35 Confidentiality

- 5.35.1 Information relating to the examination, clarification, evaluation and recommendation for the MSIs shall not be disclosed to any person who is not officially concerned with the process or is not a retained professional advisor advising CHiPS in relation to, or matters arising out of, or concerning the Bidding Process or CHiPS will treat all information, submitted as part of the Bid, in confidence and will require all those who have access to such material to treat the same in confidence. CHiPS may not divulge any such information unless it is directed to do so by any statutory entity that has the power under Applicable Law to require its disclosure or is to enforce or assert any right or privilege of the statutory entity and/ or CHiPS or as may be required by Applicable Law or in connection with any legal process. MSIs are to treat all information as strictly confidential and shall not use it for any purpose other than for preparation and submission of their Bid. The provisions of this Clause shall also apply mutatis mutandis to Bids and all other documents submitted by the MSIs, and CHiPS shall be under no obligation whatsoever to return to the MSIs any document or any information provided along therewith.
- 5.35.2 The MSI shall not use Confidential Information, the name or the logo of the Purchaser except for the purposes of providing the Service as specified under this RFP;
- 5.35.3 The MSI shall not, either during the term or 6 months after expiration of this Contract, disclose any proprietary or confidential information relating to the Services, Contract or the network architecture, Purchaser's business plan or operations without the prior written consent of the Purchaser.
- 5.35.4 The MSI may only disclose Confidential Information in the following circumstances:

- a. with the prior written consent of the Purchaser;
  - b. to a member of the MSI s' Team ("Authorized Person") if:
    - i. the Authorized Person needs the Confidential Information for the performance of obligations under this contract;
    - ii. the Authorized Person is aware of the confidentiality of the Confidential Information and is obliged to use it only for the performance of obligations under this contract
    - iii. If the information is already made available in any public domain
- 5.35.5 The MSI shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidential agreement with the members of the, subcontractors and other service provider's team members to the satisfaction of the Purchaser.
- 5.35.6 The MSI shall sign a Non-Disclosure Agreement (NDA) as per Annexure-15 with the Purchaser on mutually agreed terms & conditions. The MSI and its antecedents shall be bound by the NDA. The MSI shall be responsible for any breach of the NDA by its antecedents or delegates.
- 5.35.7 The MSI shall notify the Purchaser promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Contract or with the authority of the Purchaser.
- 5.35.8 The Purchaser reserves the right to adopt legal proceedings, civil or criminal, against the MSI in relation to a dispute arising out of breach of obligation by the MSI under this clause.

### 5.36 Taxes

- 5.36.1 The quoted price should be inclusive of all the applicable Taxes, levies, duties, etc. CHiPS shall deduct appropriate tax as applicable at source from the payment against the delivery & services and corresponding TDS certificate shall be issued at the end of respective quarter.
- 5.36.2 In case of any variation (upward or downward) in GST wherever applicable up to the date of invoice, the benefit or the burden of the same shall be passed on to CHiPS. Necessary documentary evidence shall be produced for having paid the excise duty, GST, if applicable and/ or other applicable levies. Variation would also include the introduction of any new tax / cess.

### 5.37 Warranty

- 5.37.1 A comprehensive on-site warranty and Operations & Maintenance on all goods supplied under this contract shall be provided by the respective Original Equipment Manufacturer (OEM) through MSI till the end of the Contract.
- 5.37.2 Technical Support shall be provided by the respective OEM till the end of the contract period.
- 5.37.3 The MSI shall warrant that the goods supplied under the Contract are new, non-refurbished, unused and recently manufactured; shall not be nearing End of Sale / End of Support; and shall be supported by the MSI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.
- 5.37.4 The MSI warrants that the goods supplied under this contract shall be of the reasonably acceptable grade and quality and consisted with the established and generally accepted standards for materials of this type. The goods shall be in full conformity with the specifications and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available.



- 5.37.5 The MSI further warrants that the Goods supplied under this Contract shall be free from all encumbrances and defects/faults arising from design, material, manufacture or workmanship (except insofar as the design or material is required by the Purchaser's Specifications)
- 5.37.6 The Purchaser shall promptly notify the MSI in writing of any claims arising under this warranty.
- 5.37.7 Upon receipt of such notice, the MSI shall, with all reasonable speed, repair or replace the defective Goods or parts thereof, without prejudice to any other rights which the Purchaser may have against the MSI under the Contract.
- 5.37.8 If the MSI, having been notified, fails to remedy the defect(s) within a reasonable period, the Purchaser may proceed to take such remedial action as may be necessary, at the MSI s' risk & expense and without prejudice to any other rights which the Purchaser may have against the MSI under the Contract

### 5.38 Term and Extension of the Contract

- 5.38.1 The term of this Contract shall be initially for a period of 5 years of which implementation period is 9 months and O&M period is 4.3 years (for 17 quarters) from the date of contract signing.
- 5.38.2 The Purchaser shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the MSI, at least 3 months before the expiration of the term hereof, whether it shall grant the MSI an extension of the term. The decision to grant or refuse the extension shall be at the Purchaser's discretion. Accordingly, the Bank Guarantee of the same amount shall be extended up to extended period of the Contract
- 5.38.3 Where the Purchaser is of the view that no further extension of the term be granted to the MSI, the Purchaser shall notify the MSI of its decision at least 3 (three) months prior to the expiry of the Term. Upon receipt of such notice, the MSI shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, the Purchaser shall either appoint an alternative MSI/Service provider or create its own infrastructure to operate such Services as are provided under this Contract. Purchaser shall make payment for work executed for the extended period post contract expiry.

### 5.39 Prices

- 5.39.1 Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract. Purchaser however reserves the right to review the charges payable for the Maintenance and Management of the infrastructure at any time at the request of Purchaser whichever is earlier to incorporate downward revisions as applicable and necessary.
- 5.39.2 If at any time, during the period of contract, the MSI offers identical services/products to any other Govt. Department/ Organization at prices lower than those chargeable under this contract, he shall notify the same to the purchaser and extend such reduced prices to the purchaser with immediate effect.

### 5.40 Change Orders/ Alteration/ Variation

- 5.40.1 The MSI shall agree that the requirements/quantities/ specifications and Service requirements given in the RFP are minimum requirements and are in no way exhaustive and guaranteed by the Purchaser.
  - a. Any upward revision (and/or additions consequent to errors, omissions, ambiguities, discrepancies in the quantities, specifications, architecture etc. of the RFP which the MSI had not brought to the Purchaser's notice till the time of award of work and not accounted for in his Bid shall not constitute a change order and such upward revisions

and/or addition shall be carried out by the MSI without any time and cost effect to Purchaser.

- b. It shall be the responsibility of the MSI to meet all the performance and other requirements of the Purchaser as stipulated in the RFP / Contract. Any upward revisions / additions of quantities, specifications, service requirements to those specified by the MSI in his Bid documents, that may be required to be made during installation / commissioning of the network or at any time during the currency of the contract in order to meet the conceptual design, objective and performance levels or other requirements as defined in the RFP. These changes shall be carried out as per mutual consent.
- 5.40.2 The Purchaser may at any time, by a written change order given to the MSI, make changes within the general Scope of Work. The Purchaser shall have an option to increase or decrease (decrease only if communicated to MSI prior to availing of services / dispatch of goods / equipment) the Quantities and/or Specifications of the goods/equipment to be supplied and installed by the MSI or service requirements, as mentioned in the Contract, at any time during the contract period.
- 5.40.3 The written advice to any change shall be issued by the Purchaser to the MSI up to 4 (four) weeks prior to the due date of provisioning/supply of such goods/equipment or commencement of services.
- 5.40.4 In case of increase in Quantities / Specifications or Service requirements or in case of additional requirement, the rate as provided in the Contract shall be considered as benchmark rates for procurement of the additional requirement from the MSI. However, based on the industry trends, Purchaser retains the right to review these rates. The additional requirement shall also be governed by the same terms & conditions as provided in the Contract except for the appropriate extension of time to be allowed for delivery/installation of such extra goods/equipment or for commencement of such services. In case of decrease in Quantities or Specifications of goods/equipment or Service requirements, the MSI shall give a reduction in price at the rate given in the Contract corresponding to the said decrease.
- 5.40.5 In case applicable rates for the increase/decrease in question are not available in the Contract then the rates as may be mutually agreed shall apply. The MSI shall not be entitled to any claim by way of change of price, damages, losses, etc. The MSI shall be compensated at actual for any cancellation charges provided the claim is duly supported by documentary evidence of having incurred cancellation charges, which results from Purchaser's action in reducing/cancelling Scope of Work.

**5.40.6 Conditions for Change Order**

- a. The change order shall be initiated only in case (i) the Purchaser or Purchaser's Technical Representative directs in writing the MSI to incorporate changes to the goods or design requirements already covered in the Contract. (ii) the Purchaser or Purchaser's Technical Representative directs in writing to the MSI to include any addition to the scope of work or services covered under this Contract or delete any part thereof, (iii) MSI requests to delete any part of the work which shall not adversely affect the work and if the deletions proposed are agreed to by the Purchaser and for which the cost and time benefits shall be passed on to the Purchaser
- b. Any change order comprising an alteration which involves change in the cost of the goods and/or services (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease in the Contract Value and adjustment of the implementation schedule if any
- c. If parties agree that the Contract does not contain applicable rates or that the said rates are inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall review of the Contract Value which shall represent the change in cost of the goods and/or works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing

- d. If there is a difference of opinion between the MSI and Purchaser's Representative on whether a particular item, work or part of the work constitutes a change order or not, the matter shall be handled in accordance with the procedures set forth in Clause 5.40.7 (k)

#### **5.40.7 Procedures for change Order**

- a. Upon receiving any revised requirement/advice, in writing, from the Purchaser or Purchaser's Technical Representative, the MSI would verbally discuss the matter with Purchaser's Representative.
- b. In case such requirement arises from the side of the MSI, he would also verbally discuss the matter with Purchaser's Representative giving reasons thereof.
- c. In either of the two cases as explained in Clause 5.40.7 (a) and clause 5.40.7 (b) above, the representatives of both the parties shall discuss on the revised requirement for better understanding and to mutually decide whether such requirement constitutes a change order or not.
- d. If it is mutually agreed that such requirement constitutes a "Change Order" then a joint memorandum shall be prepared and signed by the MSI and Purchaser to confirm a "Change Order" and basic ideas of necessary agreed arrangement.
- e. MSI shall study the revised requirement in accordance with the joint memorandum under Clause 5.40.7 (d) and assess subsequent schedule and cost effect, if any.
- f. Upon completion of the study referred to above under Clause 5.40.7 (e) the results of this study along with all relevant details including the estimated time and cost effect thereof with supporting documents would be submitted to the Purchaser to enable the Purchaser to give a final decision whether MSI should proceed with the change order or not in the best interest of the works.
- g. The estimated cost and time impact indicated by MSI shall be considered as a ceiling limit and shall be provisionally considered for taking a decision to implement change order.
- h. The time impact applicable to the Contract shall be mutually agreed, subsequently, on the basis of the detailed calculations supported with all relevant back up documents.
- i. In case MSI fails to submit all necessary substantiation/calculations and back up documents, the decision of the Purchaser regarding time and cost impact shall be final and binding on the MSI.
- j. If Purchaser accepts the implementation of the change order under Clause 5.40.7 (f) in writing, which would be considered as change order, then MSI shall commence to proceed with the enforcement of the change order pending final agreement between the parties with regard to adjustment of the Contract Value and the Schedule.
- k. In case, mutual agreement under Clause 5.40.7 (d) above, i.e. whether new requirement constitutes the change order or not, is not reached, then MSI in the interest of the works, shall take up the enforcement of the change order, if advised in writing to do so by Purchaser's Representative pending settlement between the two parties to the effect whether such requirement constitutes a change order or not as per the terms & conditions of Contract. The time and cost effects in such a case shall be mutually verified and recorded. Should it establish that the said work constitutes a change order, the same shall be compensated taking into account the records kept in accordance with the Contract.
- l. The MSI shall submit the necessary back up documents for the change order showing the break-up of the various elements constituting the change order for the Purchaser's review. If no agreement is reached between the Purchaser and MSI within 60 days after Purchaser's instruction in writing to carry out the change concerning the increase or decrease in the Contract Value and all other matters described above, either party may refer the dispute to arbitration.

#### **5.40.8 Conditions for Revised Work / Change Order**

- a. The provisions of the Contract shall apply to revised work / change order as if the revised work / Change order has been included in the original Scope of work. However, the Contract Value shall increase / decrease and the schedule shall be adjusted on account of the revised work / Change orders as may be mutually agreed in terms of provisions set forth in Clause 5.40. The MSI's obligations with respect to such revised work / change order shall remain in accordance with the Contract

#### 5.41 Suspension of Work

- 5.41.1 The MSI shall, if ordered in writing by the Purchaser's Representative, temporarily suspend the works or any part thereof for such a period and such a time as ordered, then MSI shall not be entitled to claim compensation for any loss or damage sustained by him by reason of temporary suspension of the Works as aforesaid but shall be eligible for the payment (of products/services delivered and accepted) during the suspension period as per contract. An extension of time for completion, corresponding with the delay caused by any such suspension of the works as aforesaid shall be granted to the MSI, if request for same is made and that the suspension was not consequent to any default or failure on the part of the MSI. Both MSI and purchaser acknowledges the suspension of work by purchaser, if results in extension of contract, the extra cost shall be on account of Purchaser which shall be mutually agreed. In case the suspension of works, is not consequent to any default or failure on the part of the MSI, and lasts for a period of more than 2 months, the MSI shall have the option to request the Purchaser to terminate the Contract with mutual consent.
- 5.41.2 In the event that the Purchaser suspends the progress of work for any reason not attributable to the MSI for a period in excess of 30 days in aggregate, rendering the MSI to extend his Bank Guarantee then Purchaser shall bear only the cost of extension of such bank guarantee for such extended period restricted to the normal bank rates as applicable in the international banking procedures subject to the MSI producing the requisite evidence from the bank concerned.

#### 5.42 Time is of Essence

- 5.42.1 Time shall be of the essence in respect of any date or period specified in this RFP or any notice, demand or other communication served under or pursuant to any provision of this RFP and in particular in respect of the completion of the Services by the MSI by the completion date.

#### 5.43 Completion of Contract

- 5.43.1 Unless terminated earlier, pursuant to Clauses 5.19, 5.30.3, 5.32, 5.33 and 5.35 the Contract shall terminate on the completion of term as specified in the Contract and only after the obligations mentioned in Clause 5.48 - Consequences of Termination are fulfilled to the satisfaction of the Purchaser

#### 5.44 Special Conditions of Contract

- 5.44.1 Amendments of, and Supplements to, Clauses in the General Conditions of Contract

#### 5.45 Event of Default by the MSI

- 5.45.1 The failure on the part of the MSI to perform any of its obligations or comply with any of the terms of this Contract which results in a material breach of the contract shall constitute an Event of Default on the part of the MSI. The events of default as mentioned above may include inter-alia the following:
  - a. the MSI has failed to adhere to any of the key performance indicators as laid down in the Key Performance Measures / Contract, or if the MSI has fallen short of matching such standards/targets as the Purchaser may have designated with respect to any task necessary for the execution of the scope of work under this Contract which results in a

material breach of the contract. The above-mentioned failure on the part of the MSI may be in terms of failure to adhere to timelines, specifications, requirements etc. or any other criteria as defined by the Purchaser;

- b. the MSI has failed to remedy a failure to perform its obligations in accordance with the directive, including specifications, timelines etc., issued by the Purchaser, despite being served with a default notice which laid down the specific deviance on the part of the MSI to comply with any stipulations or standards as laid down by the Purchaser; or
  - c. the MSI /MSIs' team has failed to conform with any of the Service/Facility Specifications/standards as set out in the scope of work of this RFP or has failed to adhere to any amended direction, modification or clarification as issued by the Purchaser during the term of this Contract and which the Purchaser deems proper and necessary for the execution of the scope of work under this Contract
  - d. the MSI has failed to demonstrate or sustain any representation made by it in this Contract, with respect to any of the terms of its Bid, the RFP and this Contract
  - e. there is an order from a court of competent jurisdiction for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to the MSI
  - f. the MSI Abandons the project during the Term of the Contract
- 5.45.2 Where there has been an occurrence of such defaults inter alia as stated above, the Purchaser shall issue a notice of default to the MSI, setting out specific defaults / deviances / omissions and providing a notice of Sixty (60) days to enable such defaulting party to remedy the default committed.
- 5.45.3 Where despite the issuance of a default notice to the MSI by the Purchaser the MSI fails to remedy the default to the satisfaction of the MSI, the Purchaser may, at its sole discretion where it deems fit, issue to the defaulting party another default notice or proceed to adopt such remedies as may be available to the Purchaser.

#### 5.46 Consequences of Event of Default

- 5.46.1 Where an Event of Default subsists or remains uncured the Purchaser may/ shall be entitled to:
- 5.46.2 The MSI shall in addition take all available steps to minimize loss resulting from such event of default
- 5.46.3 The Purchaser may, by a written notice of suspension to the MSI, suspend all payments to the MSI under the Contract, provided that such notice of suspension:
- a. shall specify the nature of the failure; and
  - b. shall request the MSI to remedy such failure within a specified period from the date of receipt of such notice of suspension by the MSI
- 5.46.4 In all cases of risk purchase, the difference in cost shall be borne by defaulting MSI / MSI
- 5.46.5 Terminate the Contract in Part or Full
- a. Retain such amounts from the payment due and payable by the Purchaser to the MSI as may be required to offset any losses caused to the Purchaser as a result of such event of default and the MSI shall compensate the Purchaser for any such loss, damages or other costs, incurred by the Purchaser in this regard. Nothing herein shall affect the continued obligation of the MSI and MSI's Team to perform all their obligations and responsibilities under this Contract in an identical manner as were being performed before the occurrence of the default.
  - b. Invoke the Performance Bank Guarantee and other Guarantees furnished hereunder, recover such other costs/ losses and other amounts from the MSI as may have resulted from such default and pursue such other rights and/or remedies that may be available to the Purchaser under law

## 5.47 Termination

- 5.47.1 The Purchaser may, terminate this Contract in whole or in part by giving the MSI a prior and written notice indicating its intention to terminate the Contract under the following circumstances:
- a. Where the Purchaser is of the opinion that there has been such Event of Default on the part of the MSI which would make it proper and necessary to terminate this Contract and may include failure on the part of the MSI to respect any of its commitments with regard to any part of its obligations under its Bid, the RFP or under this Contract.
  - b. Where it comes to the Purchaser's attention that the MSI (or the MSI s' Team) is in a position of actual conflict of interest with the interests of the Purchaser, in relation to any of terms of the MSI s' Bid, the RFP or this Contract
  - c. Where the MSI s' ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against the MSI, any failure by the MSI to pay any of its dues to its creditors, the institution of any winding up proceedings against the MSI or the happening of any such events that are adverse to the commercial viability of the MSI. In the event of the happening of any events of the above nature, the Purchaser shall reserve the right to take any steps as are necessary, to ensure the effective transition of the project to a successor MSI and to ensure business continuity
  - d. Termination for Insolvency: The Purchaser may at any time terminate the Contract by giving written notice to the MSI, without compensation to the MSI, if the MSI becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to the Purchaser.
  - e. Termination for Convenience: The Purchaser, may, by prior written notice sent to the MSI at least 6 months in advance, terminate the Contract, in whole or in part at any time for its convenience. The notice of termination shall specify that termination is for the Purchaser's convenience, the extent to which performance of work under the Contract is terminated, and the date upon which such termination becomes effective.

## 5.48 Consequences of Termination

- 5.48.1 In the event of termination of this contract due to any cause whatsoever, the contract with stand cancelled effective from the date of termination of this contract.
- 5.48.2 In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the MSI
- 5.48.3 Where the termination of the Contract is prior to its stipulated term on account of a Default on the part of the MSI or due to the fact that the survival of the MSI as an independent corporate entity is threatened/has ceased, or for any other reason, whatsoever, the Purchaser through re-determination of the consideration payable to the MSI as agreed mutually by the Purchaser and the MSI or through a third party acceptable to both the parties may pay the MSI for that part of the Services which have been authorized by the Purchaser and satisfactorily performed by the MSI up to the date of termination. Without prejudice any other rights, the Purchaser may retain such amounts from the payment due and payable by the Purchaser to the MSI as may be required to offset any losses caused to the Purchaser as a result of any act/omissions of the MSI. In case of any loss or damage due to default on the part of the MSI in performing any of its obligations with regard to the execution of the scope of work under this Contract, the MSI shall compensate the Purchaser for any such loss, damages or other costs, incurred by the Purchaser. Additionally, other members of its team shall perform all its obligations and responsibilities under this Contract in an identical manner as were being performed before the collapse of the MSI as described above in order to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all/any functions as stipulated by the Purchaser and as may

be proper and necessary to execute the scope of work under the Contract in terms of the MSI s' Bid, the RFP and this Contract.

- 5.48.4 Nothing herein shall restrict the right of the Purchaser to invoke the Bank Guarantee and other Guarantees furnished hereunder, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to the Purchaser under law.
- 5.48.5 The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of this Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

#### 5.49 Penalty

- 5.49.1 Ongoing performance and Service Levels shall be as per parameters stipulated by the Purchaser in this Contract, failing which the Purchaser may, at its discretion, impose penalties on the MSI as defined in General Conditions of the Contract and Service Level Agreement of the RFP

#### 5.50 Liquidated Damages

- 5.50.1 The MSI shall perform the Services and comply in all respects with the critical dates and the parties hereby agree that failure on part of the MSI to meet the critical dates without prejudice to any other rights that the Purchaser have, may lead to the imposition of such obligations as are laid down in the Delay and Deterrent Mechanism and/or levy of penalty as set and/or termination of the Contract at the discretion of the Purchaser.
- 5.50.2 Penalties shall be capped to maximum of 10% of the total CAPEX value and 25% of the total OPEX value. Beyond the mentioned capping, the Purchaser has the right to terminate the contract or a portion or part of the work thereof. The purchaser shall give 30 days' notice to the MSI of its intention to terminate the Contract and shall so terminate the Contract unless the MSI initiates remedial action acceptable to the Purchaser during the 30 days' notice period,
- 5.50.3 The Purchaser may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any money belonging to the MSI in its hands (which includes the Purchaser's right to claim such amount against MSI s' Bank Guarantee) or which may become due to the MSI. Any such recovery or liquidated damages shall not in any way relieve the MSI from any of its obligations to complete the Works or from any other obligations and liabilities under the Contract.
- 5.50.4 Delay not attributable to the MSI shall be considered for exclusion for the purpose of computing liquidated damages

#### 5.51 Dispute Resolution

- 5.51.1 The Purchaser and the MSI shall make every effort to resolve amicably by direct informal negotiations, any disagreement or disputes, arising between them under or in connection with the Contract
- 5.51.2 If, after Thirty (30) days from the commencement of such direct informal negotiations, the Purchaser and the MSI have been unable to resolve amicably a Contract dispute, either party may require that the dispute be referred for resolution to the formal mechanism specified in Clauses 5.51.3 and Clause 5.51.4
- 5.51.3 Arbitration: Any dispute, controversy, or claim arising out of or relating to this Agreement, including its formation, validity, or termination, shall be finally settled by arbitration in accordance with the Arbitration Act, 1996 in force at the time of the arbitration.
- 5.51.4 Appointment of Arbitrators:
  - 5.51.4.1 The arbitral tribunal shall consist of three arbitrators.
  - 5.51.4.2 Each party shall appoint one arbitrator, and the two appointed arbitrators shall jointly appoint the third arbitrator, who shall act as the presiding arbitrator.



- 5.51.4.3 If a party fails to appoint an arbitrator within 30 days from the receipt of the notice of arbitration, or if the two arbitrators fail to agree on the appointment of the presiding arbitrator within 30 days, then the appointment shall be as per the Arbitration Act, 1996.
- 5.51.5 Seat of Arbitration: The seat of arbitration shall be Raipur, Chhattisgarh.
- 5.51.6 Language: The language of the arbitration shall be English”.
- 5.51.7 It is a term of the Contract that the party invoking arbitration shall specify all disputes to be referred to arbitration at the time of invocation of arbitration and not thereafter
- 5.51.8 The fees of the arbitrator shall be borne by the parties nominating them and the fee of the Presiding Arbitrator, costs and other expenses incidental to the arbitration proceedings shall be borne equally by the parties
- 5.51.9 Subject to as aforesaid the provisions of the Arbitration and Conciliation Act, 1996 and any statutory modifications or re-enactment in lieu thereof shall apply to the arbitration proceedings under this clause
- 5.51.10 Continuance of the Contract: Notwithstanding the fact that settlement of dispute(s) (if any) under arbitration may be pending, the parties hereto shall continue to be governed by and perform the work in accordance with the provisions under this Contract

## 5.52 Insurance

- 5.52.1 The Goods supplied under this Contract shall be fully insured by the MSI, against any loss or damage up to the time it is delivered to the MSI -designated carrier for shipment to Purchaser or to Purchaser's designated location. The MSI shall submit to the Purchaser, certificate of insurance issued by the insurance company, indicating that such insurance has been taken.
- 5.52.2 The MSI shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods during their shipment from respective manufacturing/shipment site of the OEM to the port of landing.
- 5.52.3 All charges such as transportation, logistics, warehousing, security, etc. that may be applicable till the goods are delivered and upon completion of acceptance testing at the respective site of installation shall be borne by the MSI.
- 5.52.4 The MSI during the term of this contract undertakes to ensure that it has taken or shall take up all appropriate insurances for the delivery of goods that it is required to undertake under law as well as to adequately cover its obligations under this Contract: shall take out and maintain, at his own cost insurance with IRDA approved insurers against the risks, and for the coverage, as specified below: shall pay all premium in relation thereto and shall ensure that nothing is done to make such insurance policies void or voidable at the Purchaser's request, shall provide certificate of insurance to the Purchaser showing that such insurance has been taken out and maintained. Employer's liability and workers' compensation insurance in respect of the Personnel of the MSI / MSI s' Team, in accordance with the relevant provisions of the Applicable Law, as well as, with respect to such Personnel, any such life, health, accident, travel or other insurance as may be appropriate; and
- 5.52.5 Insurance against loss of or damage to (i) equipment or assets procured in full or in part for fulfilment of obligations under this Contract (ii) the MSI s' assets and property used in the performance of the Services

## 5.53 Transfer of Ownership

- 5.53.1 The MSI must transfer all goods, clear and unencumbered titles to the assets and goods procured for the purpose of the project to the Purchaser.



## 5.54 Limitation of the MSI's (MSI) Liability towards the Purchaser

- 5.54.1 Except in case of gross negligence, wilful misconduct, breach of Application Laws, breach of representations & warranties and breach of indemnity provisions on the part of the MSI or on the part of any person or company acting on behalf of the MSI in carrying out the Services, the MSI, with respect to damage caused by the MSI to Purchaser's property, shall not be liable to Purchaser
- a. For any indirect or consequential loss or damage; and
  - b. For any direct loss or damage that exceeds the total payments payable under this contract to the MSI hereunder.
- 5.54.2 This limitation of liability shall not affect the MSI's liability, if any, for direct damage to Third Parties resulting in bodily injury, death or damage to physical property caused by the MSI or any person or firm/company acting on behalf of the MSI in carrying out the Services. Notwithstanding anything stated to the contrary in the RFP, Limitation of liability, including for direct damage to Third Parties, shall be to the extent of 100% of the total cost of the project calculated up to and as on the date when such section / clause is required to be invoked.

## 5.55 Conflict of Interest

- 5.55.1 If the MSI / MSI is found to have a conflict of interest that affects the Bidding Process. Any MSI found to have a Conflict of Interest shall be disqualified. In the event of disqualification, CHiPS shall be entitled to forfeit and appropriate the EMD or PBG, for the Damages incurred by CHiPS, as the case may be, without prejudice to any other right or remedy that may be available to CHiPS under the Bidding Documents and/ or the Agreement or otherwise. Without limiting the generality of the above, a MSI shall be deemed to have a Conflict of Interest affecting the Bidding Process, if ("Conflict of Interest"):
- a. The MSI / MSI, its member or Associate (or any constituent thereof) and any other MSI, its member or any Associate thereof (or any constituent thereof) have common controlling shareholders or other ownership interest; provided that this disqualification shall not apply in cases where the direct or indirect shareholding of a MSI, its member or an Associate thereof (or any shareholder thereof having a shareholding of more than 5% (five percent) of the paid up and subscribed share capital of such MSI, member or Associate, as the case may be) in the other MSI, its member or Associate, is less than 5% (five percent) of the subscribed and paid up equity share capital thereof; provided further that this disqualification shall not apply to any ownership by a bank, insurance company, pension fund or a public financial institution referred to in sub-section (72) of section 2 of the Companies Act, 1956/2013. For the purposes of this Clause, indirect shareholding held through one or more intermediate persons shall be computed as follows:
    - i. where any intermediary is controlled by a person through management control or otherwise, the entire shareholding held by such controlled intermediary in any other person (the "Subject Person") shall be taken into account for computing the shareholding of such controlling person in the Subject Person; and
    - ii. subject to Clause 5.55.1.1 (a) above, where a person does not exercise control over an intermediary, which has shareholding in the Subject Person, the computation of indirect shareholding of such person in the Subject Person shall be undertaken on a proportionate basis; provided, however, that no such shareholding shall be reckoned under this Clause, if the shareholding of such person in the intermediary is less than 26% (twenty six percent) of the subscribed and paid up equity shareholding of such intermediary; or
    - iii. a constituent of such MSI is also a constituent of another MSI; or

- iv. such MSI, its member or any Associate thereof receives or has received any direct or indirect subsidy, grant, or subordinated debt from any other MSI, its member or Associate, or has provided any such subsidy, grant, or subordinated debt to any other MSI, its member or any Associate thereof; or
  - v. such MSI has the same legal representative for purposes of this Bid as any other MSI; or
  - vi. such MSI, or any Associate thereof, has a relationship with another MSI, or any Associate thereof, directly or through common third party/ parties, that puts either or both of them in a position to have access to each other's information about, or to influence the Bid of either or each other; or
  - vii. Such MSI or any Associate thereof has participated as a consultant to CHiPS in the preparation of any documents, design or technical specifications of the Project.
- b. The Purchaser requires that the MSI provides services which at all times hold the Purchaser's interests paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The MSI shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of the Purchaser.

## 5.56 Severance

- 5.56.1 In the event any provision of this Contract is held to be invalid or unenforceable under the applicable law, the remaining provisions of this Contract shall remain in full force and effect

## 5.57 Governing Language

- 5.57.1 The Contract shall be written in English language. Subject to Clause 5.61.5 such language versions of the Contract shall govern its interpretation. All correspondence and other documents pertaining to the Contract that are exchanged by parties shall be written in English language only

## 5.58 "No Claim" Certificate

- 5.58.1 The MSI shall not be entitled to make any claim, whatsoever against the Purchaser, under or by virtue of or arising out of, this contract, nor shall the Purchaser entertain or consider any such claim, if made by the MSI after he shall have signed a "No claim" certificate in favour of the Purchaser in such forms as shall be required by the Purchaser after the works are finally accepted.
- 5.58.2 It shall be deemed that by submitting the Bid, the MSI agrees and releases CHiPS, its employees, agents and advisers, irrevocably, unconditionally, fully and finally from any and all liability for claims, losses, damages, costs, expenses or liabilities in any way related to or arising from the exercise of any rights and/ or performance of any obligations hereunder, pursuant hereto and/ or in connection with the Bidding Process and waives, to the fullest extent permitted by Applicable Laws, any and all rights and/ or claims it may have in this respect, whether actual or contingent, whether present or in future.

## 5.59 Publicity

- 5.59.1 The MSI shall not make or permit to be made a public announcement or media release about any aspect of this Contract unless the Purchaser first gives the MSI its written consent.

## 5.60 Force Majeure

- 5.60.1 If, at any time, during the continuance of this contract, the performance in whole or in part by either party of any obligation under this contract is prevented or delayed by reasons of any war or hostility, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts or act of God (hereinafter referred to as events) provided notice of happenings of any such eventuality is given by either party to the other within 21 days from the date of occurrence thereof, neither party shall by reason of such event be entitled to terminate this contract nor shall either party have any claim for damages against other in respect of such non-performance or delay in performance, and deliveries under the contract shall be resumed as soon as practicable after such an event come to an end or cease to exist, and the decision of the Purchaser as to whether the deliveries have been so resumed or not shall be final and conclusive. Further that if the performance in whole or part of any obligation under this contract is prevented or delayed by reasons of any such event for a period exceeding 60 days, either party may, at its option, terminate the contract.
- 5.60.2 Provided, also that if the contract is terminated under this clause, the Purchaser shall be at liberty to take over from the MSI at a price to be fixed by the purchaser, which shall be final, all unused, undamaged and acceptable materials, bought out components and stores in course of manufacture which may be in possession of the MSI at the time of such termination or such portion thereof as the purchaser may deem fit, except such materials, bought out components and stores as the MSI may with the concurrence of the purchaser elect to retain.

## 5.61 General

- 5.61.1 Relationship between the Parties
- Nothing in this Contract constitutes any fiduciary relationship between the Purchaser and MSI/ MSI's Team or any relationship of employer employee, principal and agent, or partnership, between the Purchaser and MSI
  - No Party has any authority to bind the other Party in any manner whatsoever except as agreed under the terms of this Contract
  - The Purchaser has no obligations to the MSI's Team except as agreed under the terms of this Contract
- 5.61.2 No Assignment:** The MSI shall not transfer any interest, right, benefit or obligation under this Contract without the prior written consent of the Purchaser
- 5.61.3 Survival**
- The provisions of the clauses of this Contract in relation to documents, property, Intellectual Property Rights, indemnity, publicity and confidentiality and ownership survive the expiry or termination of this Contract and in relation to confidentiality, the obligations continue to apply unless the Purchaser notifies the MSI of its release from those obligations
- 5.61.4 Entire Contract**
- The terms and conditions laid down in the RFP and all annexure thereto as also the Bid and any attachments/ annexes thereto shall be read in consonance with and form an integral part of this Contract. This Contract supersedes any prior Contract, understanding or representation of the Parties on the subject matter
- 5.61.5 Governing Law and Jurisdiction of Courts**
- The Bidding Process shall be governed by, and construed in accordance with, the laws of India and the Courts in the State of Chhattisgarh, in which CHiPS has its headquarters shall have exclusive jurisdiction over all disputes arising under, pursuant to and/ or in connection with the Bidding Process
- 5.61.6 Jurisdiction of Courts**

- a. The courts of Chhattisgarh shall have exclusive jurisdiction to determine any proceeding in relation to this contract.

**5.61.7 Residuary Governing Rules**

- a. Any matter which has not been covered under these provisions shall be governed as per the provisions of Chhattisgarh State Government Rules and the Applicable Law.

**5.61.8 Compliance with Laws**

- a. The MSI shall comply with the laws in force in India in the course of performing this Contract

**5.61.9 Notices**

- a. A “notice” means:
  - i. A notice; or
  - ii. A consent, approval or other communication required to be in writing under this Contract.
- b. All notices, requests or consents provided for or permitted to be given under this Contract shall be in writing and shall be deemed effectively given when personally delivered or mailed by pre-paid certified/ registered mail, return receipt requested, addressed as follows and shall be deemed received two days after mailing or on the date of delivery if personally delivered:
  - To Purchaser at:  
Chhattisgarh infotech Promotion Society (CHiPS)  
<<Attn: XXXX, XXXX, CHiPS >>  
[Phone:]  
[Fax:]
  - To MSI at:  
Attn:  
[Phone:]  
[Fax:]
- c. Any Party may change the address to which notices are to be directed to it by notice to the other parties in the manner specified above
- d. A notice served on a Representative is taken to be notice to that Representative’s Party

**5.61.10 Waiver**

- a. Any waiver of any provision of this Contract is ineffective unless it is in writing and signed by the Party waiving its rights
- b. A waiver by either Party in respect of a breach of a provision of this Contract by the other Party is not a waiver in respect of any other breach of that or any other provision
- c. The failure of either Party to enforce at any time any of the provisions of this Contract shall not be interpreted as a waiver of such provision

**5.61.11 Modification:** Any modification of this Contract shall be in writing and signed by an authorized representative of each Party

**5.61.12 Application:** These General Conditions shall apply to the extent that provisions in other parts of the Contract do not supersede them

**5.61.13 Overriding Effect:** Notwithstanding anything to the contrary contained in this RFP (including the Annexures), and without prejudice to the obligations of the MSI set out in detail herein (which shall apply in addition to the obligations set out under the Agreement), in the event of a conflict, the detailed terms specified in the Agreement shall have overriding effect over the terms provided hereunder.

**5.61.14 Full Documents:** The MSI shall ensure that all the documents as required under this RFP for evidencing inter-alia its technical capabilities, financial capabilities and eligibility requirements, are submitted by it in full and are not redacted or suppressed in any manner except as required pursuant to the Applicable Law (in which case the MSI shall intimate CHiPS to this effect in writing before submission of the Bid).

5.61.15 RFP - CHiPS Property: This RFP and all other documents attached / annexed / appended / provided herewith, are provided by CHiPS and shall remain (or become upon their coming into existence) the property of CHiPS and are transmitted to the MSIs solely for preparation and the submission of a Bid in accordance herewith.

## 5.62 Exit Management Plan

5.62.1 This clause sets out the provisions which shall apply upon completion of the contract period or upon termination of the contract for default of the MSI. An Exit Management plan shall be furnished by MSI in writing to the Purchaser within 60 days termination of the contract for default of the MSI or before 3 months on completion of the contract period or which shall deal with at least the following aspects of exit management in relation to the contract as a whole and in relation to the Project Implementation and Service Level monitoring.

- a. A detailed program of the transfer process that could be used in conjunction with a Replacement MSI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
- b. Plans for provision of contingent support to Project and Replacement MSI for a reasonable period after transfer.
- c. Exit Management plan in case of normal termination of Contract period
- d. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.
- e. Exit Management plan in case of termination of the MSI

5.62.2 **Exit Management plan** at the minimum adhere to the following:

- a. Three (3) months of the support to Replacement MSI post termination of the Contract
- b. Complete handover of the Planning documents, bill of materials, technical specifications of all equipment, user manuals, guides, IPR, network architecture, change requests, SOPs, details of EOL/EOS of equipment, reports, transfer of ownership of documents/certificates and other relevant items to the Replacement MSI / Purchaser
- c. Certificate of Acceptance from authorized representative of Replacement MSI issued to the MSI on successful completion of handover and knowledge transfer
- d. In the event of termination or expiry of the contract, Project Implementation or Service Level monitoring, both MSI and Purchaser shall comply with the Exit Management Plan.
- e. During the exit management period, the MSI shall use its best efforts to deliver the services.
- f. During the exit management period:
  - i. MSI will allow the CHiPS or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the CHiPS to assess the existing services being delivered;
  - ii. Promptly on reasonable request by the CHiPS, MSI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by MSI or sub-contractors (Only for Non-IT Components) appointed by MSI). The CHiPS shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. MSI shall permit the CHiPS or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by MSI and to assist appropriate knowledge transfer.

- g. MSI will promptly on the commencement of the exit management period supply to the CHiPS or its nominated agency the following:
  - i. Information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services.
  - ii. Documentation relating to Intellectual Property Rights.
  - iii. Documentation relating to sub-contractors(Non-IT Components)
  - iv. All current and updated data as is reasonably required for purposes of CHiPS or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the CHiPS, its nominated agency.
  - v. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable CHiPS or its nominated agencies, or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to CHiPS or its nominated agencies, or its Replacement MSI (as the case may be).
- h. Before the expiry of the exit management period, MSI shall deliver to the CHiPS or its nominated agency all new or updated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that MSI shall be permitted to retain one copy of such materials for archival purposes only.
- i. On request by the CHiPS, MSI shall affect such assignments, transfers, licenses and sub- licenses CHiPS, or its Replacement MSI in relation to any equipment lease, maintenance or service provision agreement between MSI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the CHiPS or its nominated agency or its Replacement MSI.
- j. Promptly on reasonable request at any time during the exit management period, the MSI shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to CHiPS a list of all employees (with job titles and communication address) of the Successful MSI, dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the Successful MSI, CHiPS or Replacement MSI / Nominated Agency / Third party agency.
- k. Vendor may make an offer of contract for services to such employee of the Successful MSI and the Successful MSI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by CHiPS or any Replacement MSI.
- l. General obligations of MSI:
  - i. MSI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the CHiPS or its nominated agency or its Replacement MSI and which MSI has in its possession or control at any time during the exit management period.
  - ii. For the purposes of this Schedule, anything in the possession or control of any MSI, associated entity, or sub- contractor is deemed to be in the possession or control of MSI.
  - iii. MSI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

## 5.63 IT Act 2008

- 5.63.1 Besides the terms and conditions stated in this document, the Contract shall also be governed by the overall acts and guidelines as mentioned in IT Act 2008 (Amendment)

## 5.64 Pre-Contract Integrity Pact

- 5.64.1 A “Pre-Contract Integrity Pact” shall be signed between CHiPS and the MSI. This is a binding agreement between CHiPS and MSIs. Under this Pact, the MSIs agree with the Purchaser to carry out the assignment in a specified manner. The format of Pre-Contract Integrity Pact will be as per Form A.16.
- 5.64.2 The following set of sanctions shall be enforced for any violation by a MSI of its commitments or undertakings under the Integrity Pact:
  - a. Denial or loss of contracts;
  - b. Forfeiture of the EMD and PBG;
  - c. Liability for damages to the MSIs; and
  - d. Debarment of the violator by CHiPS for an appropriate period of time.
- 5.64.3 The MSIs are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behaviour compliance program for the implementation of the code of conduct throughout the company.

## 6. Bid Evaluation

### 6.1 Evaluation Process of Bids

- 6.1.1 A committee/s shall be formed for evaluation of the bids. Decision of the committee would be final and binding upon all the MSIs.
- 6.1.2 The purpose of this section is only to provide the MSI(s) an idea of the evaluation process that the Purchaser may adopt. However, the Purchaser reserves the right to modify the evaluation process at any time during the Tender process, without assigning any reason, whatsoever, and without any requirement of intimating the MSI(s) of any such change.
- 6.1.3 MSI must possess the requisite experience, strength and capabilities in providing the services necessary to meet the Purchaser's requirements, as described in the RFP.
- 6.1.4 MSI must possess the technical know-how and the financial wherewithal that would be required to successfully execute technology refresh including Operations & Maintenance for a period of 5 years of which implementation period is 9 months and O&M period is 4.3 years (for 17 quarters). The MSIs' bid must be complete in all respect and covering the entire scope of work as stipulated in the RFP.
- 6.1.5 The Purchaser shall examine the bids to determine their responsiveness, i.e. whether they are complete, whether the bid format conforms to the RFP requirements, whether any computational errors have been made, whether required EMD and Tender Fee (online) have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.
- 6.1.6 A bid determined as not substantially responsive shall be rejected by the Purchaser and may not subsequently be made responsive by the MSI by correction of the non-conformity.
- 6.1.7 In this part, the bid shall be reviewed for determining the Compliance of the general conditions of the Contract and Technical Bid to the RFP as mentioned in the RFP. Any deviation for general conditions of the Contract and Technical Bid may lead to rejection of the bid at the sole discretion of CHiPS.
- 6.1.8 MSIs are expected to meet all the conditions of the RFP and the Eligibility criteria as mentioned below. MSIs failing to meet these criteria or not submitting requisite supporting documents/ documentary evidence shall not be eligible for evaluation of their Commercial Bid.
- 6.1.9 Commercial bid of only those MSIs who qualify as per eligibility criteria shall be opened.
- 6.1.10 Successful MSI shall be announced based on Least Cost Selection (LCS) Method “L1” and upon proper verification of commercial bid.



## 6.2 Eligibility Criteria & Evaluation

6.1.1. CHiPS shall validate the “RFP Document fee & Bid Security/Earnest Money Deposit (EMD)”. If the contents are as per requirements, CHiPS shall open the “Technical Bid”. Each of the Eligibility criteria mentioned below is MANDATORY. In case, the MSI does not meet any one of the conditions, the MSI shall be disqualified.

6.1.2. MSIs would be informed of their qualification/disqualification based on the Eligibility criteria through Email, Phone and subsequently, the Bid Security amount shall be returned to the respective disqualified MSIs after the submission of Performance Bank Guarantee by the successful MSI.

6.1.3. Criteria for MSI has been provided in the below sections

### Eligibility Criteria for Master Systems Integrator (MSI):

S No.	Type	Eligibility Criteria	Required Documentary Evidence
1	Company Profile	The MSI/Bidder must be incorporated and registered in India under the Indian Companies Act 1956 or 2013, or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for a minimum of <b>five</b> years as on 31.03.2024. The MSI must be registered with appropriate authorities for all applicable statutory duties/taxes.	1. Copy of certificate of Incorporation/Registration under Companies Act 1956/2013 (for Indian companies) 2. Copy of GST certificate 3. Copy of Registration certificate 4. Copy of PAN Card 5. Copy of certificate in case of name change
2	Company Financial Profile	MSI/Bidder must have average annual turnover of at least INR 300 crores from IT/ITES business for last three audited financial years (i.e. FY 2021-22, 2022-23, 2023-24)  And MSI/Bidder should have a positive net worth as on bid submission date.	1. Copy of audited profit and loss account and balance sheet for latest three financial years (FY 2021-22, 2022-23, 2023-24) 2. Certificate from Statutory Auditor with UDIN and stamp for both average annual turnover and positive net worth.
3	Data Centre Experience	MSI/Bidder should have established /implemented Data Centre projects for Central / State Governments, PSUs, PSEs in India in the last <b>five (5) years</b> : a. One project of value INR 80 Crores or more; OR b. Two projects each having minimum value of INR 60 Crores or more; OR c. Three projects each having minimum value of INR 40 Crores or more  The Data Centre project consisting of Supply, Installation, Testing and Commissioning (SITC) of IT components such as server, storage, backup system, network, cyber security equipment for the Data Centre; Non-IT components including installation, commissioning of any of these Electrical Distribution & Lighting, DG sets, Precision AC/Chiller Plant, UPS System, Fire Detection	For on-going projects: 1. Work orders & Agreement highlighting scope of work. 2. Datacentre In progress certificates on the client letter head. 3. Document evidence (Payment advice against invoices) of 50% Payment realization of the total contract value of the project  For completed projects: 1. Work orders & Agreement highlighting scope of work. 2. Datacentre Completion certificates on the client letter head for the completed project also signed by the authorised signatory.



S No.	Type	Eligibility Criteria	Required Documentary Evidence
		& suppression system, Access Control and CCTV, BMS System. <b>Note: Bidder's in-house projects setup will not be considered.</b>	
4	DC/DR on Cloud Hosting Experience	MSI/Bidder should have hosted and implemented Data Centre/ Disaster Recovery Centre on Public/Virtual Private Cloud/Government Community Cloud for Central / State Governments /PSUs/PSEs in India in the last five <b>(5) years</b>  <b>Note: Bidder's in-house projects setup will not be considered.</b>	For on-going projects: 1. Work orders & Agreement highlighting scope of work. 2. Cloud hosting In progress certificates on the client letter head of the projects 3. Document evidence (Payment advice against invoices) of 50% Payment realization of the total contract value.  For completed projects: 1. Work orders & Agreement highlighting scope of work. 2. Cloud Hosting Completion certificates on the client letter head for the completed project also signed by the authorised signatory.
5	Helpdesk and NOC Experience	MSI/Bidder should have experience of setting up and managing NOC operations, Service Desk for Central / State Governments / PSUs /PSEs in India in last 5 years  <b>Note: Bidder's in-house projects setup will not be considered</b>	For on-going projects: 1. Work orders & Agreement highlighting scope of work. 2. In progress certificates on the client letter head of the projects  For completed projects: 1. Work orders & Agreement highlighting scope of work. 2. Completion certificates on the client letter head of the projects/Self-Certificate by the authorised signatory
6	Local Presence	The MSI/Bidder should have an project office in the State of Chhattisgarh or should furnish an undertaking that the same would be established within three month of signing the contract if the project is awarded.	Self-certification duly signed by authorized signatory on company letter head.
7	Key Certifications	The MSI/Bidder shall provide all the three Certifications valid at the time of bidding: <ul style="list-style-type: none"> <li>• ISO 9001:2015 or latest certification</li> <li>• ISO 20000:2018 or latest certification</li> <li>• ISO 27001:2013 or latest certification</li> </ul>	Copies of the valid certificates in the name of the MSI.
8	Undertaking on Blacklisting	As on date of submission of the proposal, the MSI/Bidder, shall not be blacklisted / debarred by any State / Central Government Department or Central /State PSUs/PSEs.	The MSI Undertaking as per the format paced at Annexure 8 for this on company letter head.
9	POA	Furnishing of the Power of Attorney	Power of Attorney executed by the MSI/Bidder in favor of the duly Authorized signatory, certifying

S No.	Type	Eligibility Criteria	Required Documentary Evidence
			him/her as an authorized signatory for the purpose of this Tender.
11	OEM Authorization	The MSI/Bidder should submit valid letter from all the OEMs confirming the following: <ol style="list-style-type: none"> <li>Authorization for MSI Confirm that the products quoted are not “end of life” or “end of sale products”.</li> <li>Undertake that the support including spares, patches for the quoted products shall be available for defined project duration</li> </ol>	Documentary evidence <ol style="list-style-type: none"> <li>Authorization letters on OEM Letter Head and</li> <li>Manufacturer’s Authorization Form (MAF) from all OEMs’ in their Letterhead whose products are being quoted by the MSI need to be attached in the proposal as per format given in the Annexure 14 provided in RFP.</li> </ol>
12	OEM Capabilities	OEM for Server, Storage, Networking, Backup, Security must have direct or registered service partner presence in India.	An undertaking from each OEM on the direct or registered service partner presence in India.

**Important Note:**

MSI/Bidder shall be solely liable to and responsible for all obligations towards the performance of works/services/adherence to SLAs under the contract.

### 6.3 Evaluation of Commercial Bids

- 6.3.1 All the qualified MSIs (Qualified in eligibility and compliant bid) will be notified to participate in the Commercial Bid opening process
- 6.3.2 Evaluation of bids shall be done on Least Cost/Lowest Cost (L1) criteria as detailed. The MSI has to qualify the Eligibility for further evaluation for being eligible for opening of commercial bid. The bids quoted as per the commercial bid format shall be considered for commercial evaluation.
- 6.3.3 The financial bids/ cover of the MSIs who qualify in eligibility criteria shall be opened at the notified time, date and place by the members of the designated Procurement Committee in the presence of the MSIs or their representatives who choose to be present.
- 6.3.4 Prices quoted in the Bid must be firm and final and shall not be subject to any modifications, on any account whatsoever except applicable tax rates. The Bid Prices shall be indicated in Indian Rupees (INR) only.
- 6.3.5 The MSI who shall have the least/lowest cost as per Annexure-12: Commercial Bid Format shall be declared as “L1” and shall be awarded the project. The decision of CHiPS shall be final and binding.
- 6.3.6 Commercial bid shall be evaluated inclusive of all applicable taxes, levies etc
- 6.3.7 If there is no price quoted for certain material or service, the bid shall be declared as disqualified.
- 6.3.8 MSIs quoting unrealistic cost of items shall be rejected summarily by the committee and EMD of such MSI shall be forfeited. Any bid found to have unsatisfactory response in any of the Eligibility criteria as mentioned may be rejected and shall not be considered for further evaluation.

### 6.4 Final Bid Evaluation

- 6.4.1 If any MSI withdraws his bid, at any stage after the last date and time of bid submission till the final evaluation or declaration of the selected MSI, it shall be declared a “defaulting

MSI” and amongst other measures, EMD of such defaulting MSI shall be forfeited. In such situation the tendering process shall be continued with the remaining MSIs as per their ranking.

- 6.4.2 If the MSI declines after being declared as selected MSI, it shall be declared as defaulting MSI and EMD of such defaulting MSI shall be forfeited and CHiPS reserves right to blacklist/debar any such MSI for next 3 Years from participating in any tender floated by CHiPS. In such situation, the tendering process shall be continued with the L2 MSI matching the L1 price. However, in-case of refusal of acceptance by the L2 MSI to match the price of L1 MSI, CHiPS would carry out discussions with the subsequent MSIs.

## 7. Scope of Work

### 7.1 Project Background & Objectives

State Data Centres (SDC) have been identified as one of the important elements of the core infrastructure for supporting e-Governance in the states.

It was proposed to create State Data Centres for the States to consolidate services, applications, and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. These services are being rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as Statewide Area Network (SWAN) and Common Service Centre (CSC) connectivity extended up to village level. State Data Centre would provide many functionalities and some of the key functionalities are Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. SDCs would also provide better operation & management control and minimize overall cost of Data Management, IT Resource Management, Deployment, and other costs.

CHiPS had established Chhattisgarh State Data Centre (CGSDC) for the State in 2013. CHiPS has successfully operated CGSDC since then and provided services to various government departments for running their applications using CGSDC. CHiPS is planning a technology refresh for its existing CGSDC, a State-of-the-Art data Centre designed to provide secure and robust infrastructure to meet the requirements of government departments termed as CGSDC 2.0.

CHiPS also intend to setup the state-of-the-art Network Operations Centre (NOC) monitoring facility at CHIPS Raipur for monitoring, managing and maintaining the CGSDC's network infrastructure for ensuring optimal performance, reliability.

CGSDC 2.0 shall be scalable both vertically and horizontally to address future needs of departments and shall provide stable services to other departments with minimum or no service disruptions.

### 7.2 Details of Existing Setup at CGSDC 1.0

CGSDC1.0, established in 2013 is providing hosting and colocation services to various user departments of Government of Chhattisgarh.

Presently the CGSDC has been established at the office of CHiPS, 1st Floor, State Data Centre Building, Civil Lines, Raipur, Chhattisgarh. The total land allocated for SDC building is 10,000 sq. feet. The total SDC has been setup in an area of approx. 6,162 sq. feet out of which farm area is of 1956 sq. feet with a capacity of 50 racks. For scalability, the 2nd floor of the building

has been designed similar to 1st floor wherein the present data centre is operational and the space in the 2nd floor is being envisaged for setting up of Network Operations Centre.

The SDC building is bifurcated into three (3) Zones as mentioned below:

- Zone A** – This DC Server room area would host servers, server racks, storage racks and Networking component. The area required for Zone A would be approximately 1956 sq feet for CGSDC. It is proposed to have 50 racks in the SFA (Server Farm Area).
- Zone B** – Comprises of NOC & Helpdesk Area room approximately 238 Sq feet, BMS Area 253 Sq ft approximately and Staging Area approximately 293 Sq ft.
- Zone C** – Comprises of room for power panels, AHU, UPS, Fire suppressions, Telecom Room, etc. This zone requires approximately 726 sq. ft. for CGSDC

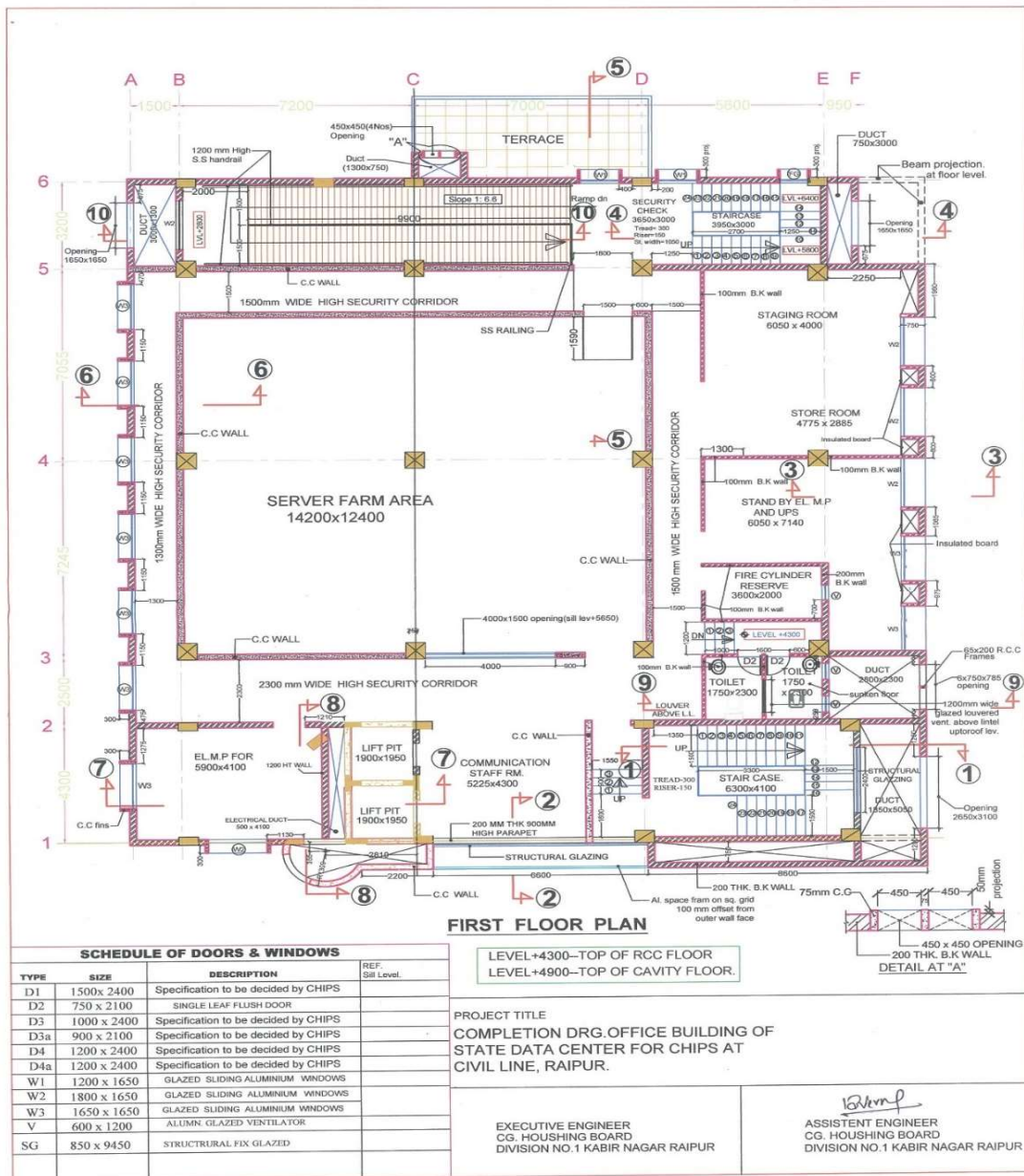




Diagram 1: Layout of First Floor at CGSDC

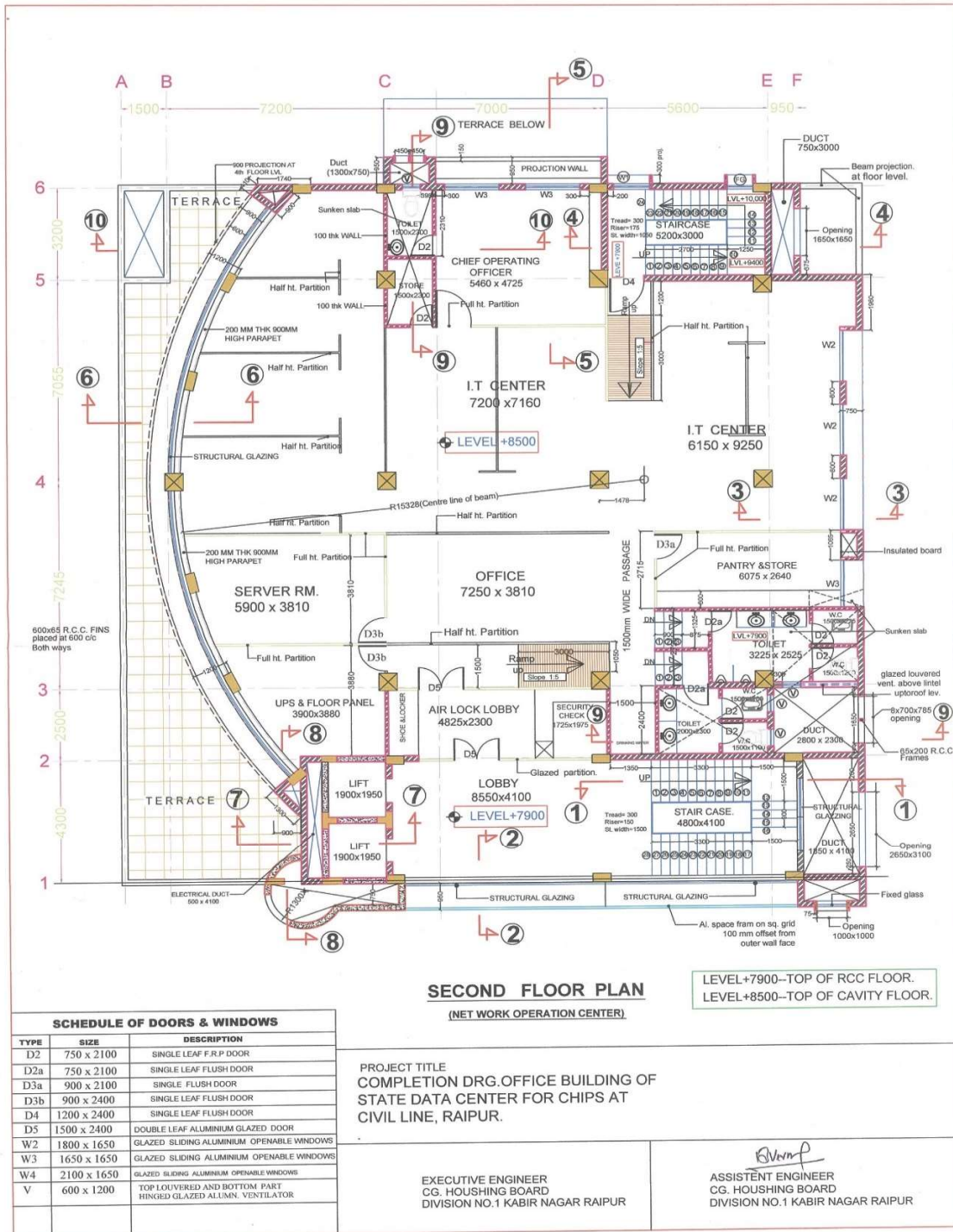


Diagram 2: Layout of Second Floor at CGSDC

### 7.2.1 Existing IT Infrastructure Details

The Primary Data Centre is hosted at the SDC building and the DR for this setup is currently at National Data Centre, New Delhi. The table below provides an overview of the existing IT infrastructure stack at the Primary DC (CGSDC1.0). The existing asset details are provided as a part of Annexure-19 of this document.

Category	Details
<b>Rack Details</b>	
<b>Total Racks</b>	56 (including network, co-location, and hardware racks)
<b>Network Racks</b>	2 (Rack No 1 & Rack No 12)
<b>CHiPS Owned Racks</b>	12
<b>Equipment in CHiPS Racks</b>	26 Servers, 2 Firewalls, 2 NIPS, Enterprise Antivirus, SIEM, switches, etc.
<b>Co-Location Racks</b>	25 (Space, power, BMS provided by CHiPS)
<b>Co-Location &amp; Network Racks</b>	8 (Space, power, BMS, network connectivity, security provided by CHiPS)
<b>Co-Location, Network &amp; Hardware</b>	3 (Space, power, BMS, network connectivity, security, server, storage provided by CHiPS)
<b>Available Rack Space</b>	8 Rack Space
<b>Floor Space for New Racks</b>	Space available for 8 additional racks
<b>Server &amp; Storage Details</b>	
<b>Total Physical Servers</b>	300 (140 Co-Located)
<b>Core Count</b>	3,400
<b>Storage</b>	804 TB HDD
<b>RAM</b>	31 TB
<b>Operating Systems</b>	
<b>Linux Distributions</b>	BOSS Linux 5.0, CentOS 6.8 to 7.4, RHEL 5.3 to 7.7, Ubuntu 22.04.4 LTS
<b>Windows</b>	Server 2003 to 2019 Standard
<b>Virtualization OS</b>	ESXi 5.5 to 6.7.0, XenServer 7.2
<b>Virtual Machines (VMs)</b>	
<b>Total VMs</b>	203
<b>OS Types</b>	CentOS, RHEL, SUSE, Ubuntu, Windows Server 2012 to 2019, ESXi 6.5
<b>Existing Cloud Infrastructure</b>	Setup on 5 servers: 4 compute nodes, 1 management node; running on Sify's Cloud Infinite
<b>Database Servers</b>	MySQL, Oracle, IBM DB2, PostgreSQL, MongoDB
<b>Virtualization Platforms</b>	VMware, Hyper-V, Citrix, RHV
<b>Application Platforms</b>	Apache Tomcat, IIS, Nginx, WebSphere

In the current landscape, the hosting infrastructure is divided into:

**a. CHiPS Owned Hosting Infrastructure:**

This setup has 26 Servers, 2 Firewalls, 2 NIPS, Enterprise Antivirus, SIEM, switches, etc populated in 12 Racks with backbone connectivity of 2 \* 1Gbps links. Most of these

items were purchased in 2012 with warranty up to Feb-2023. The details of the assets including the Serial Number and AMC details are mentioned in the Annexure 19 of this document.

**b. Co-Location Infrastructure:**

This setup has 36 Racks as Colocation Infrastructure hosting servers, storage etc, provided by different user departments

The Colocation Infra is further categorised into three (3) types:

- i. **Pure Colocation:** CHiPS has provisioned only the SDC space, power and Building Management System (BMS) to various other departments. There are a total of 25 racks in this setup. The existing MSI is responsible for supporting services related to power and BMS services only.
- ii. **Colocation with Network:** CHiPS has provisioned the SDC Space, Power, BMS and backbone services like connectivity and network security using SDC's core infrastructure to various departments. There are a total of 8 Racks in this setup. The existing MSI is responsible for supporting services related to power, BMS, backbone connectivity and network & security requirements.
- iii. **Colocation with Network + Hardware:** There are 3 Racks in this setup, Dedicated Server/Storage is also provided. The existing MSI is responsible for supporting these servers and coordinate with their OEM for AMC support.

**c. Cloud Infrastructure:**

Currently the CGSDC has a cloud setup on 5 servers (4 compute nodes and 1 management node) running on Sify's Cloud Infinite.

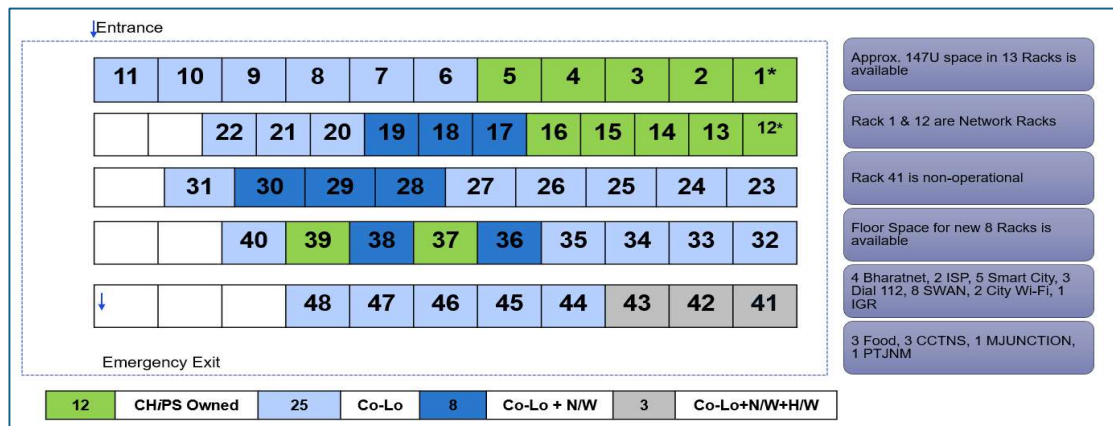
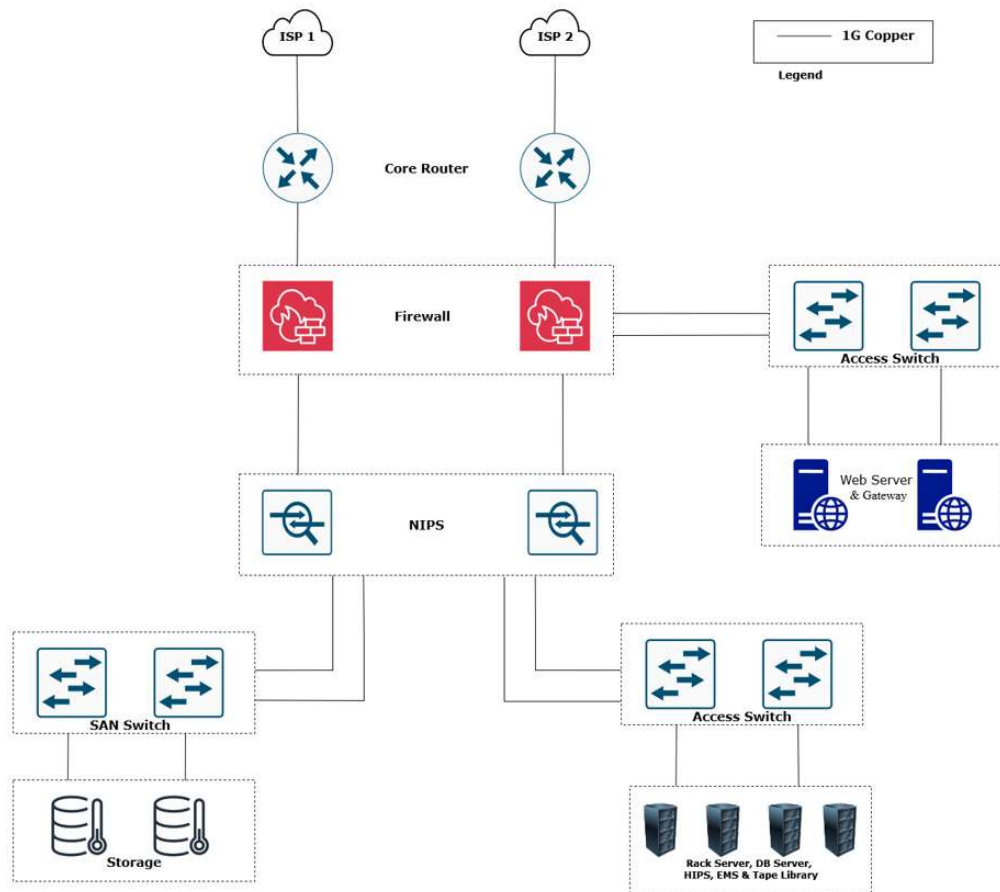


Diagram 3: Existing Rack Layout at CGSDC1.0



Existing high level network architecture diagram of CGSDC

Diagram 4: Existing network architecture for CGSDC1.0 (Indicative)

## 7.2.2 Existing Non-IT Infrastructure Details

The existing Non-IT infrastructure landscape includes DG Set, UPS Systems, Air Conditioning Systems and Building Management System. Additional details are provided as part of Annexure-19 of this document.

Category	Details
<b>Non-IT Infrastructure</b>	
<b>Power Load</b>	1 MW
<b>DG Sets</b>	3 (380 KVA each)
<b>Power Supply</b>	Single Feeder
<b>UPS</b>	2 units of 300 KVA, 2 units of 20 KVA
<b>Precision Air Conditioning (PAC)</b>	20 TR for Server Farm (5 units)
	8.5 TR for UPS & Electrical Room (3 units, including 1 standby)
	2 TR for NOC (2 cassette units: 1 working, 1 standby)
	1.5 TR for Staging Room (1 unit)
	- Additional Cooling for BMS (2 units)
<b>Building Management Systems</b>	<ul style="list-style-type: none"> <li>Fire Detection &amp; Alarm</li> </ul>



Category	Details
	<ul style="list-style-type: none"> <li>• Clean agent gas suppression system</li> <li>• Water Leak Detection System</li> <li>• Very Early Smoke Detection Apparatus (VESDA) solution</li> <li>• Access Control System</li> <li>• CCTV Surveillance System</li> <li>• Public Address System</li> <li>• Rodent Repellent System</li> </ul>

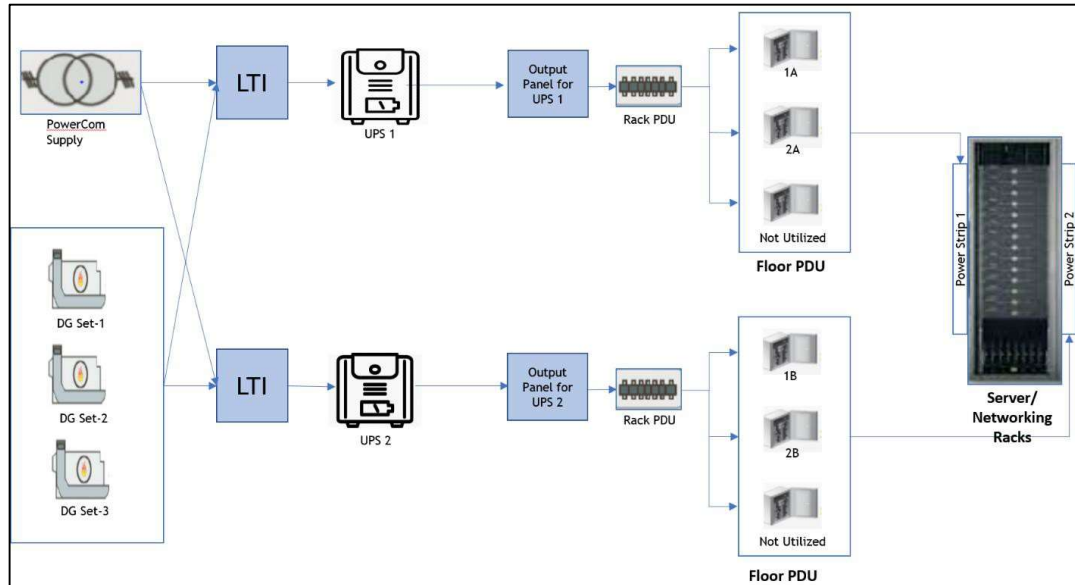


Diagram 5: Existing Electrical Architecture at CGSDC (Indicative)

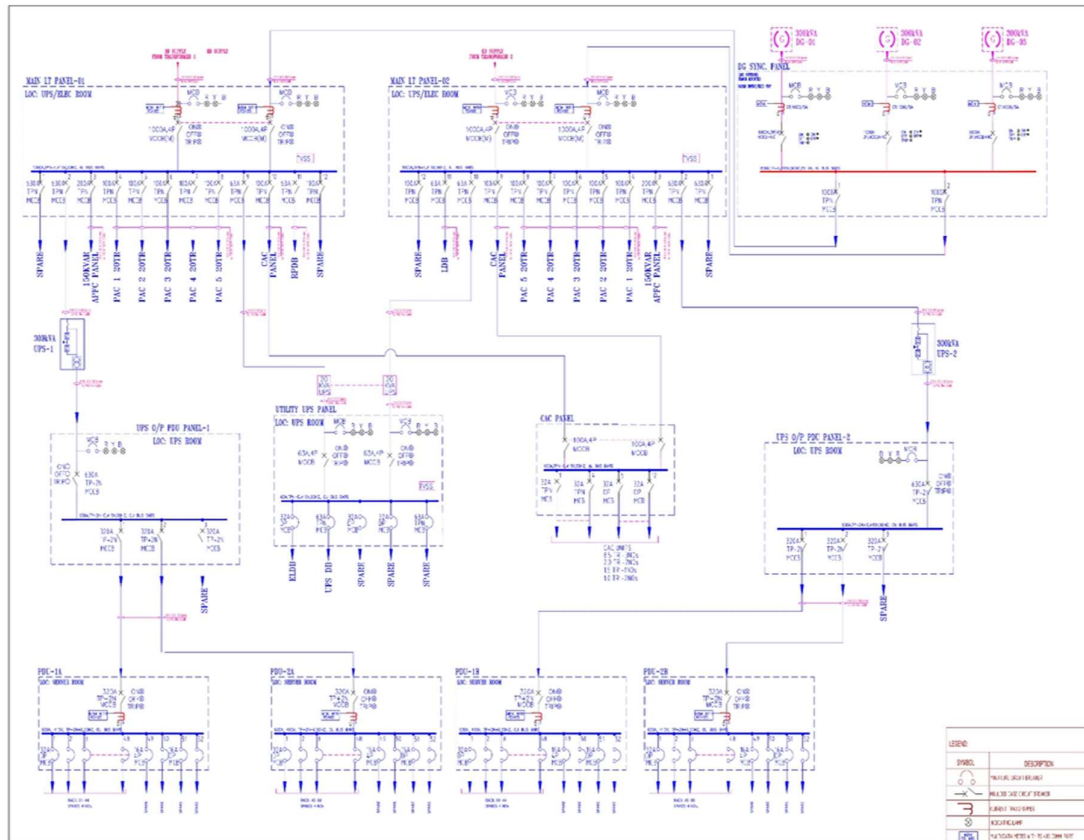


Diagram 6: Existing Electrical Single Line Diagram

## 7.3 CGSDC 2.0 Project Overview

- 7.3.1** CGSDC2.0 is an initiative by CHiPS to undertake a technology refresh of the current State Data Centre. In view of this, CHiPS intends to appoint a Master Systems Integrator (MSI) to manage the existing CGSDC, carry out technology refresh of the IT, Non-IT infrastructure and Civil work including design, supply, install, test, commission of new hardware, software and subsequently carry out Operations & Maintenance for a period of 5 years of which implementation period is 9 months and O&M period is 4.3 years (for 17 quarters). MSI shall also be responsible for establishing a robust Business Continuity Plan by establishing a Disaster Recovery (DR) on MeITY empanelled CSP.
- 7.3.2** MSI shall do the all the necessary investment (hardware, software, manpower, tools and technology etc.) to provide services as per the scope of this RFP. The selected MSI shall ensure an uptime more than 99.98% as per the SLA requirement for a period of contract.
- 7.3.3** Most of the IT infrastructure is at End of Life and will be replaced with the new infrastructure as mentioned in BOQ with the latest state of the art technology as per the design principles mentioned in the RFP by ensuring Planned downtime with prior approval from CHiPS Authority.
- 7.3.4** The overall Scope of Work (SoW) for the MSI to be appointed through this tender includes the following but not limited to.
- Take over the existing IT and Non-IT infrastructure from the existing vendor and provide support until they are migrated to new hardware/software.
  - Supply, installation, configuration, testing and commissioning of compute infrastructure (hardware & software) such as Servers, Operating systems, Virtualization etc.
  - Supply, installation, configuration, testing and commissioning of Network infrastructure like Router, SDN Controller, Spine switch, Leaf switches, Core Switch, SAN Switch,

Router, Access switch, Server Load Balancer, Link Load Balancer including laying, testing and commissioning of inter-rack and intra-rack structured cabling.

- d. Supply, installation, configuration, testing and commissioning of Rack Server, HCI, Virtualisation Software & Manager, Storage, Backup hardware and software, including all the Non-IT components with laying of OFC cables. The installed and commissioned IT infra shall provide minimum 1152 Physical cores, 12,288 GB RAM & total of 1 PB usable capacity for Storage with 500 TB Usable from HCI & 500 TB Usable from enterprise storage.
- e. Supply, installation, configuration, testing and commissioning of Security infrastructure like Next Generation Firewalls, Web Application Firewall, EDR, NDR, HSM, HIPS & DDoS etc.
- f. On premise Service implementation for Virtualization layer, Datacentre Analytics, Patch Management, Antivirus, Backup software and EMS.
- g. Migration of the existing applications and infrastructure from the existing system to the newly procured infrastructure.
- h. Setup Disaster Recovery Site for CGSDC on Cloud infrastructure facilitating seamless integration of cloud services with existing on-premise environment.
- i. Provisioning of 1 GBPS MPLS link between CGSDC and proposed DR on Cloud.
- j. Supply, installation, commissioning and maintenance of Non-IT components such as Electrical substation and power cable, DG Set, HVAC System, AC, Furniture, Fire Alarm, Fire Suppression, Rodent Repellent, Water Leakage detection system, Building Management Systems, Lightning fixtures, Smart TV, Conference room, CCTV, Structure cabling with all passive cables and components etc.
- k. Execution of Civil work which includes but not limited to Cutting and chipping of existing floors, Masonry works, Hardware and metals, Furniture (Chair, Tables Sofa etc), Paint work, False flooring, False ceiling, Storage, Partitioning, Biometric Access Doors and locks, Fireproofing all surfaces, Cement concrete works, Insulation, landscaping, beautification of area, ambient lightning, wall panelling
- l. Setup of State of art Network Operations Centre at the 2nd Floor of the SDC building by conducting a survey and prepare the design and solution for the same.
- m. Setup a centralised Helpdesk to support the CHiPS and other stakeholder department officials in performing their day- to-day functions related to this system.
- n. Supply, Installation, Commissioning of the Non-IT Infrastructure, Civil and interior works pertaining to the DC, NOC and Helpdesk.
- o. Five years on-site comprehensive maintenance and provisioning of services of all the infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance by CHiPS
- p. Onsite support for Data Centre Operations on 24x7x365 by qualified and trained engineers/personnel for a period of five years to ensure more than 99.98% service availability.
- q. Carryout the below mentioned certification of CGSDC within 6 months of Go-Live and ensure that the certifications acquired are current versions available at the time of certification to guarantee compliance with the latest industry standards and best practices. All related cost for the certification with latest version and sustenance during the period the contract will be borne by MSI:
  - i. ISO 27001: Latest
  - ii. ISO 20000: Latest
  - iii. ISO 22301: Latest
- r. Carryout regular drill of backup restoration on sampling basis every month and DR drill activity on half yearly basis as per the agreed backup and business continuity policies with CHiPS.

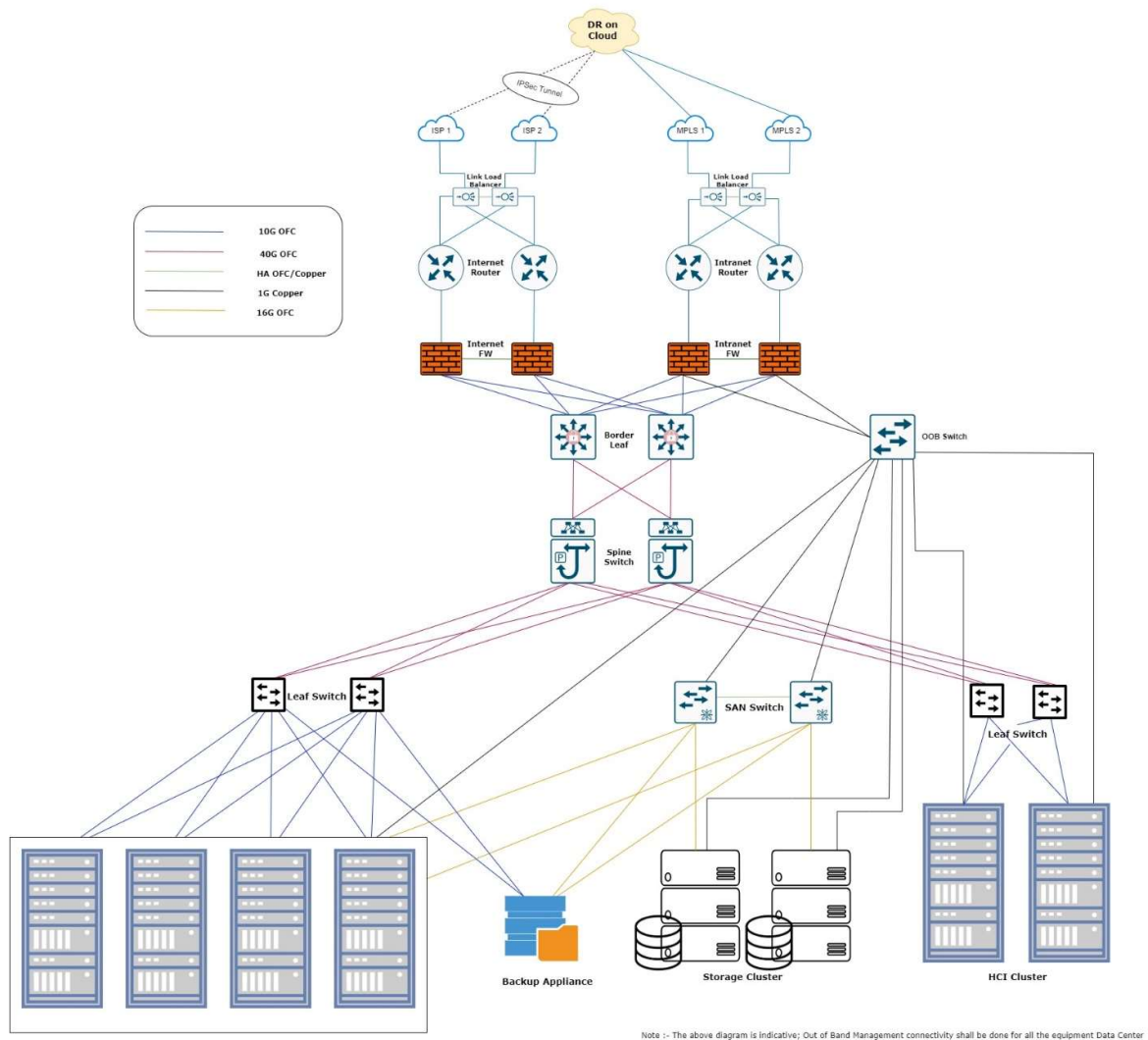
The minimum specified work to be undertaken by the MSI has been categorized as under:

- i. **Schedule I:** Hand over and Take Over of the Existing IT Infrastructure at the CGSDC
- ii. **Schedule II:** Supply, Installation, Configuration, Testing and Commissioning of new hardware, software at CGSDC, Setup of DR on Cloud and Migration to new environment.
- iii. **Schedule III:** Operations and Maintenance services for 4.3 years

Note: The MSIs are requested to submit their proposals for these Schedules in the same bid which would be combined for evaluation purposes.

## 7.4 Design Considerations for CGSDC 2.0

High Level indicative Data Centre architecture for CGSDC2.0 is depicted below



Some of the key considerations for designing the Next Generation Data Centre for CGSDC are given below:

### 7.4.1 Scalability:

- All components of the data centre must support scalability to provide continuous growth to meet the requirements and demand coming in from various user departments.
- A scalable system is one that can handle increasing numbers of requests without adversely affecting the response time and throughput of the system.
- CGSDC2.0 should support both vertical (the growth of computational power within one operating environment) and horizontal scalability (leveraging multiple systems to work together on a common problem in parallel).
- Modular design approach should be adopted for the Data Centre to address growth without major disruptions.

- e. A scalable Data Centre shall easily be expanded or upgraded on demand. Scalability is important because new computing component is constantly being deployed, either to replace legacy component or to support new missions.

#### **7.4.2 Availability:**

- a. All components of the data centre must provide adequate redundancy to ensure high availability of the e-Governance applications and other Data Centre services.
- b. Designing for availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.
- c. The MSI shall make the provision for high availability for all the services of the data centre. However, application availability is the responsibility of the application owner and the MSI cannot be held responsible for any problem related to application and its availability.
- d. The selected bidder shall ensure an uptime more than 99.98% on a quarterly basis for entire duration of the contract. However, application availability on Co-located infrastructure is the responsibility of the application owner and the MSI will not be held responsible for any problem related to application and its availability.

#### **7.4.3 Interoperability:**

- a. The entire system/ subsystem should be interoperable, in order to support information flow and integration.
- b. Operating systems and storage technologies from several vendors must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

#### **7.4.4 Cyber Security:**

- a. The Data Centre must provide an end-to-end security blanket to protect applications, services, data and the infrastructure from intentional, unintentional or malicious attacks or theft from external (through internet) and internal (through intranet and or physical) hackers/malicious intent.
- b. Such attacks and theft should be controlled and well protected using next generation cyber security components e.g. Firewalls, EDR, WAF, NAC systems and infrastructure protection mechanisms.
- c. Furthermore, all the system logs should be properly stored for 6 months & archived for future analysis and forensics whenever desired.

#### **7.4.5 Next Gen Data Centre Functional Requirements for CGSDC2.0**

- a. Consistent services and manageability on physical devices and virtual overlays: Design should support Virtualization from one or more vendors. Consistency in terms of manageability, troubleshooting, and security must be present between different virtual networks and the physical network to help minimize the administrative efforts and eliminate errors.
- b. Visibility: Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between VM to VM, VM to Physical server and vice versa, Leaf to another leaf etc. Should provide pervasive visibility of traffic across the entire data Centre infrastructure, including servers and extending all the way to processes. Should provide complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the network.
- c. Virtualization: CGSDC Fabric must integrate with minimum 3 Virtual Machine Manager of different Hypervisors.
- d. Multi-vendor service integration: Data Centre should have built on the technologies of multiple vendors. It must be verified that infrastructure components (like security, load balancing, virtualization, and storage) from various vendors operate together.
- e. Hyper Converged Infrastructure (HCI) deployment with Minimum of 24 Socket (min. 24 core/Socket) with 500 TB of Usable storage, hypervisor and operating system. Hypervisor & OS shall be same as given with Server modules.

- f. **HCI Scalability:** Any additional node added to the cluster to augment compute/storage capacities the same performance per node. The proposed HCI solution independently scale storage and compute as and when needed without any downtime. HCI should support storage only nodes as well as compute node to extend storage/compute capacity as and when needed. Solution should be capable of adding additional combined server and storage components with high performance GPU capabilities, seamlessly, with no downtime, to scale performance and capacity on demand in future if required by CHiPS.
- g. The Fabric should also provide REST APIs through a Central Management Appliance or an SDN (Software-Defined Networking) Controller. These REST APIs allow integration with third-party tools for:
  - i. **Management:** Integrating with management platforms to control, monitor, and automate the network operations.
  - ii. **Monitoring:** APIs help in monitoring network performance, identifying issues, and analysing traffic patterns.
  - iii. **Virtualisation software integration:** This ensures compatibility with virtualization platforms for better orchestration of virtual machines and network policies.
- h. The backbone connectivity shall be on 40G. The Network Fabric should be built using the Clos Architecture, which should be highly scalable, low-latency network topology. The Clos architecture consists of two main layers:
  - i. **Spine switches:** These are high-performance switches that form the backbone of the network and interconnect with the leaf switches. All data traffic between leaf switches must pass through the spine switches.
  - ii. **Leaf switches:** These are edge switches that connect to devices such as servers, storage, and other network devices. Each leaf switch connects to all spine switches, ensuring high redundancy and fault tolerance.
- i. **Programmability & SDN controller:** DC Fabric must provide open scripting interface from the central management appliance / SDN Controller for configuring the entire fabric. Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol.
- j. Fabric must act as single distributed Layer 2 switch, Layer 3 router and Stateless distributed firewall etc. Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, and Denial of Service. CGSDC2.0 Architecture should provide secure zero-trust using whitelist policy model in a heterogeneous network environment
- k. CGSDC2.0 architecture should provide threat-focused Next-Generation Firewall, IPS with best of breed industry leading stateful firewall with the best of breed threat capabilities such as next-generation intrusion prevention and Advanced Malware Protection, URL filtering (web scanning), application control. **MSI shall ensure that the Next generation Firewall for Internal and External interfaces are from two different OEMs.**
- l. **Storage Infrastructure:** Centralized storage with flexible and secure configuration shall be available in the CGSDC including backup facilities. The following is an indicative list of Components and Software that should be provided as part of this tender scope:
  - i. Enterprise Class Storage System
  - ii. Backup Hardware & Software
- m. **SAN Switching:** The SAN solution should provide highly predictable performance, scalability, Intelligence, and ease of management while protecting customer investment. The proposed switches should provide a best-of-breed solution that can work in multi-protocol FC, FCoE, and IP storage, iSCSI, VSAN and FC over IP [FCIP] environments.

- n. Enterprise Management System (EMS): The EMS system should provide for the regular monitoring, management and reporting of the ICT infrastructure of the Data centre. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS. The EMS system must have the following features including but not limited to:
  - i. Availability Monitoring, Management and Reporting
  - ii. Performance Monitoring, Management and Reporting
  - iii. Securing critical servers using Server based Access Control & recording user activity through audit logs
- o. Entire Solution (all hardware & software) should be IPv6 implementation ready from day one. No extra cost will be borne by CHiPS for IPv6 implementation or future migration from IPv4 to IPv6.
- p. MSI needs to follow ever evolving guidelines listed in the IT Policy, Data Policy, Meity, CERT-In guidelines etc from time to time and ensure adherence during entire contract period.
- q. Structured cabling for entire Data Centre to consider Multimode OM4 fiber cable to provide backbone connectivity between Spine and leaf switches (40G) and between Core & access SAN switches. Connectivity between server/storage to leaf (10/25G) and access SAN switch will also be provisioned on multimode OM4 fiber cable.

## 7.5 Schedule I - Hand Over and Take Over of the Existing IT Infrastructure at the CGSDC

- 7.5.1** MSI should understand, analyse and examine the current state of the CGSDC in discussion and knowledge transfer from the current MSI, Composite Team, Project Consultants, CHiPS and other stakeholders.
- 7.5.2** The process of handover must be seamless without any disruptions to the existing services following the Exit Management Plan agreed and the Hand-Over Take-Over (HOTO) plan approved by CHiPS. The objective is to facilitate a comprehensive handover and takeover of the existing IT and Non-IT infrastructure at the CGSDC, ensuring operational continuity, compliance, and security.
- 7.5.3** The complete handing over taking over (HOTO) activity will be done by the existing MSI to the new MSI as a part of transition activity. The transition period will be maximum of three (3) months as per the agreed HOTO plan. The HOTO activities should be jointly identified by the selected MSI, current SI, CHiPS appointed agency and CHiPS. There will be a team comprising of new and existing service provider for completion of the identified activities.
- 7.5.4** MSI shall conduct a survey of detailed inventory of all IT assets, including servers, network equipment, storage devices, software licenses, and other peripherals by verifying the operational status, configuration, and ownership of each asset.
- 7.5.5** MSI shall take over the existing assets managed by the current MSI and maintain these assets on as-is where-is basis until the completion of successful Go-Live. The details of the existing assets (IT and Non-IT) are provided in Annexure-19.
- 7.5.6** MSI should undertake takeover of equipment and operations from the existing SI with proper due diligence. The overall facilitation and moderation of the HOTO would be the responsibility of CHiPS appointed agency. The CHiPs appointed agency shall apprise and submit completion HOTO reports to CHiPs. The current MSI will provide the following to the selected MSI:
  - a. Current scope of work
  - b. A detailed documentation of the transfer process that could be used in conjunction with a Selected MSI including details to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
  - c. Communication matrix with new MSI, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on DC project's operation as a result of undertaking the transfer.
  - d. Details of provisional support of contingent support to CGSDC project and its selected MSI for a reasonable period after transfer.
  - e. Entitlement for assets to be used by selected MSI for the duration of the exit



management period.

- f. Information relating to the current services rendered and performance data relating to the performance of the services; Documentation relating to CGSDC Project's Intellectual Property Rights for transitioning of the services to successful MSI in a readily available format.
- g. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable the Client and its nominated agencies, or its selected new MSI to carry out due diligence in order to transition the provision of the Services to Client or its nominated agencies, or its replacement Successful MSI (as the case may be).

**7.5.7** The MSI should ensure that no downtime of services is attributed due to takeover. The takeover of CGSDC should include:

- i. Process, Policies & Guidelines
- ii. Inventory & Assets details (IT, Non-IT and Utilities)
- iii. Operations, Maintenance and Management of CGSDC responsibilities
- iv. Data Privacy responsibilities

**7.5.8** MSI shall review and document all infrastructure components, including network architecture, server configurations, storage setups, and security protocols and complete a full handover of Standard Operating Procedures (SOPs), maintenance logs, and incident reports.

**7.5.9** MSI shall perform a thorough security assessment to identify and mitigate any vulnerabilities by reviewing network configurations, including firewalls, VPNs, and access controls, to ensure compliance with security policies.

**7.5.10** Existing MSI shall offer post-handover support for a specified period to resolve any issues and ensure a smooth transition and designate a clear point of contact for ongoing communication and assistance during this period.

**7.5.11** Existing MSI shall provide documentation, including SOPs, network diagrams, security procedures with Training and knowledge transfer report, including contact lists and vendor information for AMC services

**7.5.12** MSI shall ensure successful completion of asset verification, including AMC for hardware. Also full documentation handover and sign-off, certifying the infrastructure is operational and all responsibilities have been transferred.

**7.5.13** The deliverable for completion of this phase would be the a sign off from the new MSI and existing MSI confirming that the HOTO activities are complete along with a HOTO Report.

## **7.6 Schedule II - Supply, Installation, Configuration, Testing and Commissioning of new hardware, software at CGSDC, Setup of DR on Cloud and Migration to new environment**

### **7.6.1 Technology Refresh of CGSDC – IT Infrastructure**

The objective of the technology refresh for CGSDC2.0 is to provide logically unified and shared infrastructure flexible enough to rapidly respond to Infrastructure requirements and accommodate future technology enhancements, distributed applications, database applications running on bare metal, virtualized applications running in multi-virtualisation environments, and cloud-based applications that are available on demand all impose different demands on infrastructure.

There is a need for technology refresh of the existing IT as most of the components have already reached end of life or becoming obsolete. Details of the existing IT and Non-IT assets along with the AMC details are provided as a part of Annexure-19.

The IT infrastructure for CGSDC will require various set of IT components for running their applications. The MSI shall be responsible to Supply, Install, Configure, Test and Maintain the entire solution for the entire duration of the contract.

The table provides only a list of indicative components to be deployed by the MSI as a part of the technology refresh for CGSDC2.0. The MSI shall analyse the requirements carefully and propose any additional components that are deemed necessary for providing the overall solution as a whole to meet the service level requirements.

MSI shall submit the unpriced Bill of Material along with the make and model details of each component proposed as per Annexure-18.

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity
<b>A</b>	<b>IT Components</b>		
1	Rack Server	Nos	12
2	Hyper Converged Infrastructure	Nos	12
3	Virtualisation Software and Management Solution for Rack server Cluster	Nos	1
4	Windows Operating System Data Center Edition - 16 Core License Model	Nos	36
5	Redhat Linux Operating System Enterprise Edition - Socket Based	Nos	12
6	MS SQL Database Enterprise Edition - Core Based	Nos	32
7	Postgres SQL Enterprise Edition - Core Based	Nos	64
8	Backup Hardware & Software (500 TB front end capacity or 500 VM)	Nos	1
9	Server Load Balancer	Nos	2
10	SDN Controller	Nos	2
11	SPINE Switch	Nos	2
12	Leaf switch – OFC	Nos	8
13	Core Router – Internet	Nos	2
14	Core Router – Intranet	Nos	2
15	Management Switch	Nos	2
16	Link Load balancer – Internet	Nos	2
17	Link Load balancer – Intranet	Nos	2
18	L2 Managed Switch for NOC	Nos	2
19	SAN Switch	Nos	2
20	Enterprise Storage (500 TB Usable Storage)	Nos	1
21	Next Generation Firewall – Internet	Nos	2
22	Next Generation Firewall – Intranet	Nos	2
23	Web Application Firewall	Nos	2
24	EDR - Endpoint Detection Response	Nos	500
25	Identity Access Manager	Nos	500
26	Enterprise Monitoring System (NMS, ITSM, ISMS)	Nos	500
27	Network Access Controller	Nos	2
28	HSM - Hardware Security Module	Nos	2
29	HIPS - Host Intrusion Prevention System	Nos	500
30	NDR - Network Detection and Response	Nos	2
31	DDoS	Nos	1
<b>B</b>	<b>Non IT Components</b>		
1	UPS - 300 KVA with battery bank upgradable to 400 KVA	Nos	2
2	Battery Bank for 300 KVA - Min 4 Hrs backup	Lot	1
3	UPS - 20 KVA with Battery Bank	Nos	2

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity
4	Battery Bank for 20 KVA - Min 4 Hrs backup	Lot	1
5	Split AC - 1.5 Ton	Nos	3
6	Split AC - 2 Ton	Nos	2
7	HVAC System - Precision Air Conditioner	Nos	4
8	Biometric Door Access System	Nos	1
9	Smart TV - 55 inch	Nos	4
10	Smart TV - 75 inch	Nos	4
11	Data Center Infrastructure Management (DCIM)	Nos	1
12	Ultrasonic Rodent Repellent System	Nos	1
13	Water Leak Detection System	Nos	1
14	Intelligent Addressable Fire Alarm System	Nos	1
15	Smoke Detection System	Nos	1
16	Fire Suppression System	Nos	1
17	Master Control Unit	Nos	1
18	Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp including substation protection and metering devices	Nos	1
19	42U Rack (Network + Server)	Nos	8
20	DG Set 380 KVA (D Check & Fuel Refilling)	Nos	1
21	Advanced Building Management System (BMS)	Nos	1
22	Structured Cabling	Lot	1
23	Loaded Fiber Enclosure for Type I MPO Cassettes	Lot	1
24	Passive Cabling	Lot	1
25	Fiber Optic solutions for DC Connectivity	Lot	1
26	Fiber Panel	Lot	1
27	CAT6A U/UTP Cable	Lot	1
28	24 Port Patch Panel loaded	Lot	1
29	CAT6 I/O for loaded Patch Panel	Lot	1
30	CAT6A Patch Cord	Lot	1
31	MFZ Verifocal Dome	Nos	24
32	Bullet Camera	Nos	2
33	PTZ Camera	Nos	2
34	Power Cables	Lot	1
<b>C</b>	<b>Civil &amp; Interior</b>		
1	One time Site Preparation (Civil & Electrical) Cost for DC including complete site preparation of Data Center, inclusive but not limited to false flooring, lighting fixture, electrical works, Mason Works, Dismantling existing Wall, Doors, Window or any structure of any material etc(Refer Scope of Work for further details)	Lot	1
2	EARTHING: Preparation of All Earth Pits, Necessary Repair, Testing earth resistivity and electrode resistance	Lot	1
3	Electrical works - for NOC, DC, DG Set UPS and LT Panel	Lot	1
4	Setting up of state of the art NOC room with required Furniture and other components including false flooring, lighting fixture, electrical works, beautifications of NOC area, wall panels, Mason Works, etc. (Refer Scope of Work for further details)	Lot	1
<b>D</b>	<b>One time cost of setting up Connectivity</b>		

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity
1	Provisioning 1 GBPS MPLS Connectivity	Lumpsum	1
<b>E</b>	<b>Data Centre latest Certifications</b>		
1	ISO 27001, ISO 20000, ISO 22301 and Surveillance Audit including Recertification	Lumpsum	1

The MSI should also consider the following while proposing the solution:

- a. The MSI should ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to the devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
- b. The technical compliance requirements are provided as a part of Annexure-17 o
- c. CHiPS will not be responsible if the MSI has not provisioned for any components, sub-components, assemblies, sub-assemblies as part of bill of material in the bid. The MSI will have to provision to meet the solution requirements, the same at no additional cost and time implications to CHiPS.
- d. The MSI should ensure there is a 24 x 7 x 365 comprehensive onsite support arrangement for the duration of contract with all the OEMs for respective IT components.
- e. It is expected that MSI and OEM shall ensure that the equipment/components being supplied by him will not be declared "End of Support Life" for minimum 7 years from date of bid submission. If the same is de-supported by the OEM for any reason whatsoever, the MSI shall replace it with an equivalent or better substitute that is acceptable to Purchaser without any additional cost to the Purchaser and without impacting the performance of the solution in any manner whatsoever. Any components, sub-components, assemblies, sub-assemblies (i.e. server, storage, OS) required for installation of EMS, backup, patch management, antivirus or any other software/management software needed for Data Centre IT infrastructure will be provided by MSI without any additional cost.

#### **7.6.2 Non-IT Infrastructure, Civil and Interior Work Requirements for CGSDC2.0**

#### **7.6.3 Non-IT Infrastructure**

##### **a. Power Distribution and Substation System**

The MSI shall be responsible for management of Power Distribution and Substation system for proper and uninterrupted working at the premises. MSI shall ensure this by having the Data centre and NOC power distribution system with redundancy:

- i. Two incoming 11KV HT feeder supply from two different source for DC and SDC building. MSI shall ensure both feeders will be automatic switchover with help of sync panel.
- ii. Two different power panels at secondary side of transformer. One power panel (switchgear) will feed to Data centre and the other power panel (switchgear) will feed to rest of building load requirements.
- iii. Emergency Diesel- Generator backup on failure of both main feeders
- iv. MSI shall submit the health check report of existing DG Set (380KVA) – 3 Nos

- v. MSI shall also conduct D Check on the existing DG Sets (three (3) nos. of 380 KVA) including and including installation of diesel theft mechanism.
- vi. AMC, Health checkup, preventive maintenance and support in checking for any loose connection in lugs or any components.
- vii. All Electrical Panel deep cleaning and connection tightness check.
- viii. MSI has to refill the diesel as and when required. Re-imbursement of Diesel expenditure will be done on actuals at every quarter-end based upon the consumption report verified by officials/Agency authorized by CHiPS.
- ix. The electrical work shall include the following
  - a. Main electrical panel
  - b. Power cabling
  - c. UPS distribution board
  - d. UPS point wiring
  - e. Power cabling for utility component and utility points etc.
  - f. Online UPS
  - g. Replacement of HT and metering panel, cables.
  - h. Transformer, APFC panel, Sync panels (Transformer output Panel)
  - i. SITC of Main and sub-LT panels.
  - j. Distribution panels and DBs
  - k. Lighting and wiring
  - l. Earthing and Grounding
  - m. Diesel generators, exhaust stack, HSD tank, Fuel pump etc.
  - n. UPS systems upgradable upto 400KVA with lithium-ion batteries for IT load, Noncritical UPS with all cabling, raceways, cable trays, tagging, connectors, terminations
  - o. Any other work not explicitly mentioned above but required to complete the project.
- x. The MSI shall use fire retardant cables of rated capacity exceeding the power requirements of existing and proposed components to be used at maximum capacity.
- xi. All materials to conform to IS standards as per industry practice
- xii. OEM certificate (Manufacturer Authorisation) are Mandatory for following items
  - 1. HT panel (Panel manufacturer)
  - 2. LT panel (Panel manufacturer)
  - 3. Transformer
  - 4. UPS systems with Batteries

**b. UPS requirements and features DC and NOC**

MSI shall Supply of UPS system with battery bank for critical loads to provide a redundant power supply to the following needs:

- i. Connection between UPS system and the network and Server racks shall be redundant. No single point of failure shall exist in the power connectivity between network racks and UPS system.
- ii. Access control, Fire Detection & suppression system and surveillance system
- iii. Old battery bank shall be replaced with lithium ion battery

The system shall be automatic with power supply from the mains and automatic switchover to DG set as secondary source for the Data centre.

**c. Air Conditioning and Natural Convection NOC**

Since Data Centre is a critical area, precision air conditioning system shall be exclusively installed to maintain the required temperature. The A/C shall be capable of providing sensible

cooling capacities at ambient temperature and humidity with adequate air flow. The task of the MSI shall include (but not limited to):

- i. Connecting the indoor unit with the mains electrical point
- ii. Connecting indoor and outdoor units mechanically (with 18 G hard gauge copper piping)
- iii. Connecting indoor and outdoor unit electrically

The air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage.

**d. HVAC system**

- i. The server farm is proposed to have 8 racks where each rack size is considered to be 800mm x 1200 mm.
- ii. All the perimeter PAC units if required for maintaining temperature Delta at server farm (MSI may propose if required), are suggested to be placed on one side (façade side).
- iii. All the refrigerant piping must run on the side of the wall below the raise floor and go out of the facility to the ODU platform.
- iv. Pipes have to be properly insulated. The exit of the pipes on the wall has to be through factory made sealing material.
- v. Adequate safety barriers must be taken care of on the platform on all sides.
- vi. Humidifier line can be taken from building water pipeline with a valve.
- vii. MSI must submit a detail table of selection of various rating of indoor units with its cooling capacity in terms of CFM, power consumption and size.
- viii. MSI must consider the equipment heat load, room area load and latent heat for selection of rating of the units.
- ix. All the AC units must have provisions to connect to DCIM. It must also be connected to the fire alarm system.

**e. Fire Detection and Suppression System for DC and NOC**

- i. The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards.
- ii. The facility is to be equipped with gas based (Suitable for Data centre environments) fire suppression system appropriately sized for the given size of the Data centre.

**f. Access control system for DC and NOC**

The Biometric/Access card-based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble connected with BMS system. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.

**g. CCTV system for DC and NOC**

The MSI shall provide CCTV system within the Data centre and Network operation centre on 24X7 bases. All-important areas of the Data centre, NOC along with the non-critical areas like locations for DG sets, Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations. The recordings shall be stored for a minimum of 30 days, after

which they may be archived. MSI is responsible for provisioning all required cables and accessories to ensure proper system functionality.

**h. Water leak detection system DC and NOC**

The Water Leak Detection System shall be installed to detect any seepage of water into the critical area and alert the security control room for such leakage. It shall consist of water leak detection cable and alarm module. The cable shall be installed in the ceiling and floor areas around the periphery.

**i. Advanced Building Management system DC and NOC**

The Building Management System (BMS) shall be implemented for effective management, monitoring and integration of various components like Access Control System, fire detection system etc.

The BMS shall perform the following general functions including but not limited to:

- i. Advanced Building Management and control
- ii. Data collection and archival
- iii. Alarm event and management
- iv. Trending
- v. Reports and MIS generation
- vi. Maintenance and complaint management

**j. Rodent Repellent DC and NOC**

The entry of rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However, the MSI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

**k. Data Centre Structured Cabling**

Data Center structured cabling involves following activities:

- i. Supply, installation, testing and commissioning of all fiber/copper panels, Network/Server Rack dressing, laying of cables (Copper STP & Fibre), terminations at both end and other passive components for all 8 Racks.
- ii. Cable laying will be through metal raceways, PVC conduits, overhead ladder / tray and other relevant activities.
- iii. Laying of STP copper Cable in raceways includes proper bunching and tagging for different Cables including colour coding. (if required)
- iv. Preliminary continuity Testing & Ferruling at both end for each cable unique identity.
- v. Termination, Installation, Fixing of Port Jack Panels including proper Dressing of Cables. Proper routing of Patch Cords in Racks, Jack Panels and wire/ cable manager with tagging of Mounting Cords.
- vi. Network rack shall be with proper cable management, Ladder, Vertical & Horizontal Wire Manager etc.
- vii. Fibre termination and Management System and Fibre routing also has to be included in the scope.
- viii. OLTS Scanning of laid Copper/Fibre Cables for the performance testing of Installed Cabling System with EIA/TIA specified parameters.
- ix. Cabling system shall include factory-terminated system components which can be quickly mated to form an end-to-end optical link between patching locations and/or equipment ports.

- x. Cabling system shall be a modular solution and should offer a greater degree of flexibility in managing equipment moves, adds or changes.
- xi. MSI shall submit the certificate from fibre glass OEM stating bend insensitive glass is supplied for all the cables in this project and attenuation report of fibre core used.
- xii. Fibre cable & jumper shall have OM4 fibre with bend insensitive fibre Trunk cable and jumper.
- xiii. There should be 25-year product warranty and Application Assurance for passive components.
- xiv. Cables should have no joints or splices; all foil should necessarily be grounded at all terminations.
- xv. Under no circumstance hand labelling of the cables will be accepted, No hand punching shall be allowed without proper tools Labelling and Punching should be done as per TIA/EIA standards.
- xvi. Any cable that does not meet TIA/EIA specifications should be repaired or replaced at the MSI's expense.
- xvii. Each outlet shall be tested for satisfactory operation based on certification parameters valid for the entire warranty period of 25 years or more as applicable.
- xviii. All outlets in the Facility be clearly marked, labelled & documented for future reference.
- xix. Maintenance of the LAN Passive components shall be done by the MSI Provision of additional Passive nodes whenever required shall need to be provided based on requests.
- xx. Cable layout plan should be submitted as part of the technical bid.

#### **7.6.4 Civil and Interior Works in DC and NOC**

The scope of MSI for civil work is to furnish the Data Centre and NOC in all aspects strictly in consultation and approval of CHiPS. MSI shall ensure that all material selection and layout plan shall be approved by CHiPS. MSI shall submit detailed BoQ required for completion of work. Given scope of work is indicative but not limited, MSI shall carry out a survey of the existing layout and prepare the design & solution and take the necessary approval from CHiPS authority.

The furnishing includes but not limited to the following:

- a. Cutting and chipping of existing floors
- b. Masonry works
- c. Hardware and metals
- d. Furniture (Chair, Tables, Sofa etc)
- e. Lightening fixtures
- f. Paint work
- g. False flooring
- h. False ceiling
- i. Storage Cabinets
- j. Partitioning
- k. Biometric Access Doors and locks
- l. Fireproofing all surfaces
- m. Cement concrete works
- n. Insulation

All material to be used shall be of fine quality ISI marked unless otherwise specified.

The Government encourages making the built environment truly accessible and inclusive for persons with disabilities. Accordingly, the built environment should be in accordance with the National Building Code (NBC) of India 2016 including Part 3, Section 13 of NBC 2016.



The furnishing includes but not limited to the following:

- a. Cutting and chipping of existing floors
- b. Masonry works
- c. Hardware and metals
- d. Furniture (Chair, Tables, Sofa etc)
- e. Lightening fixtures
- f. Paint work
- g. False flooring
- h. False ceiling
- i. Storage Cabinets
- j. Partitioning
- k. Biometric Access Doors and locks
- l. Fireproofing all surfaces
- m. Cement concrete works
- n. Insulation

All material to be used shall be of fine quality ISI marked unless otherwise specified. The Government encourages making the built environment truly accessible and inclusive for persons with disabilities. Accordingly, the built environment should be in accordance with the National Building Code (NBC) of India 2016 including Part 3, Section 13 of NBC 2016.

**a. Interior design and finishing**

Interior and civil works includes all partition installations, loose furniture and accessories, Ramps, rolling shutters, grill partition and doors, ergonomic chairs, tables, interior landscaping, beautification, painting, and other wall finishes, with waterproofing where required, Modular false ceiling, raise flooring inside server hall, Vitrified/Marble tile flooring tile carpet flooring in NOC area (appx >5000 sq ft), PCC flooring on all area if required.

NOC Room Table/Desk/console: Furniture required for NOC Setup:

- i. The table top height should allow operators to sit and work comfortably. The table width per operator must be sufficient to accommodate two 25-inch monitors while providing ample workspace for additional tasks.
- ii. The console finish shall be resistant to rubbing and liquids, impact-proof and easy to clean, All Board Cladding (Laminates) must be 1MM & the Laminate supplier must be Green Guard Certified, Certificates of which must be provided.
- iii. Standard top height of modular control desk shall be 750 mm. The Console Tabletop / Working Surface should be made in 26mm Laminated MDF Board with PU Nosing. The Side Panels should be fixed type, made in 26mm MDF Board Cladded on 18mm MDF Board. All panels must be attached to the frame with concealed fasteners. Console access panels (Front & Rear Panels) must be removable without the use of tools. The Front panel should be positioned in such a way that there should be sufficient leg space (min of 450 – 500 mm from the front edge
- iv. NOC room Chair: NOC room chair must ergonomically designed in such a manner that long hour seating does not become tiring. The minimum requirement of chair is as follows.

1. Wheel Based
  2. Mid Back Chair
  3. Mesh Back & Silver Epoxy Backbone
  4. 2-Way Adjustable Armrest
  5. Gas lift for Seat height adjustment
- v. Conference room table: Conference room table must be for 8 seater with provisions for power and data outlets. The top surface of the table must be water spill proof and smooth finish with matching laminate. The colour and design will be decided by CHiPS prior to the delivery by the bidder. Conference room shall be equipped with sound and visual equipment, smart screens.
  - vi. Storage: There has to be storage cabinets on all cabins, conference rooms, BMS room, Reception, Storeroom etc. All storage cabinets must be 2 ft depth and width as required.
  - vii. Office area Furniture: Office area furniture should be modular type. This bidder must select the furniture which has to be factory made. All modular desks must have cable management system and raceways concealed inside the desk.
  - viii. Cabin Desk/Table: Each cabin will have a table for the officer who will use this for day work purpose. The top surface must be made of MDF / Commercial board with laminate for a smooth finish. A side table with 3 drawers, a computer stand, bookshelf etc
  - ix. Reception Table: Reception table must be selected by allowing CHiPS to make choices from the available options by the bidder. The table must be for seating of 2 people with adequate size. it must have provisions for power and data point with concealed cable management system.
  - x. Shoe Rack: A shoe rack must be supplied with 20 pair of slippers to be placed near the entrance of the server room.
  - xi. Toilet interiors with faucets, fitting, wall and floor tiles plumbing and all scope to make the work complete.
  - xii. Installation of electrical wiring and sockets for workstations, raceways, cable trays, earthing systems, floor distribution boards, UPS systems, UPS panels, lighting.
  - xiii. Installation of complete lighting and air-conditioning systems, along with all necessary electrical wiring.
  - xiv. Installation of addressable multi-sensor detectors, fire hydrant, detector cabling, fire panels, access control systems and wiring, CCTV systems, camera cabling, public address (PA) systems, fire exit doors, Fire rated glass partition, Toughened glass partition, Gypsum partition Fire rated doors, Glass doors and flush doors, Shutters, Grills.
  - xv. Each workstation will be equipped with two data points for CAT6 LAN cabling.

**b. False Ceiling DC and NOC**

The MSI shall install the top false ceiling. This false ceiling shall house A/C ducts (if required) and cables of electrical lighting, firefighting, and CCTV. Appropriate pest control measures shall be taken to keep pests at bay.

**c. Raised flooring DC and NOC**

The MSI shall be responsible for raised flooring and provide for suitable pedestal and under structure designed to withstand various static and rolling loads subjected to it in server racks. The entire raised floor shall have laminated floor covering and beadings on all sides of the panel.

### 7.6.5 Setting up of State-of-Art Network Operations Centre and Helpdesk

- i. MSI will be responsible for conducting a comprehensive survey to establish a state-of-the-art Data Centre Network Operations Centre (NOC) on the second floor of the CGSDC building. Refer Section 7.2. – Layout of Second Floor of SDC building. The successful MSI is required to perform this survey to identify the necessary requirements and develop a proposed design and solution for the NOC, as outlined in this tender document and the scope of work.
- ii. NOC solution setup for CGSDC shall support CHiPS's network operations, network monitoring, and incident response capabilities. This setup aims to ensure continuous network performance, effective threat detection, incident response, and enhanced operational resilience.
- iii. NOC setup will be responsible for monitoring, managing, and maintaining network infrastructure to ensure optimal performance and availability.
- iv. NOC setup shall support 24x7 monitoring of network devices, servers, and infrastructure for optimal performance and uptime.
- v. Rapid detection, diagnosis, and resolution of network and security incidents, with root cause analysis and documentation.
- vi. Regular review of network performance metrics for optimization and capacity planning.
- vii. Monitoring and reporting on key performance indicators to ensure compliance with defined SLAs.
- viii. Maintenance of network asset configurations and timely application of updates and patches.
- ix. Development and testing of disaster recovery plans for network resilience.
- x. Solution with automation capabilities and a unified dashboard for streamlined NOC management.
- xi. Detailed staffing plan for 24/7 coverage, including training and knowledge transfer for continuous improvement.
- xii. Response times, uptime commitments, and escalation procedures with regular reporting.
- xiii. The help desk service will serve as a single point of contact for all incidents and service requests at the CHiPS Raipur. The service will provide a Single Point of Contact (SPOC) and also escalation / closure of incidents for the user. The activities shall include:
- xiv. Managing Help Desk facility during service period window for reporting user department incidents / issues / problems with the IT and non-IT infrastructure.
- xv. Provide and manage necessary channels for reporting issues to the help desk. MSI shall provision facility access to access helpdesk locally as well as publicly as per need of CHiPS.
- xvi. The incident reporting channels could be the following: Specific E-Mail account, Telephone Line, Portal for Ticketing & incident reporting
- xvii. Management of a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls and assign an incident/ call ID number.
- xviii. Creation of knowledge base on frequently asked questions to assist user in resolving basic issues themselves.
- xix. Track each incident / call to resolution
- xx. Provide feedback to callers.
- xxi. Analyse the call statistics
- xxii. Creation of knowledge base on frequently asked questions to aid users.
- xxiii. Continuous monitoring of the IT & Non-IT infrastructure at both DC & DR to ensure availability as per agreed SLAs.

- xxiv. Monitoring shall be done with the help of monitoring tools and system logs/counters and therefore the reports and alerts can be auto generated.
- xxv. Escalate the calls, to the appropriate levels, if necessary, as per the escalation matrix agreed between the MSI and the department. The escalation matrix shall be developed by the MSI in discussion with the CHiPS.
- xxvi. Coordinate with respective team/users for closure of calls.
  - a. Analyse the incident / call statistics and provide monthly reports including but not limited to:
  - b. Type of incidents / calls logged
  - c. Incidents / calls resolved
  - d. Incidents / calls open
  - e. Maintaining up to date details.

#### **7.6.6 DR on Cloud**

- i. The MSI shall be responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of Chhattisgarh State Data Centre (CHiPS Raipur) and meet the RPO and RTO requirements
- ii. The CSP selected by MSI should be MeITY empanelled. MSI shall ensure that compliance in terms of empanelment of the selected CSP is valid throughout the project tenure. In case of termination of empanelment of the selected CSP by MeITY, the MSI shall ensure that an alternate empanelled CSP is onboarded without any additional cost to CHiPS and that the migration to the new CSP is seamless.
- iii. The DR shall be physically located in India. The proposed Data Center for DR should be at least 100 KM away from current State Data Centre.
- iv. The DR Solution shall be on Active (DC) – Standby mode.
- v. The proposed requirement for DR will be 40% of DC and can be changed later by the CHiPS as per requirement
- vi. All the components mentioned will follow Pay as you go pricing model on actual consumption
- vii. The quantity and configuration of the service requested may vary in future, and the bidder needs to make the provision for accommodating the same
- viii. CHiPS is not bound to avail all the services mentioned in the list (Annexure 12)
- ix. RPO/RTO requirement of application shall be as 15 Min RPO & 4 Hrs RTO
- x. MSI shall meet the above mentioned RPO/RTO for entire contract duration. However, during the change from Primary DC to DR on cloud or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DR on cloud and the MSI shall be responsible for sizing and providing the DC-DR replication link to meet the RTO and the RPO requirements.
- xi. MSI shall also factor in requisite replication tool, hardware & software required for CGSDC and DR on Cloud replication based on the solutions deployed at CGSDC. MSI shall be responsible for ensuring compatibility of the solutions between DC and DR.
- xii. MSI shall also ensure and procure required number of virtualisation software and management licenses for the rack server cluster.
- xiii. The Primary DC (CGSDC) and the DR on cloud should be in different seismic zones. During normal operations, the Primary Data Centre will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the Cloud solution offered. The application environment shall be installed and ready for use. Cloud DR Database/Storage shall be replicated asynchronously and shall be available in full as per designed RTO/RPO and replication strategy.

- xiv. In the event of a site failover or switchover, DR site shall take over the active role, and all requests shall be routed through DR site. Application data and application states will be replicated between data centres so that when an outage occurs, failover to the surviving data Centre can be accomplished within the specified RPO/RTO
- xv. During any failover or DR drill compute environment for the application shall be equivalent to DC or as configured for DR & bandwidth at the DR shall be scaled to the level of data centre requirement. Users of application should be routed seamlessly from DC site to DR site.
- xvi. Till a disaster (planned/ testing or otherwise) is declared by CHiPS, the users should not be allowed to access the IT applications from DR site (or as per discretion of department).
- xvii. The MSI shall conduct DR drill on a half yearly basis wherein the Primary DC has to be deactivated and complete/partial operations shall be carried out from the DR Site. However, during the change from DC to DR or vice-versa (regular planned changes), there should not be any data loss.
- xviii. MSI has to demonstrate one successful DR drill before Go-Live.
- xix. The MSI shall clearly define the procedure for announcing DR based on the proposed DR Cloud solution. The MSI shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR.
- xx. The MSI shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill. The CSP should offer dashboard to monitor RPO and RTO of each application and database.
- xxi. The MSI should offer switchover and switchback of individual applications instead of entire system. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.
- xxii. MSI shall provide access of web console/dashboard to monitor the SLA and availability of resources.
- xxiii. MSI shall provide 1 Gbps MPLS link/bandwidth connectivity between CGSDC and CSP DC where DR is proposed to be hosted with unlimited upload and download of data. MSI shall ensure that the traffic shall be encrypted.
- xxiv. MSI shall be responsible for provisioning, securing, monitoring, and maintaining the hardware, network(s), and software that support the infrastructure and present Virtual Machines (VMs) and IT resources to the CHiPS. MSI shall be responsible for the security of the “guest” Operating System (OS) and any additional software including the applications running on the guest OS.
- xxv. In case, the CSP provides some of the System Software as a Service for the project, CSP shall be responsible for securing, monitoring, and maintaining the System and any supporting software.
- xxvi. MSI should ensure base minimum security in data & network or likewise which shall include data & network security, Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, Integrated Vulnerability Assessment, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting. MSI shall also meet any new security requirements as specified by CERT-In (<http://www.cert-in.org.in/>)
- xxvii. Compliance to Cloud Security ISO Standard ISO 27017:2015, Privacy Standard ISO 27018:2014
- xxviii. Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.
- xxix. Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes should be in a separate zone with higher security layer.

- xxx. There should be sufficient compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement) during any unanticipated spikes in the user load.
- xxxi. Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures..
- xxxii. CSP shall not provision any unmanaged VMs for the applications.
- xxxiii. Should adhere to the ever evolving guidelines as specified by CERT-IN (<http://www.cert-in.org.in/>)
- xxxiv. Should adhere to the relevant standards published (or to be published) by MeitY or any standards body setup / recognized by Government of India and notified to the CSP by MeitY as a mandatory standard.
- xxxv. MSI shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.
- xxxvi. The empanelled cloud service offerings must comply with the additional guidelines / standards (applicable for the Empanelled Cloud Service Offerings) as and when such guidelines / standards are published by MeitY at no additional cost to retain the empanelment status.
- xxxvii. MSI shall provide a self-service/orchestration platform so that CHiPS team can provision IT resources like virtual machines, storage volume, archival data as they required

#### **7.6.7 Installation and Configuration of the Commissioned ICT Infrastructure**

The MSI would be required to undertake pre-installation planning at the Data Centre including but not limited to Rack planning, structured cabling, SAN cabling, power points, etc. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS.

The MSI shall be responsible for the delivery, installation testing and commissioning of the servers, storage, network, security, orchestration, EMS and related equipment in the Data Centre. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS.

- a. The MSI shall carry out the planning and layout design for the placement of equipment in the provisioned Data Centre. The plan and layout design should be developed in a manner so as to optimally and efficiently use the resources and facilities being provisioned at the Data Centre. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS.
- b. The plan and design documents thus developed shall be submitted to CHiPS for approval and the acceptance would be obtained prior to commencement of installation.
- c. The MSI shall carry out installation of equipment in accordance with plans and layout design as approved by the CHiPS or its Third Party Agency.

#### **7.6.8 Migration to the new IT Infrastructure**

- a. MSI is expected to carry out all the activities pertaining to migration to the new infrastructure to the planned CGSDC2.0. The activities will include (but not limited to):
  - i. Maintaining a dust-free environment in the DC during civil and electrical work and shall clean the site daily before leaving
  - ii. Providing a detailed migration plan covering all aspects such as Civil, Electrical, passive, and active related activities
  - iii. Data migration from existing storage to new storage.
  - iv. Application migration in coordination with application owners / departments and under the guidance or approval of CHiPS and user departments (if any)
  - v. Migration of Servers, network and security stack and other necessary items based on business requirement with minimal downtime as possible.

- b. The scope of MSI is only the migration and management of the physical infrastructure and provides facilitation to the Application owner. Application will be migrated by individual application owner. However, MSI shall extend required support to the application teams while carrying out this activity.
- c. The MSI shall have to ensure that required dependencies along with their associated items are met and/or are included in their solution for the said application migration to CGSDC 2.0. However, Application enhancement will not be the responsibility of the MSI.
- d. MSI shall ensure that all the data migration is done from existing systems to the new infrastructure.
- e. MSI shall be responsible for safeguarding the data integrity during the migration process. Appropriate measures, risk & mitigation shall be documented by MSI in details and discussed with CHiPs and CHiPs appointed agency.
- f. In the case of heterogeneous migrations, MSI is obligated to manage and execute the transition of data and services between disparate systems with meticulous attention to detail. This includes ensuring compatibility and maintaining operational continuity throughout the migration process.
- g. MSI must develop and maintain a detailed fallback plan as well as a rollback plan to swiftly address and rectify any issues that may occur during the migration. These plans must be designed to minimize service disruption and must be executed in coordination with the CHiPS and CHiPs appointed agency to ensure a smooth transition to the updated data center and cloud services infrastructure.

#### **7.6.9 Commissioning & Acceptance of the Equipment**

##### **a. Commissioning of System.**

- i. The MSI should submit in advance the tests and details of the process that will be adopted to demonstrate the correct working of the equipment supplied both individually and as an integrated system. The acceptance testing plan (equipment wise) will be validated by CHiPS / their appointed Third party agency and agreed before commencing the Acceptance testing
- ii. System testing schedules, formats for testing and commissioning reports and dissemination mechanism for such reports shall be drawn by The MSI in consultation with CHiPS / their appointed Third party agency.
- iii. It shall be the responsibility of the MSI to get pre-despatch inspection of the goods and furnish necessary certificate to CHiPS certifying that the goods conform to the specifications in the proposed bill of material and are in line with the mandatory Technical specifications as specified in Annexure 17 – Technical Specifications of this Tender.
- iv. Commissioning of the solution shall be complete only after the following conditions have been met successfully to the satisfaction of CHiPS.
- v. Successful completion of Final Acceptance Tests and submission of necessary reports and certificates to CHiPS.
- vi. Delivery of all the items under the proposed bill of material at the designated locations of installation. Short shipment of goods will not be acceptable.
- vii. Installation and Configuration of all the components of the solutions including, but not limited to, hardware, software, devices, accessories, etc. to the satisfaction of CHiPS.
- viii. Successful completion of Commissioning would need to be certified by CHiPS and operations shall commence only after approval of CHiPS.

**b. Final Acceptance Testing of System**

- i. The final acceptance shall cover testing of 100% of the components and solutions proposed a part of CGSDC2.0. Upon completion of successful testing by CHiPS or its third-party agency; a Final Acceptance Test Certificate (FAT) and Go-Live certificate shall be issued by CHiPS.
- ii. Prerequisite for carrying out FAT activity:
  - a. Detailed test plan, formats and schedules, shall be defined by MSI in consultation and agreement with CHiPS and its appointed Third Party agency. This shall be submitted before FAT activity is to be carried out.
  - b. All documentation, artefacts related to CGSDC2.0 and relevant acceptance test document should be completed & submitted before the final acceptance test to CHiPS.
- iii. The FAT shall include the following:
  - a. All the IT, Non-IT hardware / software, civil work, interiors must be installed at CGSDC site as per the specifications, scope of work and RFP terms and conditions
  - b. Integration of all the solutions proposed as a part of the RFP
  - c. Demonstration of all the features / facilities / functionalities as mentioned in the RFP.

**7.7 Schedule III – Operations & Maintenance for contract period for IT and Non-IT Infrastructure.**

The following is the summary of operations and maintenance services to be provided by the MSI:

- a. The MSI shall provide comprehensive onsite support to CHiPS on a 24 x 7 x 365 basis to ensure an uptime of 99.98% for the ICT infrastructure solution at the Data Centre in accordance with the Service Level Agreement mentioned as part of this tender.
- b. The MSI shall commit to provide all necessary manpower resources onsite to resolve any issues/incidents and carry out required changes, optimizations and modification.
- c. The MSI shall assign onsite manpower resources on a 24 x 7 x 365 basis to diagnose, troubleshoot and resolve issues related to the Data Centre services. The onsite support staff should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning, etc. The MSI shall also provision for necessary offsite support to ensure continuity of operations for CHiPS.
- d. The MSI shall provide comprehensive technical support services for all the hardware and software proposed for the entire period of the contract. The technical support should include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.
- e. The MSI shall provide comprehensive onsite warranty on a 24 x 7 x 365 basis for the entire period of contract of all IT and Non-IT infrastructure provided as part of scope of this tender.
- f. The contract period for the Operation and Maintenance might be extended as per provision in clause 5.38.
- g. Besides the IT and Non-IT infrastructure procured for CGSDC as part of this RFP, MSI shall be responsible for supporting services related to power, BMS, backbone connectivity and network & security requirements for the infrastructure hosted by other government departments in the colocation environment. The three types of



hosting environment is provided in Section 7.2 of the RFP. The MSI shall provide 24x7x365 onsite support to such infrastructure also.

- h. The MSI shall provide all necessary training to the CHiPS officials (approx. 10) for successful functioning of the Data Centre operation and management.
- i. The MSI should ensure that the entire IT Infrastructure solution is operational in accordance with the stipulated service standards in Service Level Agreement.
- j. The MSI along with all the associated OEMs should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and modification to ensure that the IT infrastructure is operational in accordance with the stipulated service standards in Service Level Agreement.
- k. The onsite technical support should also include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.
- l. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS and its appointed third-party agency

#### **7.7.1 Ongoing Operations and Maintenance Services**

The MSI would be responsible for managing and maintaining the Data Centre operations on a 24x7x365 basis. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS. Ongoing operations and maintenance of the Data Centre shall comprise of the following activities in conjunction with the indicative features required by the centralized management system as specified:

##### **a. Technical Support**

The onsite Technical team will be responsible for the resolution of all IT infrastructure related issues / problems. The technical support desk shall undertake the following activities:

- i. Log issues / complaints related to IT and Non-IT infrastructure at the Data Centre and issue an ID number against the issue / complaint.
- ii. Assign severity level to each issue / complaint to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels
- iii. Track each issue / complaint to resolution
- iv. Escalate the issues / complaints, to CHiPS officials if necessary as per the escalation matrix defined in discussion with CHiPS.
- v. Analyze the issue / complaint statistics and MSI's SLA
- vi. Should provision for all necessary channels for reporting issues to onsite technical team.
- vii. The incident reporting channels will be the following: Email, Telephone (mobile phone alerts), Web Based
- viii. Should implement a call logging system in line with the severity levels as mentioned in the SLA

##### **b. System Maintenance and Management**

Certain minimum deliverables sought from the MSI with regards to System Maintenance and Management are provided below: -

- i. The MSI shall be responsible for tasks including but not limited to setting up servers, HCI systems configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting

tasks, and executing hardware and software updates when necessary. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS.

- ii. The MSI shall provision skilled and experienced manpower resources to administer and manage the entire IT Infrastructure solution at CGSDC.
- iii. On an ongoing basis, the MSI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
- iv. The MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.
- v. The MSI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with CHiPS and based on the industry best practices / frameworks. The MSI shall also create and maintain adequate documentation / checklists for the same.
- vi. The MSI shall be responsible for managing the usernames, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc.
- vii. The MSI shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy formulated in discussion with CHiPS and based on the industry best practices / latest frameworks like ISO 27001, ISO 20000, ISO 22301 etc.
- viii. The administrators will also be required to have experience in latest technologies like Orchestration, virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario

### **c. System Administration**

Certain minimum deliverables sought from the MSI with regards to System Administration are provided below:

- i. 24\*7\*365 monitoring and management of the servers in the Data Center.
- ii. The MSI shall ensure proper configuration of server parameters. The MSI shall be the single point of accountability for all hardware maintenance and support the IT infrastructure at the Data Centre. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS
- iii. The MSI shall be responsible for Operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.
- iv. The MSI shall also be responsible for installation and re-installation in the event of system crash/failures.
- v. The MSI shall appoint system administrators to regularly monitor and maintain a log of the monitored servers to ensure their availability of such logs as required.
- vi. The MSI shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators should also ensure that the logs are backed up and truncated at regular intervals. The

MSIs are advised to refer CERT-In Guidelines so as to ensure their alignment with the practices followed.

- vii. The system administrators should adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.
- viii. The system administrators should provide hardening of servers in line with the defined security policies
- ix. The system administrators should provide integration and user support on all supported servers, data storage systems etc.
- x. The system administrators should provide directory services such as local LDAP services and DNS services and user support on all supported servers, data storage systems etc.
- xi. The system administrators will be required to trouble shoot problems with web services, application software, desktop/server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
- xii. Documentation regarding configuration of all servers, IT Infrastructure etc.
- xiii. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.
- xiv. The administrators will also be required to have experience in latest technologies like Orchestration, virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement-based scenario.

#### **d. Storage Administration**

Certain minimum deliverables sought from the MSI with regards to Storage Administration are provided below:-

- i. The MSI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric / switches. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS.
- ii. The MSI shall be responsible for storage management, including but not limited to management of space, SAN volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc
- iii. CHiPS would additionally remotely manage the storage system and components and appropriate setup should be provided by the MSI.
- iv. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
- v. The storage administrator will be required to create/delete, enable/disable zones in the storage solution
- vi. The storage administrator will be required to create/delete/modify storage volumes in the storage solution
- vii. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution
- viii. To facilitate scalability of solution wherever required.

- ix. The administrators will also be required to have experience in latest technologies like virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement-based scenario.

**e. Database Administration**

MSI shall be responsible for monitoring database availability and performance, changing the database logical structure to embody the requirements of new and changed programs.

- i. The MSI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.
- ii. The MSI shall be responsible for tuning of the relational database, ensuring the integrity of the data and configuring the data dictionary.
- iii. The MSI shall be responsible for testing and installing new database software releases, if any.

**f. Backup / Restore**

The MSI shall be responsible for backup of storage as per the policies of CHiPS at the Data Centre. These policies would be discussed with MSI at the time of installation and configuration. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS.

- i. The MSI shall be responsible for monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies
- ii. The MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by CHiPS or in case of upgrades and configuration changes to the system.
- iii. The MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. The MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
- iv. The administrators shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fireproof cabinets (onsite and offsite).
- v. The MSI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

**g. Network monitoring**

The MSI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the MSI will be under the supervision of CHiPS

- i. The MSI shall be responsible for monitoring and administering the network within the Data Centre up to the integration points with WAN. The MSI will be required to provide network related services for routers, switches, load balancer services etc.
- ii. The MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
- iii. The MSI shall be responsible for the break fix maintenance of the LAN cabling or maintenance work requiring civil work.

#### **h. Information Security Monitoring and Management**

The MSI shall provide services (monitoring and management) of all the security related infrastructure systems related to information security. Management of this environment in order to ensure confidentiality, integrity, availability and non-repudiation of the services on a 24 x 7 basis. It should be noted that the activities performed by the MSI will be under the supervision of CHIPS. The team will be required to provide monitoring and management of activities including but not limited to the following:-

#### **i. Patch Management**

The MSI will be required to provide services related to Patch Management. The security administrators should be aware of security precautions in place in their environment. The patch management should be executed efficiently for all kinds of environments like for operating systems and Data bases.

#### **j. Vulnerability Assessment**

MSI will be required to undertake Vulnerability Assessment as per the agreed Security policy and Cert-In guideline. The activities performed should be included but not limited to the following:

Vulnerability Assessment will span for the following core areas:

- OS level vulnerability assessment:
  - i. To provide proper evaluation of security vulnerabilities associated with operating systems deployed in CGSDC2.0 environment thereby, recommending solutions to problems and implementing the same,
- Database Vulnerability assessment:
  - ii. To provide proper evaluation of security vulnerabilities associated with database—Microsoft SQL Server, and Postgres, deployed in CGSDC2.0 environment thereby recommending solutions to problems and implementing the same.

Vulnerability Assessment will include checks like Port scan, unnecessary or vulnerable services, file permission, user access control, password protection, system vulnerability etc.

#### **k. OS Hardening**

OS Hardening will include activities but not limited to the removal of all non-essential tools, utilities, and services with other system administration by activating & configuring all appropriate security features. The entire scope of this service will differ on different Operating System basis. Most of the Windows based Operating Systems will include following activities in conjunction to CHIPS OS hardening guidelines:

- a. Broad category:
  - i. User Account Management
  - ii. Access Control Management
  - iii. Configuration and supporting processes
  - iv. System logging and auditing.
  - v. Network and environmental variables.
- b. A preview on the activities associated with Broad categories:
  - i. Identifying unused or unnecessary ports.
  - ii. Disable/Shut down/remove unused and unnecessary services and daemons.
  - iii. Removing rogue connections: wireless and dial-up.
  - iv. Setting up filters for malicious content for each OS.
  - v. Test Backup and restoring procedures.
  - vi. Account Policies: Password policy, Account lockout policy etc.
  - vii. Local server Policies: Audit policies, User rights assignments, security options etc.

- viii. Event logs settings
- ix. System services
- x. Registry settings
- xi. File & Folder permissions

#### **I. Penetration Testing**

The Penetration Testing will include activities but not limited to the test should simulate activities in conjunction to CHIPS cyber security and Cert-In guidelines. These activities should identify specific exploitable vulnerabilities and expose potential entryways to vital or sensitive data. The results should clearly articulate security issues and recommendations and create a compelling event for the entire management team to support a security program.

A complete project-based approach should be followed that covers areas including but not limited to the following:

- a. Network Security
- b. Network Surveying
- c. Port Scanning
- d. System Identification
- e. Services Identification
- f. Vulnerability Research & Verification
- g. Router Testing
- h. Firewall Testing
- i. Intrusion Detection System Testing
- j. Trusted Systems Testing
- k. Password Cracking
- l. Denial of Service Testing
- m. Containment Measures Testing

#### **7.7.2 Other Key Operations and Maintenance Activities**

- a. The MSI should provide round-the-clock monitoring of systems, networks, and applications in data Centres and cloud environments. This includes real-time tracking of CPU utilization, memory usage, storage capacity, and other performance metrics, with alerts for threshold breaches.
- b. Proposals should include a comprehensive incident management plan detailing how the MSI will identify, log, and resolve incidents. The MSI should also perform root cause analysis on recurring issues to prevent future incidents, documenting findings and solutions.
- c. The MSI should conduct regular assessments of the DC and cloud resources to ensure they can meet both current and projected demands. For cloud environments, the MSI should propose strategies for resource optimization to manage costs effectively while maintaining high performance.
- d. The MSI must regularly apply updates and patches to software, firmware, and operating systems within the data Centre and cloud environments. The proposal should include a patch management schedule and a protocol for addressing urgent vulnerabilities as they arise.
- e. The MSI should outline a strategy for regular data backups and an associated disaster recovery plan, ensuring data integrity and availability. The disaster recovery plan should be tested periodically, with documentation of testing procedures, results, and improvements.
- f. Proposals should include a security management plan that covers continuous threat monitoring, vulnerability scanning, and the application of security best practices. The vendor should provide regular security audits, implement access controls, and maintain robust endpoint protection measures.
- g. The MSI should implement a structured change management process to control modifications to systems, software, and configurations in both data Centres and cloud environments. The proposal

should include details on the change request process, impact analysis, scheduling, and documentation.

- h. The MSI must ensure that data Centre and cloud operations comply with relevant industry standards and regulations, such as ISO 27001, DPDP. Proposals should describe the approach to regular audits, documentation practices, and how compliance adherence will be maintained.
- i. The proposal should also include a reporting plan, specifying the frequency, format, and content of regular performance and incident reports.
- j. The MSI is expected to maintain comprehensive and up-to-date documentation of all systems, configurations, and resources. This includes network diagrams, inventory lists, system configurations, and process documentation.
- k. The proposal should include a plan for training internal staff on system operations, updates, and new features. Regular knowledge transfer sessions are expected to ensure that internal teams are equipped to manage routine tasks and understand the operational framework.
- l. The MSI should identify and implement opportunities for efficiency improvements on an ongoing basis, including energy usage optimization in data Centres, cost management in cloud environments, and general performance enhancements.
- m. The MSI should describe a preventive maintenance schedule to ensure all systems, hardware, and infrastructure components remain in optimal condition. This may include hardware inspections, cooling system checks, and testing of backup power systems in data Centres.
- n. Proposals should address how the vendor will ensure the scalability of both data Centre and cloud resources. This should include considerations for future upgrades, expansions, and the ability to accommodate new technologies as they become relevant.
- o. The MSI must ensure Continuous monitoring of connectivity links between the data Centre and cloud to ensure reliable and uninterrupted data flow, with alerts for any connectivity issues that may impact operations.
- p. The MSI must ensure regular testing and maintenance of redundant connections and failover mechanisms to ensure that backup pathways are functional, minimizing potential downtime during primary link failures.
- q. The MSI must ensure Routine security assessments on connectivity links, including encryption verification and compliance checks, to maintain data integrity and meet regulatory standards for data transmission between the data Centre and cloud.

### **7.7.3 Reporting Requirement**

MSI shall submit the reports on a regular basis in an approved format by CHiPS. The following is only an indicative list of MIS reports that shall be submitted by SI to CHiPS and any designated agency by CHiPS. Any other report required in any desired format by CHiPS, the SI shall be responsible to share the same as per the frequency desired.

#### **a. Daily Reports:**

- i. Summary of issues / complaints logged at the Help Desk
- ii. Summary of resolved, unresolved and escalated issues / complaints
- iii. Log of backup and restoration undertaken.
- iv. Log of DC/DR replication
- v. Log of IPv4 & IPv6 dual stack nodes
- vi. Application monitoring report which will cover underlying infrastructure, application middle ware, Operating System and licenses along with their utilization through an online dashboard

#### **b. Weekly Reports:**

- i. Issues / Complaints Analysis report for virus calls, call trend, call history, etc.
- ii. Summary of systems rebooted.

- iii. Summary of issues / complaints logged with the OEMs.
- iv. Inventory of spare parts in the DC & DR.
- v. Summary of changes undertaken in the DC & DR including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc.

**c. Monthly Reports:**

- i. Component wise IT & Non-IT infrastructure availability and resource utilization
- ii. Consolidated SLA / (non)- conformance report.
- iii. Summary of component wise DC & DR uptime.
- iv. Summary of changes in the DC & DR.
- v. Logs of preventive / scheduled maintenance undertaken
- vi. Logs of break-fix maintenance undertaken
- vii. Report Software licenses usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the CGSDC.

**d. Quarterly Reports:**

- i. Consolidated component-wise physical and IT infrastructure availability and resource utilization.

**e. Half Yearly Reports:**

- i. DC & DR Security Audit Report
- ii. IT infrastructure Upgrade / Obsolescence Report

**f. Incident Reporting:**

- i. Detection of security vulnerability with the available solutions / workarounds for fixing.
- ii. Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems
- iii. Software license violations

**Please Note:-**

- i. MIS and SLA Reports shall be provided by the MSI via automated tool in dashboard
- ii. The above give reports are indicative, the MSI may have to provide additional reports as per the requirements of the CGSDC and CHIPS.

## 7.8 Data Centre Certifications

MSI shall be responsible for obtaining the following latest certifications within six (6) months from Go-Live and all related cost for the certification will be borne by MSI. MSI shall be responsible for any renewals of the certification within the contract period.

- i. ISO 27001: Latest
- ii. ISO 20000: Latest
- iii. ISO 22301: Latest

Cost of sustenance audit for above certification shall be responsibility of the MSI for the entire contract period.

MSI shall also be responsible for documentation for CGSDC2.0's ISO 27001, ISO 20000 & ISO 22301 certification framework and further certification from concerned authorities. Therefore, it shall be the



responsibility of the MSI to assess the CGSDC 2.0 project from its inception for implementation of ISO frameworks as and when required until the contract duration.

MSI shall be responsible for preparing policy, procedure, frameworks and implementation to fulfil the requirement of said audits.

## 7.9 OEM Obligations

### 7.9.1 Deployment Phase

- a. Each OEM should be involved in Planning, Designing, and final acceptance to make sure that proposed solution should work seamlessly as per tender requirements.
- b. Bidder should provide the overall program management and OEMs to ensure that the solution, which may include multiple technologies from various OEM, to work together seamlessly as per the proposed solution design. The seamless integration with all devices would be OEM responsibility for their respective products offered.
- c. After completion of the deployment, OEMs to validate the design and certify the design meets industry best practices.
- d. Each OEM to assign SPOC during implementation phase.
- e. Upon successful commissioning and completion of acceptance testing activities, MSI shall ensure comprehensive handover and knowledge transfer from the OEMs for operational and management responsibilities

### 7.9.2 Support Phase

- a. The MSI should further ensure that a robust support model is put together along with OEM in such a way that the data center runs with the level of availability it is designed for and with a predictable restoration time in case of any failures.

## 7.10 Manpower Deployment

The MSI shall deploy relevant manpower at for managing Data Centre and to meet the desired SLAs during entire contract period. The domain wise list of minimum indicative Manpower to be deployed under the project is given below table. However, MSI shall deploy additional manpower if required to meet the desired SLA and timelines at no extra cost to the purchaser during entire contract period.

The deployed resources shall be required to operate from the Data Centre mentioned in the RFP. The schedule of the sitting arrangement shall be finalized by the tendering authority. The shift schedule and sitting arrangement may be changed as per the requirement during entire contract period by the Department.

### 7.10.1 Manpower Deployment – HOTO and Installation and Commissioning Phase (9-Months)

S.No.	Manpower	Quantity
1	Project Manager - Technical	1
2	System Administrator- Windows/Linux	2
3	HCI Administrator	1
4	Database Administrator	1
5	Security Administrator	1
6	Storage Administrator	1
7	Core Network Engineer	2
8	Backup Administrator	1
9	Server Administrator	1
10	Cloud Expert (Hybrid)	2
11	BMS Expert	1

**7.10.2 Manpower Deployment – Operation and Maintenance Phase (51 Months / 17 Quarters)**

S.No.	Manpower Role	General Shift (9:00 AM to 6:00 PM)
1	Project Manager - Technical	1
2	System Administrator- Windows/Linux - Level 2	2
3	HCI Administrator	1
4	Database Administrator	1
5	Security Administrator	2
6	Storage Administrator	1
7	Core Network Engineer	2
8	Backup Administrator	1
9	Server Administrator	1
10	Cloud Expert (Hybrid)	2
11	NOC Engineer	1
12	Helpdesk Support Engineer	1
13	BMS Expert	1

#### 7.10.3 Minimum Manpower in other shifts

S.No.	Manpower Role	Shift IInd (3:00 PM to 12:00 AM)	Shift IIIrd (12:00 AM to 9:00 AM)
1	Helpdesk Support Engineer	1	1
2	NOC Engineer	1	1

#### 7.10.4 Manpower Criteria

MSI shall highlight the details required below for the key resources proposed in the CV format as per Annexure-09

Sl. No.	Position	Mandatory Qualification
1.	Project Manager	Mandatory: Educational Qualification in BE / B. Tech / M.Tech from recognised Institute, with PGDM/ MBA from recognised Institute. a. Certification in PMP/ Prince2 Practitioner: b. Minimum 15 Years' Experience, out of which, 5 years in the capacity of Project/Program Manager in ICT implementation and Datacentre projects c. Minimum 5 Years' Experience of Project of Data Centre Implementation / O&M d. Minimum 1 Year Experience in managing Cloud Service Project
2.	Cloud Expert (Hybrid)	Mandatory: Educational Qualification in BE / B. Tech / MCA and 5+ Years of Experience in Cloud Solution Implementation, Management and Operations a. Experience in at least 2 projects involving on-premise to Cloud Migration / hybrid cloud implementation b. Any Associate / Architect level Cloud Certification
3.	HCI Expert	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 5 Years of Experience in Server Solution & Management. a. Relevant industry HCI Certification / as per the solution proposed by MSI b. HCI Administration Experience of at least 2 projects in Data Centre
4.	Server Administrator	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 5 Years of Experience in Server Solution & Management. a. Server related Certification on Red hat/Microsoft b. Server Administration Experience of at least 3 projects in Data Centre
5.	Core Network Administrator	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 5 Years of Experience

Sl. No.	Position	Mandatory Qualification
		in network system provisioning, configuration, and management a. CCNA/JNCIA/CCNP/JNCIP/JNCIS or equivalent certification b. Network Security Implementation & Management Experience in at least 2 large Data centre projects
6.	Security Administrator	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 5 Years of Experience in security system provisioning, configuration, and management a. Certified in CCSA/CCIE or equivalent b. Network Security Implementation & Management Experience in 2 large Data centre projects
7.	Database Administrator	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 7 Years of Experience in Database Administration. a. Mid-level (Professional/Associate level) Certifications in Postgres/MS SQL/My SQL b. Database Administration Experience in at least 3 Data Centre projects
8.	Storage Expert	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 5 Years of Experience in Storage Implementation & Management. a. Mid-level Storage OEM related Certification as per Bidder's Solution b. Storage Implementation & Management Experience in at least 2 large Data Centre projects
9.	System Administrator – Linux/Windows	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 6 Years of Experience in Server Solution & Management. a. Windows/Linux Server related professional level Certification b. Server Administration Experience in at least 2 large Data Centre projects
10.	Backup Expert	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 5 Years of Experience in Storage Implementation & Management. a. Relevant Backup OEM related Certification (Expert Level) as per Bidder's Solution b. Backup Implementation & Management Experience in at least 3 projects
11.	NOC Engineer	BE / B. Tech / MCA with minimum 3 Years of Experience in Network/Server Configuration/Performance Monitoring
12.	Helpdesk Engineer	BE / B. Tech / MCA / Polytechnic Diploma(IT) with minimum 3 Years of Experience in IT Infra Helpdesk handling.

Sl. No.	Position	Mandatory Qualification
13.	BMS Expert	Mandatory: Educational Qualification in BE / B. Tech (Electrical/Electronic or related streams) with minimum 3 Years of Experience in BMS Solution Implementation & Management BMS Implementation & Management Experience in at least 3 projects including minimum one data center experience

**Note: Levels mentioned above are indicative of years of experience a Manpower has in the respective fields.**

- i. The MSI shall deploy the resources within 15 days of the receipt of the LOI/PO from CHIPS. The deployed resources shall be present onsite on all Government of Chhattisgarh working days and also on other days, if there is a requirement for the project.
- ii. MSI must clearly mention these details in their manpower deployment plan and CV's will need to be provided for all proposed resources, as part of bidder's technical proposal.
- iii. Bidder should deploy resource with requisite skills and experience. CHiPS reserve the right to ask for replacement of any resource who do not display adequate expertise and experience or for any other reasons for the intended job.
- iv. CHiPS may conduct technical interview of the candidates proposed by the bidder to examine if they are suitable for the position proposed. In case proposed resources by the bidder for selection, is rejected by CHiPS during interview process, the bidder will provide an alternative resource who will be subjected to the above same selection process comprising of interview.
- v. Bidder shall clearly indicate the manpower to be deployed for various stages of the project as per the Schedule indicated in the above sections in their technical proposal.
- vi. Bidder shall provide as part of the bid, CVs of above mentioned Manpower as per the format mentioned at Annexure 9 of this RFP.

## 7.11 Responsibilities of CHiPS

**7.11.1** CHiPS shall provide approvals & signoffs to the deliverables within the stipulated time period. CHiPS shall direct and monitor the activities performed by the MSI as per the Tender Document and in turn validate the service levels attained as per the SLA document. CHiPS will also be responsible for the following activities:

- a. Internet Bandwidth at CGSDC
- b. Power supply from multiple sources at CGSDC
- c. Cost of Electricity bills will be borne by CHiPS

## 8. Implementation Plan, Deliverables, Payment Milestones and Penalties

**T0-** Represents the Project Start Date (i.e. Contract Signing Date)

Milestone Number	Milestone Name	Timelines	Payment	Deliverables
Milestone 1	<b>Mobilisation Advance</b> 10% of capex value of the contract against submission of advance bank guarantee of 110% of the value of mobilisation advance.	T0+15 days	Nil Or 10% of capex cost against submission of BG equivalent to 110% of mobilization advance value, applicable if submitted	<ul style="list-style-type: none"> <li>Submission of Advance Bank Guarantee by MSI</li> </ul>
Milestone 2	Kick-off Meeting	T0+15 days	NIL	<ul style="list-style-type: none"> <li>Project Plan along with Timelines</li> <li>Hand Over-Take Over Plan for existing IT &amp; Non-IT Infrastructure</li> <li>Resource Deployment Plan</li> <li>Migration Plan and Timelines</li> </ul>
Milestone 3	Delivery of 100% of Non-IT Components (Attached in BOQ Schedule)	T0+45 days	10% of total CAPEX value	<ul style="list-style-type: none"> <li>The MSI will deliver the items at designated location as per the purchase order and obtain signature with date and stamp of the Delivery Proof (s).</li> <li>Delivery Approval email from CHiPS</li> <li>Copy of duly signed, stamped and CHiPS approved delivery challan, Material Inspection report,</li> </ul>
Milestone 4	Completion of Civil work	T0+60 days	5% of total CAPEX value	<ul style="list-style-type: none"> <li>Installation reports &amp; Certificate of completion signed by CHiPS</li> </ul>
Milestone 5	Installation of Non- IT Components	T0+75 days	10% of total CAPEX value	<ul style="list-style-type: none"> <li>Installation reports signed by CHiPS</li> </ul>
Milestone 6	Commissioning, Integration & Testing of Non-IT hardware	T0+90 days	5% of total CAPEX value	<ul style="list-style-type: none"> <li>Acceptance reports signed by CHiPS</li> </ul>
Milestone 7	Delivery of 100% IT Components	T0+90 days	20% of total CAPEX value	<ul style="list-style-type: none"> <li>The MSI will deliver the items at designated</li> </ul>

Milestone Number	Milestone Name	Timelines	Payment	Deliverables
	(Attached in BOQ schedule)			<p>location as per the purchase order and obtain signature with date and stamp of the Delivery Proof (s).</p> <ul style="list-style-type: none"> <li>▪ Copy of duly signed, stamped and CHiPs approved delivery challan, Material Inspection report, Receipt of the components</li> </ul>
Milestone 8	Installation of IT Components including One time Cloud Setup at DR	T0+160 days	10% of total CAPEX value	<ul style="list-style-type: none"> <li>▪ Installation reports signed by CHiPS</li> </ul>
Milestone 9	Commissioning, Integration & Testing of IT components (including DR Cloud, EMS, Setup of NOC and Helpdesk)	T0+210 days	20% of total CAPEX value	<ul style="list-style-type: none"> <li>▪ Acceptance reports signed by CHiPS against each component</li> </ul>
Milestone 10	Project Go-live	T0+ 270 days	10% of total CAPEX value	<ul style="list-style-type: none"> <li>▪ Final acceptance reports and Acceptance Test Reports of each milestone</li> <li>▪ Go-Live Certificate from CHiPS</li> </ul>
Milestone 11	i. ISO 27001: Latest ii. ISO 20000: Latest iii. ISO 22301: Latest	T0+ 450 days	10% of total CAPEX value	<ul style="list-style-type: none"> <li>▪ ISO Certificates from the concerned authority</li> </ul>
Milestone 12	Quarterly O&M payment	Go-live date + 51 Months	Quarterly Payment as per OPEX	<ul style="list-style-type: none"> <li>▪ Manpower attendance details</li> <li>▪ Uptime and SLA reports as per the RFP requirements</li> <li>▪ AMC/Support Certificate of existing and newly supplied hardware and software from respective OEMs</li> </ul>

**Note:**

1. A deduction of 10% will be applied to each successive invoice until advance mobilization of 10% against 110% bank guarantee is recovered.
2. Definition of Go-live: Go-Live shall refer to the successful commissioning of the project, following the completion of all Data Centre components, encompassing IT, Non-IT and Civil

works, as delineated in the Scope of Work outlined in the Request for Proposal (RFP). This milestone signifies that all upgraded or replaced systems, hardware, and infrastructure are fully operational, integrated, and seamlessly functioning within the existing environment, including the successful migration of data and services to the new systems and successful setup and operations of Network Operations Centre and Helpdesk. Go-Live is considered successful once Go-Live certificate is issued by CHiPS or their appointed Third-Party Agency.

3. The Annual Maintenance Contract (AMC) shall take effect from the Go-Live date and shall remain in force for O&M period, during which the Successful MSI shall provide maintenance and support.

#### **Penalties**

- i. If the bidder fails to achieve Milestone 3 and any subsequent milestones until Milestone 11, within the specified timelines, a penalty of 0.5% of the total consolidated CAPEX value of that milestone will be incurred weekly until such milestones are met.
- ii. MSI shall be entitled to reclaim any penalties previously imposed for delays in earlier milestones by successfully meeting the final 'Go-Live' milestone within the overall project timeline.
- iii. If Penalty would be deducted more than 10% of the total consolidated CAPEX with any of the reason, the tendering authority may at anytime terminate the Contract by giving a written notice of at least 30 days to the supplier/ selected MSI.

## **9. Service Level Agreement**

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof to be offered by MSI to CHiPS. The MSI shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels to provide quality services.

The MSI shall meet service level objectives and corresponding parameters to ensure the delivery and quality of services on time as per standard mentioned in the document. Service level indicators & and the target performance levels to be maintained by the Bidder during the contract period. SLA shall be strictly imposed, and a third-party audit/certification agency shall be deployed for certifying the performance of the MSI against the target performance metrics. All logs, reports and data that shall be made available for the purpose of evaluation/audit of SLA parameters/target performance metrics should be system generated only. The benefits of this SLA are to:

- i. Trigger a process that applies Customer and the MSI management attention to some aspect of performance when that aspect drops below an agreed upon threshold, or target.
- ii. Makes explicit the expectations that Customer has for performance.
- iii. Helps Customer to control the service level and performance of MSI services.
- iv. The MSI shall have to submit a quarterly report to monitor the performance of the services being provided by the Bidder and the effectiveness of this SLA



## 9.1 Data Centre Availability

#	Parameters	Target (Uptime)	Penalty	Measurement Interval / Method
1	Data Centre Availability $\text{Availability} = \{1 - [(\text{Downtime}) / (\text{Total Time} - \text{Maintenance Time})]\} * 100$ Availability of Power will be measured up to the socket level in the equipment room that will be providing power to the racks	>=99.98%	No Penalty	Measured Quarterly.  Tools for measurement shall be provided by MSI
		>=99.97% to <99.98%	0.5% of the total Quarterly Payment of OPEX	
		>=99.96% to <99.97%	0.75% of the total Quarterly Payment of OPEX	
		>=99.93% to <99.96%	1 % of the Quarterly Payment of OPEX	
		<99.93%	2% of the Quarterly Payment of OPEX	

## 9.2 SLA for Availability of IT Infrastructure

#	Parameters	Target (Uptime)	Penalty	Measurement Interval / Method
1	Uptime of the Data Centre IT Equipment (including individual server level availability, software, OS and Database running on it):	>=99.98%	No Penalty	Measured Quarterly.  Tools for measurement shall be provided by MSI
		<99.98% to >=99.80%	0.08% of the Quarterly Payment of OPEX of IT components	
		<99.80% to >=99.75%	0.1% of the Quarterly Payment of OPEX of IT components	
		<99.75%	0.25 % of the Quarterly Payment of OPEX of IT Components and for every 0.05 % downtime below 99.75% additional penalty of 2% of the Quarterly Payment of OPEX of IT components	
	i. Enterprise Storage ii. Complete HCI solution iii. Servers iv. SAN Switches v. Core Switches vi. Core Router vii. Leaf and Spine Switches viii. SDN Controller ix. NGFW (Internal & External) x. WAF xi. Load Balancers xii. Server Load Balancer xiii. Backup Solution (Hardware & Software) xiv. All Security Equipment xv. Virtualization Layer xvi. Operating System xvii. Enterprise Monitoring System xviii. Identity & Access Management xix. Hardware Security Module xx. DDoS xxi. HIPS xxii. NDR			

## 9.3 SLA for Non-IT Infrastructure

S. No.	Parameter	Target	Penalty	Measurement Interval / Method
1	Uptime of the Data Centre Non-IT Equipment (including but not limited to):	>=99.98%	No Penalty	Measured Quarterly  Tools for measurement shall be provided by MSI
		<99.98% to >=99.80%	0.08% of the Quarterly Payment of OPEX of Non-IT components	
	i. PAC			

S. No.	Parameter	Target	Penalty	Measurement Interval / Method
	ii. DG	<99.80% to ≥99.75%	0.1% of the Quarterly Payment of OPEX of Non-IT components	
	iii. UPS			
	iv. BMS	<99.75%	0.2 % of the Quarterly Payment of OPEX and for every 0.05 % downtime below 99.75% additional penalty of 2% of the Quarterly Payment of OPEX of Non-IT components	
	v. CCTV			
	vi. Access Control			
	vii. Rodent Repellant System	<99.80% to ≥99.75%	0.5% of the Quarterly Payment of OPEX	<= 30 minutes to > 25 minutes of downtime
	viii. WLD			
	ix. Fire Alarm System	<99.75%	For every 0.25% reduction in the uptime there will be a penalty of 2% of the Quarterly Payment of OPEX	> 30 minutes of downtime
	x. DCIM			
3	The server farm area temperature should be maintained all the time (22° Celsius +/- 2° Centigrade all-time). Temperature log reports should be stored for a period of minimum 4 months.	<99.98% to ≥99.80%	No Penalty	0-4 instances in a week
		<99.80% to ≥99.75%	Penalty of 0.25% of the Quarterly Payment of OPEX for [If Instances count more than 10 then it Record as Event of Default], a letter of warning may be issued to the bidder.	5 no of instances or more than that in a week
4	The server farm relative humidity should be maintained all the time (range from 40% to 70%). Humidity log reports should be stored for a period of minimum 4 months.	<99.98% to ≥99.80%	No Penalty	0-4 instances in a week
		<99.80% to ≥99.75%	Penalty of 0.25% of the Quarterly Payment of OPEX for [If Instances count more than 10 then it Record as Event of Default], a letter of warning may be issued to the bidder.	5 no of instances or more than that in a week
5	Availability of Access Control Devices	≥ 99.98%	No Penalty	25 minutes
		Between 99.98% and 99.75%	0.5% of the of Quarterly Payment of OPEX on an incremental basis.	<= 30 minutes to > 25 minutes of downtime
		< 99.75%	1% of the of the Quarterly Payment of OPEX	> 30 minutes of Downtime

S. No.	Parameter	Target	Penalty	Measurement Interval / Method
6	Major Civil & other Electrical Works	Major Civil Work including the False Flooring, False Ceiling, raised flooring, Doors & Locking, Partitioning, Fire Proofing of all surfaces, Furniture & Fixtures (Door, windows, Table, chair), Painting etc to be attended ideally within 2 days of reporting the problem. The SI should maintain sufficient inventory to carry out civil, electrical HVAC and DCIM, etc. repairs without any disruption to operations. For critical items, the resolution time shall be mutually agreed by the CHiPS and the MSI at the time of award of contract	NA	T
			0.5% of the Quarterly Payment of OPEX for every unresolved call	T1=T+ up to 2 days
			0.75% of the Quarterly Payment of OPEX for every unresolved call	T2 =T1+ up to 2 days
			1% of the OPEX value for every unresolved call.	>T2

**Note:**

- Uptime will be measured on monthly and quarterly basis.
- Uptime % =  $\frac{((\text{Total Uptime} - \text{Planned downtime}) - \text{Downtime}) * 100}{(\text{Total Uptime} - \text{Planned downtime})}$
- The Penalty shall be calculated on weekly/monthly/quarterly basis as per the target specified against difference service requirements.
- Maintenance may include scheduled maintenance, or any other maintenance required to ensure continuity of Data Centre operations. Any downtime for maintenance shall be with prior written intimation to CHiPS.
- If downtime of system or subsystem affects the operation of other systems, then vendor has to pay penalty for the affected systems also.
- The downtime shall be the time from the point the respective equipment becomes unavailable (due to any reason attributable to the MSI) till the time the same becomes fully available for carrying out intended operations (including reinstallation, configuration, restoration, boot-up time, etc.) OR till the time a standby equipment is made available for carrying out intended operations (including installation, configuration, restoration, boot-up time, etc.).

## 9.4 SLA for Help Desk

#	Type of Incident	Target	Penalty	Measurement Interval / Method
1	Critical	<=30 Minutes	No Penalty	Tools for calculating Resolution Time shall be provided by the MSI
		>30 to <=60 minutes	0.5% of the Quarterly payment of OPEX for every unattended call	
		>60 to <= 90 minutes	1% of the Quarterly payment of OPEX for every unattended call	
		>90 minutes	2% of the Quarterly payment of OPEX for every unattended call for delay of every two hours	
2	Medium	<=1 day	No Penalty	
		>1 to <= 2 days	1% of the quarterly payment of OPEX for every unattended call	
		> 2 days	2% of the quarterly payment of OPEX for every unattended call for delay of every two days	
3	Low	<=2 days	No Penalty	
		>2 to <= 4 days	5 % of the quarterly payment of OPEX for every unattended call	
		> 4 days	1 % of the quarterly payment of OPEX for every unattended call for delay of every three days	

### Note:

“Incident” refers to any event / abnormalities in the functioning of the Data Centre Equipment / Services that may lead to disruption in normal operations of the Data Centre services.

- Critical: Incidents, whose resolution shall require additional investment in component or time or shall involve coordination with OEMs. These incidents shall impact the overall functioning of the SDC. For example, Power failure, failure of Spine switch, etc.
- Medium: Incidents, whose resolution shall require replacement of hardware or software parts, requiring significant interruption in working of that individual component, for example, installation of operating system, replacement of switch, etc.
- Low: Incidents, whose resolution shall require changes in configuration of hardware or software, which will not significantly interrupt working of that component.

### Measurement Matrix

#### a. Response Time:

- Response time is the total time taken registering the complaint at Helpdesk or through web telephone to reach the user.
- Response time % =  $\frac{[(\text{Calls Responded Time} - \text{Call Logged Time}) / \text{Total Quarterly Calls}] \times 100}{1}$

#### b. Resolution Time:

- The total time taken registering the complaint at Helpdesk or through web telephone at respective location and rectifying the fault. This time includes time taken to reach the site, diagnose, installation, configuration and repair of operating systems and all other applicable software including anti-virus software; escalation of call or other applicable third party for resolution of the

call as per requirement; installation, shifting/ reinstallation of systems along with applicable software; and any other applicable FMS services etc. to make the system functional as per requirement.

- ii. Resolution time % =  $\frac{[(\text{Calls Resolution Time} - \text{Call Logged Time}) / \text{Total Quarterly Calls}] * 100}{1}$

## 9.5 SLA for Cloud Services

S. No.	Service Level Objective	Measurement	Target Service Level	Penalty
1.	Availability/Uptime of cloud services and Resources for CSP's Infrastructure	Availability (as per the definition in the SLA) will be measured Quarterly for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components, orchestration layer, virtualization layer) provisioned in the cloud. Measured with the help of SLA reports provided by MSP	<99.95% & ≥ 99.5%	2.5% of Quarterly Payment of Cloud Service
			< 99.5% & ≥ 99%	5% of Quarterly Payment of Cloud Services
			Subsequently, every 0.5% drop in SLA criteria	Additional 2.5% of Quarterly Payment of Cloud Services till event of default and termination
2.	Availability of Critical Services (e.g., Logging Support Request or Incident; Provisioning / De-Provisioning of resources; User Activation / De-Activation; User Profile Management; Access Utilization Monitoring Reports)	Availability (as per the definition in the SLA) will be measured Quarterly for each of the critical services over both the User / Admin Portal (where applicable)	Availability for each of the critical services over both the User / Admin Portal (where applicable) ≥ 99.5%	No Penalty
			<99.5% and ≥ 99%	5% of the Quarterly Payment of Cloud Services
			<99% ≥ 98%	10% of Quarterly Payment of Cloud Services
			Subsequently, every 3% drop in SLA criteria	Additional 2.5% of Quarterly Payment of Cloud services till event of default and termination
3.	Availability of Regular Reports indicating the compliance to the	Timely submission of Reports	Reports shall be submitted every	2.5% of Quarterly Payment of Cloud Services

S. No.	Service Level Objective	Measurement	Target Service Level	Penalty
	Provisional MelTY Empanelment Requirements	Monthly	month (first calendar day).	for delay of every 15 days post submission day.
4.	Provisioning and De-provisioning of Virtual Machines	Per occurrence.	Within Week of occurrence / reported	0.5% of Quarterly Payment of Cloud Services for every one hour of delay beyond target time. To the maximum capping of 5 hours. Beyond 5 hours, 1% of the quarterly payment for every 1 hour.
5.	Data Security, Data Privacy Incident or Data Breach, Data Mining and Management Reporting - Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. Quarter).  Incident Response - MSI shall assess and acknowledge the defined incidents within 1 hour after discovery otherwise additional penalties shall be applicable.	<95% and ≥ 90% within 1 hour	5% of Quarterly Payment of Cloud Services
			<90% and ≥ 85% within 1 hour	10% of Quarterly Payment of Cloud Services
			Subsequently, every 5% drop in SLA criteria	Additional 5% of Quarterly of Cloud Services Payment till event of default and termination
			<95% and ≥ 90% more than 1 hour <90% and ≥ 85% more than 1 hour	10% of Quarterly Payment of Cloud Services & 15% of Quarterly Payment of Cloud Services
			Subsequently, every 5% drop in SLA criteria	Additional 5% of Quarterly of Cloud Services Payment till event of default and termination
6.	Data Security, Data Privacy Incident or Data Breach, Data Mining and Management Reporting – Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a	<95% and ≥ 90% within 1 hour	5% of Quarterly Payment of Cloud Services
			<90% and ≥ 85% within 1 hour	10% of Quarterly Payment of Cloud Services

S. No.	Service Level Objective	Measurement	Target Service Level	Penalty
		<p>predefined time limit (quarter) over the total number of defined incidents to the cloud service within a predefined period (quarter). Measured from Incident Reports</p> <p>Incident Resolution - MSI shall resolve the raised incidents within 1 hour after acknowledgement otherwise additional penalties shall be applicable.</p>	Subsequently, every 5% drop in SLA criteria	Additional 5% of Quarterly Payment of Cloud Services till event of default and termination
			<95% and ≥ 90% more than 1 hour	10% of Quarterly Payment of Cloud Services
			<90% and ≥ 85% more than 1 hour	15% of Quarterly Payment of Cloud Services
			Subsequently, every 5% drop in SLA criteria	Additional 5% of Quarterly Payment of Cloud Services till event of default and termination
7.	Security and Privacy breach including Data Theft / Loss/ Corruption/Mining	Any incident where in system compromised, privacy breached, data is corrupted, data is mined or any case wherein data theft occurs (including internal incidents) impacting business operations in a major way		<p>For each breach/data theft/data corruption/data mining issue/privacy breach, penalty will be levied as per following criteria. Any security incident detected INR 10 Lakhs. This penalty is applicable per incident.</p> <p>These penalties will not be part of overall SLA penalties cap per quarter. In case of serious breach of security wherein the data is stolen, mined, privacy breached or corrupted, Client reserves the right to terminate the contract.</p>
8.	<p>Meeting Recovery Time Objective (RTO) i.e. 4 Hrs/</p> <p>Meeting Recovery Point Objective (RPO) i.e. 15 Min</p>	Measured during the regular planned or unplanned (outage) changeover from	As per project requirement mentioned in scope of work section.	For every 10 minutes delay in RPO and 1 Hr delay in RTO - 5% of Quarterly



S. No.	Service Level Objective	Measurement	Target Service Level	Penalty
		DC to Cloud DR or vice versa.		Payment shall be deducted
9	DR Drill	Measured every six (6) months	At least two DR drills in a year (once every six months)	i. No of DR Drills = 1 1% of the Yearly Payment of the Project ii. No of DR Drills = 0 2% of the Yearly Payment of the Project
10.	Availability of the network link/s between DC and DR on Cloud	Availability will be measured for each of the network link/s provisioned between DC and DR on cloud.	Availability for each of the network links: $\geq 99.5\%$	No Penalty
			$<99.5$ and $\geq 99\%$	5% of quarterly payment
			$<99$ and $\geq 98.5\%$	10% of quarterly payment
			$<98.5$ and $\geq 95\%$	15% of quarterly payment
			$<95\%$	Additional 2% of quarterly payment for every drop of 5%

## 9.6 SLA for Security and Incident Management

MSI shall leverage appropriate security mechanisms that could track such occurrences. MSI shall provide a platform to CHiPS to monitor the consolidated list of events of virus attack, denial of service attack and intrusion attack.

S.No	Parameter	Description	Target	Penalty
1	Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement)	Security incidents could consist of any of the following: <b>Malware Attack:</b> This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. <b>Denial-of-Service Attack:</b> This shall include non-availability of any of the service on-premise or cloud due to attacks that consume related resources. MSI shall be responsible for	a) Any Denial-of-service attack shall not lead to complete service non-availability. b) Zero Malware attack / Denial of Service attack / Intrusion / Data Theft	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 10% of the Quarterly Payment of the Project

S.No	Parameter	Description	Target	Penalty
		monitoring, detecting and resolving all Denial of Service (DoS) attacks. <b>Intrusion:</b> Successful unauthorized access to system, resulting in loss of confidentiality/ Integrity/availability of data. MSI shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.		
2	Security breach including Data Theft/Loss/Corruption	<p>Any incident wherein system including all on-premise and cloud-based services and components are compromised or any case wherein data theft occurs.</p> <p><b>Severity-1:</b> Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available.</p> <p><b>Severity-2:</b> Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.</p> <p><b>Severity-3:</b> Moderate loss of performance resulting in multiple users (includes</p>	No breach	<p>For each breach/data theft occurrence, penalty will be levied as per following criteria.</p> <ol style="list-style-type: none"> <li>1. Severity 1 - Penalty of Rs 30 Lakh per incident.</li> <li>2. Severity 2 - Penalty of Rs 20 Lakh per incident.</li> <li>3. Severity 3 - Penalty of Rs 10 Lakh per incident.</li> </ol> <p>These penalties will not be part of overall SLA penalties cap per month.</p> <p>In case of serious breach of security wherein the data is stolen or corrupted, CHiPS reserve the right to terminate the contract.</p>

S.No	Parameter	Description	Target	Penalty
		public users) impacted in their normal functions		
3	Intrusion reported by firewall or IPS	Action Taken time and measured once in a quarter	<=1 hour	No Penalty
			>1 hour	3 % of the quarterly payment of Quarterly payment for every 30 minutes delay in taking action
4	Patch Management (including rules updating in firewall, IPS & updating of any SPAM control policies etc.)	Time taken from approved changemanagement request for rules & patches updating & spam control policies. (Maximum up to two hours downtime is allowed for Patch Management)	Critical Patches to be implemented within 2 hours from approval of Change Request by CHiPS	No Penalty
			>2 hours and <=3 hours	Rs.1,00,000
			>3 hours and <=5 hours	Rs.2,00,000
			Beyond 5 hours for every 3 hours	Rs.5,00.000
			Non-Critical Patches to be implemented within 7 days of patch release	No Penalty
			Non-Critical Patches implemented after 7 days of patch release	0.1 % of the quarterly payment of OPEX for every 1-day delay in taking action

## 9.7 Change Management

S. No.	Parameter	Target	Penalty	Measurement Tool / Method
1	Change Management Measurement of quality and timeliness of changes to the Data Centre facilities	100% of changes should follow formal change control procedures. All changes need to be approved by CHiPS.	Rs.50000 for every non-compliance	Monthly
		All changes should be implemented on time and as per schedule & without any disruption to business.	Rs.10000 for every non-compliance	

## 9.8 Scheduled Maintenance

S. No.	Parameter	Target	Penalty	Measurement Tool / Method
1	Scheduled Maintenance Measures timely maintenance of the IT and Non-IT Infrastructure equipment installed at the Data Centre. The MSI shall provide a detailed ICT Infrastructure maintenance plan on the Commencement of the project.	100 % of scheduled maintenance should be carried out as per maintenance plan submitted by the MSI.  Any scheduled maintenance needs to be planned and intimated to CHiPS at least 2 working days in advance	Rs.10000 for every non-compliance	Monthly

### 9.9 DC Certifications

S. No.	Parameter	Target	Penalty	Measurement Tool / Method
1	Latest Certifications of CG SDC  i. ISO 27001 ii. ISO 20000 iii. ISO 22301  MSI has to obtain the CGSDC certified within 6 Months of completing the Go-Live and Recertification during contract period	100% Certified for all required Certifications within 6 Months of completion of FAT and Go-Live	10 % of the quarterly payment of OPEX  If certification is delayed beyond 6 months, subsequent Quarterly payment will be deferred till the certification is obtained.	Once after Go-Live and subsequent recertification during the contract period
2	Implementation of Audit recommendations. Repeat observations (same observations that has been reported earlier)		Rs.50000 for every non-compliance	Monthly

### 9.10 SLA for Compliance and Reporting:

S. No.	Parameter	Target	Penalty	Measurement Tool / Method
1	Submission of MIS Reports for SLA calculation (previous month)	5th of current month	No Penalty	
		Delay beyond date of submission	1% of the Quarterly payment of OPEX for every single instance of non-compliance for delay of every two days	
2	Maintenance of Inventory/ Asset Management	100% as per the inventory log committed and maintenance by SI	No Penalty	
		Non- compliance to committed inventory log	1% of the quarterly payment of OPEX for every single instance of non-compliance	
3.	Incident Reporting	Any failure/incident on any part of the Data Centre infrastructure or its facilities shall be communicated immediately to	100% incidents to be reported to CHiPS within 1 hour with the cause, action, and remedy for the incident.	No Penalty

S. No.	Parameter	Target	Penalty	Measurement Tool / Method
		CHiPS as an exceptional report giving details of downtime, if any.		

### 9.11 Manpower SLA

SLA would be applicable from the project Go-live and in operations and maintenance phase of the project. SLA would be applicable on the availability of manpower and the service levels mentioned below:

S.No.	Service level agreement	Penalties for non-compliance
1	Non-deployment of total manpower mentioned in the contract as per the date of joining	Beyond 15 Days, 0.5% of total Quarterly Payment value of the respective quarter per resource per week.
2	If the employee is found responsible for any theft, loss of material/ articles and damages	Immediate payment in actuals, equivalent to the value of the article theft/lost/damaged. Replacement within 7 day/disciplinary action as decided by the buyer depending on the gravity of the act.
3	If the employee is found responsible for disobedience/ misconduct	Warning/counselling/Immediate replacement of resource within 7 days as decided by the buyer depending on the gravity of the act
4	If the employee is absent for more than 7 days without informing or taking prior approval	Substitute within 7 days with equivalent resource failing which, 0.5% of total Quarterly Payment value of the respective quarter per resource per week up to 15 days.
5	If the employee is found responsible for adopting illegal and foul methods or exercising any corrupt practice in collusion with any third party or officials at the workplace	Replacement within 7 day/disciplinary action as decided by the buyer depending on the gravity of the act
6	Replacement of resources until Go-Live	Rs.40,000/-per replacement
7	Post Go-Live until completion of contract - Up to 2 replacement per resource	No penalty
8	Post Go-Live until completion of contract - More than 2 but up to 4 replacements	Rs.40,000/-per replacement (applicable beyond 2 replacements up to 4 replacements)
9	Post Go-Live until completion of contract - More than 4 replacements	Rs. 60,000/- per replacement (applicable beyond 4 replacements)

### 9.12 Service Level Monitoring

The Service Level parameters defined in this RFP shall be monitored on a periodic basis, as per the individual parameter requirements. The MSI shall be responsible for providing appropriate web based online SLA measurement and monitoring tools for the same. The

MSI will be expected to take immediate corrective action for any SLA that has been breached. In case issues are not rectified to the complete satisfaction of Purchaser within a reasonable period of time then the Purchaser will have the right to take appropriate penalizing actions, including termination of the contract.

### 9.13 SLA Change Process

It is acknowledged that this SLA may change as CHiPS business needs evolve over the course of the contract period. This document also defines the following management procedures:

- a. A process for negotiating changes to the SLA.
- b. An issue management process for documenting and resolving difficult issues.
- c. CHiPS and MSI management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement will be requested, documented, and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this SLA and, subsequently, the Contract.

If there is any confusion or conflict between this document and the Contract, the Tender and its addenda, the Contract will supersede.

The parties may amend this SLA by mutual agreement in accordance with terms of this contract. Changes can be proposed by either party. The MSI can initiate an SLA review with the CHiPS. Normally, the forum for negotiating SLA changes will be CHiPS quarterly meetings. Unresolved issues will be addressed using the issue management process.

The MSI shall maintain and distribute current copies of the SLA document as directed by CHiPS. Additional copies of the current SLA will be made available at all times to authorized parties.

## 10. Annexures

### Annexure-1: Request for Clarifications/ Pre-bid queries

MSI/Bidder requiring specific points of clarification may communicate with CHiPS during the specified period using the following format to be submitted in (.xls):

MSI's Request for clarification/ pre-bid queries			
Name of Organization submitting request		Name & position of person submitting request	Full address of the Organization including phone, fax and email points of contact
			Tel:
			Fax:
			Email:
S. No.	Bidding Document Reference(s) (Section number/ page)	Content of RFP requiring Clarification	Points of clarification Required
1.			
2.			

**Note:** The name of the organization and the date shall appear in each page of such as document/ email in the header or footer portion.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Address: \_\_\_\_\_

Location: \_\_\_\_\_ Date: \_\_\_\_\_



## Annexure-2: Proforma for Bank Guarantee for Earnest Money Deposit

### Proforma for the Bank Guarantee for Earnest Money Deposit

(To be stamped in accordance with stamp act)

Ref: Bank Guarantee # Date  
CEO, Chhattisgarh Infotech Promotion Society (CHiPS)  
3rd Floor, SDC BUILDING,  
Civil Lines, Raipur, Chhattisgarh, 492001

Dear Sir,

In accordance with your bid reference no. \_\_\_\_\_ Dated  
\_\_\_\_\_ M/s \_\_\_\_\_ having its registered office at

\_\_\_\_\_ herein after

(Called 'bidder') wish to participate in the said bid for **RFP for the Selection of Master System Integrator (MSI) for CGSDC2.0 in the State of Chhattisgarh.**

An irrevocable Financial Bank Guarantee (issued by a nationalized / scheduled commercial Bank) against Earnest Money Deposit amounting to Rs. \_\_\_\_\_ Rupees (in words \_\_\_\_\_) valid up to is required to be submitted by the bidder, as a condition for participation in the said bid, which amount is liable to be forfeited on happening of any contingencies mentioned in the bid document.

M/s \_\_\_\_\_ having its registered office at \_\_\_\_\_ has undertaken in pursuance of their offer to CHiPS (hereinafter called as the beneficiary) dated \_\_\_\_\_ has expressed its intention to participate in the said bid and in terms thereof has approached us and requested us \_\_\_\_\_ (Name of Bank) \_\_\_\_\_ (Address of Bank) to issue an irrevocable financial Bank Guarantee against Earnest Money Deposit (EMD) amounting to Rs /- Rupees (in words \_\_\_\_\_) valid up to.

We, the \_\_\_\_\_ (Name of Bank) \_\_\_\_\_ (Address of Bank) having our Head office at \_\_\_\_\_ therefore Guarantee and undertake to pay immediately on first written demand by CHiPS, the amount Rs. \_\_\_\_\_ Rupees (in words \_\_\_\_\_) without any reservation, protest, demur and recourse in case the bidder fails to Comply with any condition of the bid or any violation against the terms of the bid, Without the beneficiary needing to prove or demonstrate reasons for its such demand. Any Such demand made by said beneficiary shall be conclusive and binding on us irrespective of any dispute or difference raised by the bidder.

This guarantee shall be irrevocable and shall remain valid up to \_\_\_\_\_. If any further extension of this Guarantee is required, the same shall be extended to such required period on receiving instructions in writing, from CHiPS, on whose behalf guarantee is issued.

This Bank guarantee shall be valid up to \_\_\_\_\_. We are liable to pay the guaranteed amount or any part thereof under this Bank guarantee only if you serve upon us a written claim or demand, on or before hours (Indian Standard Time) where after it ceases to be in effect in all respects whether or not the original Bank guarantee is returned to us."

In witness whereof the Bank, through its authorized officer has set its hand stamped on this \_\_\_\_\_ Day of \_\_\_\_\_ 2024 at \_\_\_\_\_ .

**Name of signatory:**

**Designation:**

**Email ID:**

**Contact No. :**

**Bank Common Seal**

## Annexure-3: Guidelines for E-Procurement

(Guidelines for Bidder/MSIs on using integrated e-Procurement System Govt. of Chhattisgarh. <https://eproc.cgstate.gov.in>)

**Note: These conditions will over-rule the conditions stated in the tender document(s), wherever relevant and applicable.**

### 1. Vendor / MSI Registration on the e-Procurement System:

All the Users / MSIs (Manufacturers / Contractors / Suppliers / Vendors / Distributors etc.) registered with and intending to participate in the Tenders of various Govt. Departments / Agencies / Corporations / Boards / Undertakings under Govt. of Chhattisgarh processed using the Integrated e-Procurement System are required to get registered on the centralized portal <https://eproc.cgstate.gov.in> and get approval on specific class (e.g. A, B, C, D, UGE, UDE, Others/Open) from Public Works Department (in case to participate in tenders restricted to vendors / MSIs in a particular class).

The non – registered users / MSIs who are also eligible to participate in the tenders floated using the e-Procurement system are also required to be registered online on the e-Procurement system. Vendors are advised to complete their online enrolment / registration process on the portal well in advance to avoid last minute hassle, it is suggested to complete enrolment at least four days before the last date of bid submission date, failing which may result in non-submission of bids on time for which vendor/end user shall be solely responsible.

For more details, please get in touch with e-Procurement system integrator on Toll free 1800 258 2502 or email [helpdesk.eproc@cgswan.gov.in](mailto:helpdesk.eproc@cgswan.gov.in).

### 2. Digital Certificates:

The bids submitted online must be signed digitally with a valid Class II / Class – III Digital Signature Certificate to establish the identity of the MSIs submitting the bids online. The MSIs may obtain pair of Encryption & Signing Class – II / Class – III Digital Certificate issued by an approved Certifying Authority (CA) authorized by the Controller of Certifying Authorities (CCA), Government of India.

Note: It may take up to 7 to 10 working days for issuance of Class-II / Class-III Digital Certificate, Therefore the MSIs are advised to obtain it at the earliest. It is compulsory to possess a valid Class-II / Class-III Digital Certificate while registering online on the above mentioned e-Procurement portal. A Digital Certificate once mapped to an account / registration cannot be remapped with any other account / registration however it may be inactivated / deactivated.

Important Note: Bid under preparation / creation for a particular tender may only be submitted using the same digital certificate that is used for encryption to encrypt the bid data during the bid preparation / creation / responding stage. However MSI may prepare / create and submit a fresh bid using his/her another / reissued / renewed Digital Certificate only within the stipulated date and time as specified in the tender.

In case, during the process of a particular bid preparation / responding for a tender, the MSI loses his/her Digital Certificate because of any reason they may not be able to submit the same bid under preparation online, Hence the MSIs are advised to keep their Digital Certificates secure to be used whenever required and comply with IT Act 2000 & its amendments and CVC guidelines.

The digital certificate issued to the authorized user of an individual / partnership firm / private limited company / public limited company / joint venture and used for online bidding will be considered as equivalent to a no-objection certificate / power of attorney to the user.

Unless the certificate is revoked, it will be assumed to represent adequate authority of the specific individual to bid on behalf of the organization / firm for online tenders as per Information Technology Act 2000. This authorized user will be required to obtain a valid Class-II / Class-III Digital Certificate. The Digital Signature executed through the use of Digital Certificate of this authorized user will be binding on the organization / firm. It shall be the responsibility of management / partners of the concerned organization / firm to inform the Certifying Authority, if the authorized user changes, and apply for a fresh digital certificate for the new authorized user.

### **3. Online Payment**

As the bid is to be submitted only online, MSIs are required to make online payment(s) of the Registration fee / Transaction or Service fees / EMD using the online payments gateway services integrated into the e-Procurement system using various payment modes like Credit Card / Debit Card / Internet Banking / Cash Card / NEFT / RTGS etc.

For the list of available online modes of electronic payments that are presently accepted on the online payments gateway services, please refer the link 'Payments accepted online' on the e-Procurement portal <https://eproc.cgstate.gov.in>.

### **4. Setup of User's Computer System**

In order to operate on the e-Procurement system for a MSI / user, the computer system / desktop / laptop of the MSI is required to have Java ver. 765 , Internet explorer 9 / 11, latest Mozilla, firefox with IE Tab V2 (Enhanced IE Tab) or any other latest browser. A detailed step by step document on the same is available on the home page. Also internet connectivity should be minimum one MBPS.

### **5. Publishing of N.I.T.:**

For the tenders processed using the e-Procurement system, only a brief advertisement notice related to the tender shall be published in the newspapers and the detailed notice shall be published only on the e-Procurement system. MSIs can view the detailed notice, tender document and the activity time schedule for all the tenders processed using the e-Procurement system on the portal <https://eproc.cgstate.gov.in>.

### **6. Tender Time Schedule:**

The MSIs are strictly advised to follow the tender time for their side for tasks / activities and responsibilities to participate in the tender, as all the activities / tasks of each tender are locked before the start time & date and after the end time & date for the relevant activity of the tender as set by the concerned department official.

### **7. Download Tender Document(s):**

The tender document and supporting document(s) if any can be downloaded only online. The tender document(s) will be available for download to concerned MSIs after online publishing of the tender and up to the stipulated date & time as set in the tender.

### **8. Submit Online Bids:**

MSIs have to submit their bid online after successful filling of forms within the specified date and time as set in the tender.

The encrypted bid data of only those MSIs who have submitted their bids within the stipulated date & time will be accepted by the e-Procurement system. It is expected that the MSI complete his bid and submit within timeline, a MSI who has not submitted his bid within the stipulated date & time will not be available during opening. Bid documents uploading during bid preparation should be less than five MB (for individual document) and over all bid documents should be less than fifty MB.

### **9. Submission of Earnest Money Deposit:**

The MSIs shall submit their Earnest Money Deposit Either as usual in a physically sealed Earnest Money Deposit envelope and the same should reach the concerned office OR Online using payment gateway as stated in the Notice Inviting Tender. MSIs also have to upload scanned copy of Earnest Money Deposit instrument.

### **10. Opening of Tenders:**

The concerned department official receiving the tenders or his duly authorized officer shall first open the online Earnest Money Deposit envelope of all the MSIs and verify the same uploaded by the MSIs. He / She shall check for the validity of Earnest Money Deposit as required. He / She shall also verify the scanned documents uploaded by the MSIs, if any, as required. In case, the requirements are incomplete, the next i.e. technical and commercial envelopes of the concerned MSIs received online shall not be opened.

The concerned official shall then open the other subsequent envelopes submitted online by the MSIs in the presence of the MSIs or their authorized representatives who choose to be present in the bid opening process or may view opened details online.

**11. Briefcase:**

MSIs are privileged to have an online briefcase to keep their documents online and the same can be attached to multiple tenders while responding, this will facilitate MSIs to upload their documents once in the briefcase and attach the same document to multiple bids submitting.

**For any further queries / assistance, MSIs may contact:**

The Service Integrator of e-Procurement system. on Help Desk Toll free No. 1800 258 2502 or email [helpdesk.eproc@cgswan.gov.in](mailto:helpdesk.eproc@cgswan.gov.in), or Tel. No. 0771 - 4014158 or email: [pro-chips@nic.in](mailto:pro-chips@nic.in).

#### Annexure-4: Eligibility Bid Cover Letter (Company Letter head)

To,  
Chief Executive Officer  
Chhattisgarh Infotech Promotion Society (CHIPS)  
SDC Building, 02nd floor, Near Police Control Room,  
Civil Lines, Raipur, Chhattisgarh-492001

**Sub: Submission of the response to the RFP No \_\_\_\_\_  
dated \_\_\_\_\_ for Selection of Master System Integrator (MSI) for CGSDC2.0 Project in  
the State of Chhattisgarh**

Dear Sir,

We, the undersigned, offer to provide Implementation & Maintenance of SDC, Chhattisgarh for CHIPS in response to the Request for Proposal dated <insert date> and Tender Reference No <> for "Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh". We are hereby submitting our Proposal online, which includes the PQ, Technical Bid and Commercial Bid.

We hereby declare that all the information and statements made in this Technical Bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our Proposal is accepted, to initiate the Implementation services related to the assignment not later than the date indicated in this tender.

We agree to abide by all the terms and conditions of the RFP and related corrigendum(s)/ addendum(s). We would hold the terms of our bid valid for 180 days as stipulated in the RFP. We hereby declare that as per RFP requirement, we have not been black-listed/ debarred by any Central/ State Government and we are not the subject of legal proceedings for any of the foregoing.

We understand you are not bound to accept any Proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Address: \_\_\_\_\_

Location: \_\_\_\_\_ Date: \_\_\_\_\_

## Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS

### Annexure-5: Eligibility Bid Compliance Checklist

Following are the compliance and reference documents for "Selection of Master System Integrator (MSI) for CGSDC2.0 Project for the State of Chhattisgarh" against Tender Reference No. < Tender Reference No. \_\_\_\_\_ > Dated < \_\_\_\_\_ >

S No.	Type	Eligibility Criteria	Required Documentary Evidence
1	Company Profile	<p>The MSI/Bidder must be incorporated and registered in India under the Indian Companies Act 1956 or 2013, or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for a minimum of <b>five</b> years as on 31.03.2024.</p> <p>The MSI must be registered with appropriate authorities for all applicable statutory duties/taxes.</p>	<ol style="list-style-type: none"> <li>Copy of certificate of Incorporation/Registration under Companies Act 1956/2013 (for Indian companies)</li> <li>Copy of GST certificate</li> <li>Copy of Registration certificate</li> <li>Copy of PAN Card</li> <li>Copy of certificate in case of name change</li> </ol>
2	Company Financial Profile	<p>MSI/Bidder must have average annual turnover of at least INR 300 crores from IT/ITES business for last three audited financial years (i.e. FY 2021-22, 2022-23, 2023-24)</p> <p>And MSI/Bidder should have a positive net worth as on bid submission date.</p>	<ol style="list-style-type: none"> <li>Copy of audited profit and loss account and balance sheet for latest three financial years (FY 2021-22, 2022-23, 2023-24)</li> <li>Certificate from Statutory Auditor with UDIN and stamp for both average annual turnover and positive net worth.</li> </ol>
3	Data Centre Experience	<p>MSI/Bidder should have established /implemented Data Centre projects for Central / State Governments, PSUs, PSEs in India in the last <b>five (5) years</b>:</p> <p>a. One project of value INR 80 Crores or more; OR</p> <p>b. Two projects each having minimum value of INR 60 Crores or more; OR</p> <p>c. Three projects each having minimum value of INR 40 Crores or more</p> <p>The Data Centre project consisting of Supply, Installation, Testing and Commissioning (SITC) of IT components such as server, storage, backup system, network, cyber security equipment for the Data Centre; Non-IT components including installation, commissioning of any of these Electrical Distribution &amp; Lighting, DG sets, Precision AC/Chiller Plant, UPS System, Fire Detection &amp; suppression system, Access Control and CCTV, BMS System.</p> <p><b>Note: Bidder's in-house projects setup will not be considered.</b></p>	<p>For on-going projects:</p> <ol style="list-style-type: none"> <li>Work orders &amp; Agreement highlighting scope of work.</li> <li>Datacentre In progress certificates on the client letter head.</li> <li>Document evidence (Payment advice against invoices) of 50% Payment realization of the total contract value of the project</li> </ol> <p>For completed projects:</p> <ol style="list-style-type: none"> <li>Work orders &amp; Agreement highlighting scope of work.</li> <li>Datacentre Completion certificates on the client letter head for the completed project also signed by the authorised signatory.</li> </ol>
4	DC/DR on Cloud Hosting Experience	MSI/Bidder should have hosted and implemented Data Centre/ Disaster Recovery Centre on Public/Virtual Private	<p>For on-going projects:</p> <ol style="list-style-type: none"> <li>Work orders &amp; Agreement highlighting scope of work.</li> </ol>

## Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS

S No.	Type	Eligibility Criteria	Required Documentary Evidence
		<p>Cloud/Government Community Cloud for Central / State Governments /PSUs/PSEs in India in the last five <b>(5) years</b></p> <p><b>Note: Bidder's in-house projects setup will not be considered.</b></p>	<p>2. Cloud hosting In progress certificates on the client letter head of the projects</p> <p>3. Document evidence (Payment advice against invoices) of 50% Payment realization of the total contract value.</p> <p>For completed projects:</p> <ol style="list-style-type: none"> <li>1. Work orders &amp; Agreement highlighting scope of work.</li> <li>2. Cloud Hosting Completion certificates on the client letter head for the completed project also signed by the authorised signatory.</li> </ol>
5	Helpdesk and NOC Experience	<p>MSI/Bidder should have experience of setting up and managing NOC operations, Service Desk for Central / State Governments / PSUs /PSEs in India in last 5 years</p> <p><b>Note: Bidder's in-house projects setup will not be considered</b></p>	<p>For on-going projects:</p> <ol style="list-style-type: none"> <li>1. Work orders &amp; Agreement highlighting scope of work.</li> <li>2. In progress certificates on the client letter head of the projects</li> </ol> <p>For completed projects:</p> <ol style="list-style-type: none"> <li>1. Work orders &amp; Agreement highlighting scope of work.</li> <li>2. Completion certificates on the client letter head of the projects/Self-Certificate by the authorised signatory</li> </ol>
6	Local Presence	<p>The MSI/Bidder should have an project office in the State of Chhattisgarh or should furnish an undertaking that the same would be established within three month of signing the contract if the project is awarded.</p>	<p>Self-certification duly signed by authorized signatory on company letter head.</p>
7	Key Certifications	<p>The MSI/Bidder shall provide all the three Certifications valid at the time of bidding:</p> <ul style="list-style-type: none"> <li>• ISO 9001:2015 or latest certification</li> <li>• ISO 20000:2018 or latest certification</li> <li>• ISO 27001:2013 or latest certification</li> </ul>	<p>Copies of the valid certificates in the name of the MSI.</p>
8	Undertaking on Blacklisting	<p>As on date of submission of the proposal, the MSI/Bidder, shall not be blacklisted / debarred by any State / Central Government Department or Central /State PSUs/PSEs.</p>	<p>The MSI Undertaking as per the format paced at Annexure 8 for this on company letter head.</p>
9	POA	<p>Furnishing of the Power of Attorney</p>	<p>Power of Attorney executed by the MSI/Bidder in favor of the duly Authorized signatory, certifying him/her as an authorized signatory for the purpose of this Tender.</p>
11	OEM Authorization	<p>The MSI/Bidder should submit valid letter from all the OEMs confirming the following:</p>	<p>Documentary evidence</p> <ol style="list-style-type: none"> <li>1. Authorization letters on OEM Letter Head and</li> </ol>

### **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

<b>S No.</b>	<b>Type</b>	<b>Eligibility Criteria</b>	<b>Required Documentary Evidence</b>
		<ul style="list-style-type: none"><li>c. Authorization for MSI Confirm that the products quoted are not “end of life” or “end of sale products”.</li><li>d. Undertake that the support including spares, patches for the quoted products shall be available for defined project duration</li></ul>	2. Manufacturer's Authorization Form (MAF) from all OEMs' in their Letterhead whose products are being quoted by the MSI need to be attached in the proposal as per format given in the Annexure 14 provided in RFP.
12	OEM Capabilities	OEM for Server, Storage, Networking, Backup, Security must have direct or registered service partner presence in India.	An undertaking from each OEM on the direct or registered service partner presence in India.



**Annexure-6: Certificate for No Conflict-of-Interest Certificate (Company Letter head)**

To,  
Chief Executive Officer  
Chhattisgarh Infotech Promotion Society (CHiPS)  
SDC Building, 02nd floor, Near Police Control Room,  
Civil Lines, Raipur, Chhattisgarh-492001

**Sub: Undertaking on No Conflict-of-Interest Certificate regarding Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh**

Dear Sir,

I/We do hereby undertake that there is absence of, actual or potential conflict of interest on the part of the MSI or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with CHiPS.

I/We also confirm that there are no potential elements (time-frame for service delivery, resource, financial or other) that would adversely impact our ability to complete the requirements as given in the RFP.

We undertake and agree to indemnify and hold CHiPS harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees and fees of professionals, reasonably) by CHiPS and/ or its representatives, if any such conflict arises later.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Address: \_\_\_\_\_

Location: \_\_\_\_\_ Date: \_\_\_\_\_

## **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

### **Annexure-7: Format for Power of Attorney for Sole MSI**

[To be executed on stamp paper of appropriate value]

Know all men by these presents, We, [Insert full legal name of the bidding entity], having registered office at [Insert registered office address] (hereinafter referred to as the "Principal") do hereby constitute, nominate, appoint and authorize [Insert full name of authorized signatory] son of [Insert father's name] presently residing at [Insert address of authorized signatory] who is presently employed with us and holding the position of [Insert position / designation of the authorized signatory] as our true and lawful attorney (hereinafter referred to as the "Authorized Attorney") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to the submission of our proposal in response to the RFP bearing number \_\_\_\_\_ for '<RFP Name>' dated \_\_\_\_\_, including but not limited to signing and submission of all applications, proposals and other documents and writings, participating in pre-Bid and other conferences and providing information/ responses to the Chhattisgarh Infotech Promotion Society (hereinafter referred to as the "CHiPS"), representing us in all matters before the CHiPS, signing and execution of all contracts and undertakings/ declarations consequent to acceptance of our Proposal and generally dealing with the CHiPS in all matters in connection with or relating to or arising out of our Proposal for the said assignment and/ or upon award thereof to us till the execution of appropriate Agreement/s with the CHiPS. AND, we do hereby agree to ratify and confirm all acts, deeds and things lawfully done or caused to be done by our said Authorized Attorney pursuant to and in exercise of the powers conferred by this deed of Power of Attorney and that all acts, deeds and things done by our said Authorized Attorney in exercise of the powers hereby conferred shall always be deemed to have been done by us.

IN WITNESS THEREOF WE, \_\_\_\_\_ THE ABOVE NAMED  
PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS DAY OF \_\_\_\_\_,  
2018

For \_\_\_\_\_

(Signature, name, designation and address)

[Please put company seal if required]

[Notarize the signatures]

Witness 1:

Name:

Designation:

Address:

Signature:

Witness 2:

Name:

Designation:

Address:

Signature:

**Annexure-8: Undertaking on Blacklisting**

{Place}

{Date}

To,

Chief Executive Officer

Chhattisgarh Infotech & Promotion Society (CHiPS)

SDC Building, Civil Lines, 02<sup>nd</sup> Floor, Near Civil Lines, Police Station, Raipur,

Chhattisgarh– 492001

Ref: Tender Reference No. : \_\_\_\_\_ dated \_\_\_\_\_

Subject: Declaration for not being under an ineligibility for corrupt or fraudulent practices or blacklisted/debarred with any of the Government or Public Sector Units

Dear Sir/Madam,

We, the undersigned, hereby declare that we are not under a declaration of ineligibility for corrupt or fraudulent practices or blacklisted / debarred by any State / Central Government Department or Central /State PSUs/PSEs as on bid submission date.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Address: \_\_\_\_\_

Location: \_\_\_\_\_ Date: \_\_\_\_\_

## Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS

### Annexure-9: CV Format

C.V. format of the Key Professionals mentioning experience each in relevant fields

1.	Name of the employee				
2	Designation				
3	Date of Birth				
4	Nationality				
5	Education	Qualification	Name of School/College/University	Degree Obtained	Date Attended
6	Language	Language	Read	Write	Speak
7	Employment Record	Employer	Position	From	To
		<i>(Starting with present position list in reverse order – Up to three quarters of a page)</i>			
8	Relevant Experience	<i>(Give an outline on the experience most pertinent to tasks mentioned In the project. Describe degree of responsibility held on these relevant Assignments – Up to half of a page).</i>			
9	Certification	<p>I, the undersigned, certify that to the best of my knowledge and belief, this bio-data correctly describes myself, my qualifications, and my Experience.</p> <p style="text-align: center;"> <span style="margin-right: 100px;">Date: Place member</span> <span>Signature of the Lead</span> </p>			

For and on behalf of

Signature of the candidate:

**Bidder:**

**Signature**      -----

**Name**      -----

**Designation**      -----

**Company Seal** -----

**Date**      -----

**Annexure-10: Pre-Contract Integrity Pact**

**PRE- CONTRACT INTEGRITY PACT**

**1. GENERAL**

1.1 This pre-bid contract Agreement (hereinafter called the Integrity Pact) is made on .....day of the month..... 20..... between, the Government of Chhattisgarh acting through Shri..... (Designation of the officer, Department) Government of Chhattisgarh (hereinafter called the "**Tendering Authority**", which expression shall mean and include, unless the context otherwise requires, his successors in the office and assigns) and the First Party, proposes to procure (name of the Stores/Equipment/Work/Service) and M/s.....represented by Shri..... (hereinafter called the "MSI/Seller", which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) as the Second Party, is willing to offer/ has offered.

1.2. WHEREAS the MSI is a Private Company/Public Company/ Government Undertaking/ Partnership firm, constituted in accordance with the Applicable Laws in the matter and the TENDERING AUTHORITY is a Ministry/Department of the Government, performing its function on behalf of the Government of Chhattisgarh.

**2. OBJECTIVES**

2.1. Enabling the TENDERING AUTHORITY to obtain the desired Stores/Equipment/Work/Service at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

2.2. Enabling MSIs to abstain from bribing or indulging in any corrupt practices in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing any corrupt practices and the TENDERING AUTHORITY will commit to prevent corruption, in any form, by its official by following transparent procedures.

**3. COMMITMENTS OF THE TENDERING AUTHORITY**

3.1. The TENDERING AUTHORITY undertakes that no official of the TENDERING AUTHORITY, connected directly or indirectly with the contract, will demand, take promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the MSI, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the Bidding Process, bid evaluation, contracting or implementation process related to the contract.

3.2. The TENDERING AUTHORITY will, during the pre-contract stage, treat MSIs alike, and will provide to all MSIs the same information and will not provide any such information to any particular MSI which could afford an advantage to that particular MSI in comparison to the other MSIs.

3.3. All the officials of the TENDERING AUTHORITY will report the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach. In case any such preceding misconduct on the part of such official(s) is reported by the MSI to the TENDERING AUTHORITY with the full and verifiable facts and the same prima fade found to be correct by the TENDERING AUTHORITY, necessary disciplinary proceedings, or any other action as deemed, fit, including criminal proceedings may be initiated by the TENDERING AUTHORITY and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the TENDERING AUTHORITY the proceedings under the contract would not be stalled.

**4. COMMITMENTS OF MSIS**

4.1. The MSI will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the TENDERING AUTHORITY, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

4.2. The MSI further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other

## **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

advantage, commission, fees, brokerage, or inducement to any official of the TENDERING AUTHORITY or otherwise in procuring the Agreement or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or dis-favour to any person in relation to the contract or any other contract with the Government.

4.3. The MSI further confirms and declares to the TENDERING AUTHORITY that the MSI in the original Manufacture/Integrator/Authorized government sponsored export entity of the stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the TENDERING AUTHORITY or any of its functionaries, whether officially or unofficially to the award of the contract to the MSI, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

4.4. The MSI, either while presenting the bid or during pre-contract negotiations or before signing the Agreement, shall disclose any payment he has made, is committed to or intends to make to officials of the TENDERING AUTHORITY or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

4.5. The MSI will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the Bidding Process, bid evaluation, contracting and implementation of the contract.

4.6. The MSI will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

4.7. The MSI shall not use improperly, for purpose of competition or personal gain, or pass on to others, any information provided by the TENDERING AUTHORITY as part of the business relationship, regarding plans, technical proposal and business details, including information contained in any electronic data carrier. The MSI also undertakes to exercise due and adequate care lest any such information is divulged.

4.8. The MSI commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

4.9. The MSI shall not instigate or cause to instigate any third person to commit any of the acts mentioned above.

### **5. PREVIOUS TRANSGRESSION**

5.1. The MSI declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify MSI's exclusion from the tender process.

5.2. If the MSI makes incorrect statement on this subject, MSI can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

### **6. EARNEST MONEY (SECURITY DEPOSIT)**

**Every MSI while submitting commercial bid, shall deposit an amount as specified in RFP as Earnest Money/Security Deposit online through e-procurement portal**

6.1. No interest shall be payable by the TENDERING AUTHORITY to the MSI on Earnest Money/Security Deposit for the period of its currency.

### **7. SANCTIONS FOR VIOLATIONS**

7.1. Any breach of the aforesaid provisions by the MSI or any one employed by it or acting on its behalf (whether with or without the knowledge of the MSI) shall entitle the TENDERING AUTHORITY to take all or any one of the following actions, wherever required:-

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the MSI. However, the proceedings with the other MSI(s) would continue.

(ii) To forfeit fully or partially the Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed), as decided by the TENDERING AUTHORITY and the TENDERING AUTHORITY shall not be required to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the MSI.

(iv) To recover all sums already paid by the TENDERING AUTHORITY, and in case of the Indian MSI with interest thereon at 2% higher than the prevailing Prime Lending Rate while in case of a MSI from a country other than India with interest thereon at 2% higher than the LIBOR. If any

## **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

outstanding payment is due to the MSI from the TENDERING AUTHORITY in connection with any other contract such outstanding payment could also be utilized to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the MSI, in order to recover the payments, already made by the TENDERING AUTHORITY, along with interest.

(vi) To cancel all or any other contracts with the MSI and the MSI shall be liable to pay compensation for any loss or damage to the TENDERING AUTHORITY resulting from such cancellation/rescission and the TENDERING AUTHORITY shall be entitled to deduct the amount so payable from the money(s) due to the MSI.

(vii) To debar the MSI from participating in future Bidding Processes of the Government of Chhattisgarh for a minimum period of five years, which may be further extended at the discretion of the TENDERING AUTHORITY.

(viii) To recover all sums paid in violation of this Pact by MSI(s) to any middlemen or agent or broken with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the TENDERING AUTHORITY with the MSI, the same shall not be opened.

(x) If the MSI or any employee of the MSI or any person acting on behalf of the MSI, either directly or indirectly, is closely related to any of the officers of the TENDERING AUTHORITY, or alternatively, if any close relative of an officer of the TENDERING AUTHORITY has financial interest/stake in the MSI's firm, the same shall be disclosed by the MSI at the time of filling of tender. Any failure to disclose the interest involved shall entitle the TENDERING AUTHORITY to rescind the contract without payment of any compensation to the MSI

The term 'close relative' for this purpose would mean spouse whether residing with the Government servant or not, but not include a spouse separated from the Government servant by a decree or order of a competent court; son or daughter or step son or step daughter and wholly dependent upon Government servant, but does not include a child or step child who is no longer in any way dependent upon the Government servant or of whose custody the Government servant has been deprived of by or under any Applicable Law; any other person related, whether by blood or marriage, to the Government servant or to the Government servant's wife or husband and wholly dependent upon Government servant.

(xi) The MSI shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the TENDERING AUTHORITY, and if he does so, the TENDERING AUTHORITY shall be entitled forthwith to rescind the contract and all other contracts with the MSI. The MSI shall be liable to pay compensation for any loss or damage to the TENDERING AUTHORITY resulting from such rescission and the TENDERING AUTHORITY shall be entitled to deduct the amount so payable from the money(s) due to the MSI.

7.2. The decision of the TENDERING AUTHORITY to the effect that a breach of the provisions of this pact has been committed by the MSI shall be final and conclusive on the MSI. However, the MSI can approach the Monitor(s) appointed for the purposes of this Pact.

### **8. FALL CLAUSE**

8.1. The MSI undertakes that he has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Department of the Government of Chhattisgarh or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the MSI to any other Department of the Government of Chhattisgarh or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the MSI to the TENDERING AUTHORITY, if the contract has already been concluded.

### **9. INDEPENDENT MONITORS**

9.1. The TENDERING AUTHORITY will appoint Independent Monitors (hereinafter referred to as Monitors) for this Pact.

9.2. The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

9.3. The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

9.4. Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. The Monitor shall be under

## **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

contractual obligation to treat the information and documents of the MSI/Sub-Selected MSI(s) with confidentiality.

9.5. As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the TENDERING AUTHORITY.

9.6. The Monitor will submit a written report to the designated Authority of TENDERING AUTHORITY/Secretary in the Department/within 8 to 10 weeks from the date of reference or intimation to him by the TENDERING AUTHORITY/MSI and, should the occasion arise, submit proposals for correcting problematic situations

### **10. FACILITATION OF INVESTIGATION**

In case of any allegation of violation of any provisions of this Pact or payment of commission, the TENDERING AUTHORITY or its agencies shall be entitled to examine all the documents including the Books of Accounts of the MSI and the MSI shall provide necessary information of the relevant documents and shall extend all possible help for the purpose of such examination.

### **11. LAW AND PLACE OF JURISDICTION**

This Pact is subject to Indian Law, the place of performance and jurisdiction shall be the seat of the TENDERING AUTHORITY.

### **12. OTHER LEGAL ACTIONS**

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the any other Applicable Law in force relating to any civil or criminal proceedings.

### **13. VALIDITY**

13.1. The validity of this Integrity Pact shall be from the date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the TENDERING AUTHORITY and the MSI/Seller whichever is later. In case MSI is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

13.2. If one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In such case, the parties will strive to come to an agreement to their original intentions.

14. The parties hereby sign this  
Integrity Pact  
at.....on.....

#### **CHiPS**

\_\_\_\_\_ [Signature]

\_\_\_\_\_ [Name]

\_\_\_\_\_ [Designation]

#### **Witness**

1.

2.

#### **MSI**

\_\_\_\_\_ [Signature]

\_\_\_\_\_ [Name]

\_\_\_\_\_ [Designation]

#### **Witness**

1.

2.



## **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

### **Annexure-11: Commercial Bid Cover Letter**

To,

Chief Executive Officer  
Chhattisgarh Infotech Promotion Society (CHiPS)  
SDC Building, 02nd floor, Near Police Control Room,  
Civil Lines, Raipur, Chhattisgarh-492001

**Sub: Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh**

**Ref: Tender Reference No: < > dated < >**

Dear Sir,

We, the undersigned MSI, having read and examined in detail all the Tender documents in respect of **Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh** do hereby propose to provide services as specified in the Tender Reference No.

< \_\_\_\_\_ > dated < \_\_\_\_\_ >

#### **I. PRICE AND VALIDITY**

- a. All the prices mentioned in our Bid are in accordance with the terms & conditions as specified in the RFP. Prices of all hardware items under this RFP are valid for a period of 1 year from the date of opening of the commercial bid. Prices of Operations & Maintenance are valid for a period of 5 years from project Go-Live. The validity of bid is 180 days from the date of bid submission.
- b. We are an Indian Firm and do hereby confirm that our prices are inclusive of all taxes, duties, levies etc.
- c. We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other Corporate Tax in altered under the law, we shall pay the same.

#### **II. UNIT RATES**

We have indicated in the relevant schedules enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to/ decrease from the Scope of Work under the Contract.

#### **III. DEVIATIONS**

We declare that all the services shall be performed strictly in accordance with the RFP irrespective of whatever has been stated to the contrary anywhere else in our bid. Further we agree that additional conditions, if any, found in our bid documents, shall not be given effect to.

#### **IV. EARNEST MONEY DEPOSIT (EMD)**

We have enclosed an EMD in the form of Non-refundable & Irrevocable Bank Guarantee for a sum of INR \_\_\_\_\_/- (**Rupees** \_\_\_\_\_ **only**). This EMD is liable to be forfeited as per clause 4.17

#### **V. TENDER PRICING**

We further confirm that the prices stated in our bid are in accordance with your Instruction to MSIs included in Tender documents.

#### **VI. QUALIFYING DATA**

We confirm having submitted the information as required by you in your Instruction to MSIs. In case you require any other further information/ documentary proof in this regard before evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

## **Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS**

### **VII. BID PRICE**

We declare that our Bid Price is for the entire scope of the work as specified in the RFP. These prices are indicated in Annexure-12: Commercial Bid Format attached with our Tender as part of the Tender.

### **VIII. PERFORMANCE BANK GUARANTEE**

We hereby declare that in case the Contract is awarded to us, we shall submit the Performance Bank Guarantee in the form prescribed in Annexure-13: Format for Performance Bank Guarantee

We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive.

We confirm that no Technical deviations are attached here with this commercial offer.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Address: \_\_\_\_\_

Location: \_\_\_\_\_ Date: \_\_\_\_\_

## Annexure-12: Commercial Bid Format

**Table 1: Summary of Cost Component – Overall** \*The financial bid has to be filled online

Summary of Price Bid for CGSDC2.0		
Sr. No.	Item Description	Total Cost (Inclusive of all Taxes)
		INR
1	Total CAPEX (A)	A
2	Total OPEX (Value for one Quarter X 17 Quarters) (B)	B
3	Total Cost for DR on Cloud including Managed Services Cost for 5 Years (C)	C
	Total INR in Figures D =(A+B+C)	D= A+B+C
	Total INR in words	

**Total Cost (C= A+B+C i.e. CAPEX + OPEX+ Cost for DR) would be considered for commercial evaluation of the bids**

**Note 1: The total cost would be considered for commercial evaluation of the bids, CHiPS reserves the right at the time of award of Contract to increase or decrease goods and/ or services from what was originally specified while floating the RFP without any change in unit price or any other terms and conditions.**

**Note 2: Prices in Commercial Bid should be quoted in the provided format. All prices should be quoted in Indian Rupees and indicated both in figures and words. Price in words shall prevail, in the event of any mismatch.**

---

### Instructions to fill the Commercial Bid:

- i. MSI should provide all prices as per the prescribed format under this Annexure. MSI should not leave any field blank. In case the field is not applicable, MSI must indicate "0" (Zero) in all such fields.
- ii. All the prices are to be entered in Indian Rupees ONLY (percentage (%) values are not allowed)
- iii. CHiPS reserves the right to ask the MSI to submit proof of payment against any of the taxes, duties, levies indicated
- iv. CHiPS shall take into account that all Taxes, Duties & Levies shall be paid as per actual.
- v. CHiPS shall take into account all Taxes, Duties & Levies for the purpose of Evaluation
- vi. The MSI needs to account for all Out-of-Pocket expenses due to Boarding, Lodging and other related items.
- vii. The Unit Rate as mentioned in the formats in the commercial bid shall be used for the purpose of 'Change Order' for respective items, if any. However, based on the market trends, Purchaser retains the right to negotiate this rate for future requirements.
- viii. For the purpose of evaluation of Commercial Bids, CHiPS shall make appropriate assumptions to arrive at a common bid price for all the MSIs. This however shall have no co-relation with the Contract value or actual payment to be made to the MSI.
- ix. The soft copy of the commercials should be either in MS Excel only and not PDF.
- x. The commercial bid shall not be altered, modified, changed, or any additional conditions applied therein. Any changes to this format will lead to disqualification. Decision of CHiPS shall be final.
- xi. CAPEX or one time cost means cost incurred in the first year which includes the cost of Supply, Delivery, Configuration, Installation, Customization, Integration, Training, Testing, and Implementation of Hardware, software and any other component/s required for the proposed solution.
- xii. The Bill of Material provided in this RFP indicative, bidder shall include details of all the components product-wise and unit-wise.
- xiii. The MSI's annual OPEX quote must equal or exceed 6% of the total CAPEX value. Failure to meet this requirement (i.e., quoting less than 6% of CAPEX) will render the financial bid invalid and ineligible for consideration

**Table A: Total CAPEX Cost Component: \*The financial bid must be filled in excel and uploaded in Envelope C**

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity	Unit Cost (INR) (Inclusive of all taxes)	Total Cost (INR) (Inclusive of all taxes)
			A	B	C=(A*B)
<b>A</b>	<b>IT Components</b>				
1	Rack Server	Nos	12		
2	Hyper Converged Infrastructure	Nos	12		
3	Virtualisation Software and Management Solution for Rack server Cluster	Nos	1		
4	Windows Operating System Data Center Edition - 16 Core License Model	Nos	36		
5	Redhat Linux Operating System Enterprise Edition - Socket Based	Nos	12		
6	MS SQL Database Enterprise Edition - Core Based	Nos	32		
7	Postgres SQL Enterprise Edition - Core Based	Nos	64		
8	Backup Hardware & Software (500 TB front end capacity or 500 VM)	Nos	1		
9	Server Load Balancer	Nos	2		
10	SDN Controller	Nos	2		
11	SPINE Switch	Nos	2		
12	Leaf switch – OFC	Nos	8		
13	Core Router - Internet	Nos	2		
14	Core Router - Intranet	Nos	2		
15	Management Switch	Nos	2		
16	Link Load balancer - Internet	Nos	2		
17	Link Load balancer – Intranet	Nos	2		
18	L2 Managed Switch for NOC	Nos	2		
19	SAN Switch	Nos	2		
20	Enterprise Storage (500 TB Usable Storage)	Nos	1		
21	Next Generation Firewall - Internet	Nos	2		

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity	Unit Cost (INR) (Inclusive of all taxes)	Total Cost (INR) (Inclusive of all taxes)
			A	B	C=(A*B)
22	Next Generation Firewall - Intranet	Nos	2		
23	Web Application Firewall	Nos	2		
24	EDR - Endpoint Detection Response	Nos	500		
25	Identity Access Manager	Nos	500		
26	Enterprise Monitoring System (NMS, ITSM, ISMS)	Nos	500		
27	Network Access Controller	Nos	2		
28	HSM - Hardware Security Module	Nos	2		
29	HIPS - Host Intrusion Prevention System	Nos	500		
30	NDR - Network Detection and Response	Nos	2		
31	DdoS	Nos	1		
<b>B</b>	<b>Non IT Components</b>				
1	UPS - 300 KVA with battery bank upgradable to 400 KVA	Nos	2		
2	Battery Bank for 300 KVA - Min 4 Hrs backup	Lot	1		
3	UPS - 20 KVA with Battery Bank	Nos	2		
4	Battery Bank for 20 KVA - Min 4 Hrs backup	Lot	1		
5	Split AC - 1.5 Ton	Nos	3		
6	Split AC - 2 Ton	Nos	2		
7	HVAC System - Precision Air Conditioner	Nos	4		
8	Biometric Door Access System	Nos	1		
9	Smart TV - 55 inch	Nos	4		
10	Smart TV - 75 inch	Nos	4		
11	Data Center Infrastructure Management (DCIM)	Nos	1		
12	Ultrasonic Rodent Repellent System	Nos	1		
13	Water Leak Detection System	Nos	1		
14	Intelligent Addressable Fire Alarm System	Nos	1		
15	Smoke Detection System	Nos	1		
16	Fire Suppression System	Nos	1		

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity	Unit Cost (INR) (Inclusive of all taxes)	Total Cost (INR) (Inclusive of all taxes)
			A	B	C=(A*B)
17	Master Control Unit	Nos	1		
18	Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp including substation protection and metering devices	Nos	1		
19	42U Rack (Network + Server)	Nos	8		
20	DG Set 380 KVA (D Check & Fuel Refilling)	Nos	1		
21	Advanced Building Management System (BMS)	Nos	1		
22	Structured Cabling	Lot	1		
23	Loaded Fiber Enclosure for Type I MPO Cassettes	Lot	1		
24	Passive Cabling	Lot	1		
25	Fiber Optic solutions for DC Connectivity	Lot	1		
26	Fiber Panel	Lot	1		
27	CAT6A U/UTP Cable	Lot	1		
28	24 Port Patch Panel loaded	Lot	1		
29	CAT6 I/O for loaded Patch Panel	Lot	1		
30	CAT6A Patch Cord	Lot	1		
31	MFZ Verifocal Dome	Nos	24		
32	Bullet Camera	Nos	2		
33	PTZ Camera	Nos	2		
34	Power Cables	Lot	1		
<b>C</b>	<b>Civil &amp; Interior</b>				
1	One time Site Preparation (Civil & Electrical) Cost for DC including complete site preparation of Data Centre, inclusive but not limited to false flooring, lighting fixtures, electrical works, Mason Works, Dismantling existing Wall, Doors , Window or any structure of any material etc(Refer Scope of Work for further details)	Lot	1		
2	EARTHING: Preparation of All Earth Pits, Necessary Repair, Testing earth resistivity and electrode resistance	Lot	1		
3	Electrical works - for NOC, DC, DG Set UPS and LT Panel	Lot	1		

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity	Unit Cost (INR) (Inclusive of all taxes)	Total Cost (INR) (Inclusive of all taxes)
			A	B	C=(A*B)
4	Setting up of state of the art NOC room with required Furniture and other components including false flooring, lighting fixtures, electrical works, beautifications of NOC area, wall panels, Mason Works, etc. (Refer Scope of Work for further details)	Lot	1		
<b>D</b>	<b>One time cost for Connectivity</b>				
1	One time cost for provisioning 1 GBPS MPLS Connectivity between CGSDC and DR Site	Lumpsum	1		
<b>E</b>	<b>Data Centre Certification</b>				
1	Cost for ISO 27001, ISO 20000, ISO 22301 and Surveillance Audit for the entire contract period and Recertification	Lumpsum	1		
<b>Total Cost of Table A</b>					



**Table B: Total OPEX Cost Component: \*The financial bid must be filled in excel and uploaded in Envelope C**

Sr. No.	Item Description	Total Cost (Inclusive of all Taxes) INR
1	Total Cost of AMC (B1)	B1
2	Total Cost of Manpower (B2)	B2
	Total OPEX (Value for one Quarter X 17 Quarters) (B)	B=B1+B2

**Table B1: OPEX Cost Component: Annual Maintenance Charges \*The financial bid has to be filled in excel and uploaded in Envelope C**

Sr. No.	Components	Unit of measurement	Qty	Cost for one Quarter (inclusive of all Taxes)	Total number of Quarters (17)	Total Cost for 17 Quarters (inclusive of all Taxes)
			A	B	C	D= B*C
<b>A</b>	<b>IT Components</b>					
1	Rack Server	Nos	12		17	
2	Hyper Converged Infrastructure	Nos	12		17	

Sr. No.	Components	Unit of measurement	Qty	Cost for one Quarter (inclusive of all Taxes)	Total number of Quarters (17)	Total Cost for 17 Quarters (inclusive of all Taxes)
			A	B	C	D= B*C
3	Virtualisation Software and Management Solution for Rack server Cluster	Nos	1		17	
4	Windows Operating System Data Center Edition - 16 Core License Model	Nos	36		17	
5	Redhat Linux Operating System Enterprise Edition - Socket Based	Nos	12		17	
6	MS SQL Database Enterprise Edition - Core Based	Nos	32		17	
7	Postgres SQL Enterprise Edition - Core Based	Nos	64		17	
8	Backup Hardware & Software (500 TB front end capacity or 500 VM)	Nos	1		17	
9	Server Load Balancer	Nos	2		17	
10	SDN Controller	Nos	2		17	
11	SPINE Switch	Nos	2		17	
12	Leaf switch – OFC	Nos	8		17	
13	Core Router – Internet	Nos	2		17	
14	Core Router – Intranet	Nos	2		17	
15	Management Switch	Nos	2		17	
16	Link Load balancer – Internet	Nos	2		17	
17	Link Load balancer – Intranet	Nos	2		17	
18	L2 Managed Switch for NOC	Nos	2		17	
19	SAN Switch	Nos	2		17	
20	Enterprise Storage (500 TB Usable Storage)	Nos	1		17	
21	Next Generation Firewall – Internet	Nos	2		17	
22	Next Generation Firewall – Intranet	Nos	2		17	
23	Web Application Firewall	Nos	2		17	
24	EDR - Endpoint Detection Response	Nos	500		17	
25	Identity Access Manager	Nos	500		17	

Sr. No.	Components	Unit of measurement	Qty	Cost for one Quarter (inclusive of all Taxes)	Total number of Quarters (17)	Total Cost for 17 Quarters (inclusive of all Taxes)
			A	B	C	D= B*C
26	Enterprise Monitoring System (NMS, ITSM, ISMS)	Nos	500		17	
27	Network Access Controller	Nos	2		17	
28	HSM - Hardware Security Module	Nos	2		17	
29	HIPS - Host Intrusion Prevention System	Nos	500		17	
30	NDR - Network Detection and Response	Nos	2		17	
31	DDoS	Nos	1		17	
<b>B</b>	<b>Non IT Components</b>					
1	UPS - 300 KVA with battery bank upgradable to 400 KVA	Nos	2		17	
2	Battery Bank for 300 KVA - Min 4 Hrs backup	Nos	1		17	
3	UPS - 20 KVA with Battery Bank	Nos	2		17	
4	Battery Bank for 20 KVA - Min 4 Hrs backup	Nos	1		17	
5	Split AC - 1.5 Ton	Nos	3		17	
6	Split AC - 2 Ton	Nos	2		17	
7	HVAC System - Precision Air Conditioner	Nos	4		17	
8	Biometric Door Access System	Lot	1		17	
9	Smart TV - 55 inch	Nos	4		17	
10	Smart TV - 75 inch	Nos	4		17	
11	Data Center Infrastructure Management (DCIM)	Nos	1		17	
12	Ultrasonic Rodent Repellent System	Nos	1		17	
13	Water Leak Detection System	Lot	1		17	
14	Intelligent Addressable Fire Alarm System	Nos	1		17	
15	Smoke Detection System	Lot	1		17	
16	Fire Suppression System	Lot	1		17	
17	Master Control Unit	Nos	1		17	

Sr. No.	Components	Unit of measurement	Qty	Cost for one Quarter (inclusive of all Taxes)	Total number of Quarters (17)	Total Cost for 17 Quarters (inclusive of all Taxes)
			A	B	C	D= B*C
18	Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp including substation protection and metering devices	Nos	1		17	
19	42U Rack (Network + Server)	Nos	8		17	
20	DG Set 380 KVA (D Check & Fuel Refilling)	Nos	1		17	
21	Advanced Building Management System (BMS)	Nos	1		17	
22	Structured Cabling	Lot	1		17	
23	Loaded Fiber Enclosure for Type I MPO Cassettes	Lot	1		17	
24	Passive Cabling	Lot	1		17	
25	Fiber Optic solutions for DC Connectivity	Lot	1		17	
26	Fiber Panel	Lot	1		17	
27	CAT6A U/UTP Cable	Lot	1		17	
28	24 Port Patch Panel loaded	Lot	1		17	
29	CAT6 I/O for loaded Patch Panel	Lot	1		17	
30	CAT6A Patch Cord	Lot	1		17	
31	MFZ Verifocal Dome	Lot	24		17	
32	Bullet Camera	Lot	2		17	
33	PTZ Camera	Lot	2		17	
34	Power Cables	Lot	1		17	
<b>C</b>	<b>Civil &amp; Interior</b>					
1	Maintenance Cost (Civil & Electrical)	Lot	1		17	
2	EARTHING: Maintenance of All Earth Pits, Necessary Repair, Testing earth resistivity and electrode resistance	Lot	1		17	

Sr. No.	Components	Unit of measurement	Qty	Cost for one Quarter (inclusive of all Taxes)	Total number of Quarters (17)	Total Cost for 17 Quarters (inclusive of all Taxes)
			A	B	C	D= B*C
<b>D</b>	<b>Cost of Connectivity</b>					
1	1 Gbps MPLS Link from CGSDC to DR on Cloud	Lot	1		17	
<b>Total Cost for AMC – Table B1</b>						

**Table B2: OPEX Cost Component: Manpower Services Cost** \*The financial bid has to be filled in excel and uploaded in Envelope C

S.No	Resource	Number of Resources	Cost for one quarter (inclusive of all Taxes)	Total number of Quarters	Total Cost for Manpower for 17 Quarters (inclusive of all Taxes)
		A	B	C	D= B*C
1	Project Manager - Technical	1		17	
2	System Administrator- Windows/Linux	2		17	
3	HCI Administrator	1		17	
4	Database Administrator	1		17	
5	Security Administrator	2		17	
6	Storage Administrator	1		17	
7	Core Network Engineer	2		17	

S.No	Resource	Number of Resources	Cost for one quarter (inclusive of all Taxes)	Total number of Quarters	Total Cost for Manpower for 17 Quarters (inclusive of all Taxes)
8	Backup Administrator	1		17	
9	Server Administrator	1		17	
10	Cloud Expert (Hybrid)	2		17	
11	NOC Engineer	3		17	
12	Helpdesk Support Engineer	3		17	
13	BMS Expert	3		17	
<b>Total Cost for Manpower (Table B2)</b>					

**\*Note:** The Value of Column B should include the costing of number of resources specified in Column A

**Table C: Total Cost for DR on Cloud \*The financial bid has to be filled in excel and uploaded in Envelope C**

S.No	Description	Specification	Quantity	Unit of Measurement	Indicative Duration of Usage (Not to be considered in unit price)	Unit Price (inclusive of all taxes)	Total Price (inclusive of all taxes)
			A		B	C	D=A*C
<b>Compute Pricing</b>							
		<b>vCPU</b>	<b>RAM</b>				
1	Compute [Windows]	16	56	10	Per VM per Hour	800 hours	
2	Compute [Linux]	16	56	10	Per VM per Hour	800 hours	
3	Compute [Windows]	8	56	10	Per VM per Hour	800 hours	
4	Compute [Linux]	8	56	10	Per VM per Hour	800 hours	
5	Compute [Windows]	4	32	10	Per VM per Hour	800 hours	
6	Compute [Linux]	4	32	10	Per VM per Hour	800 hours	
7	Compute [Windows] +MSSQL	16	128	10	Per VM per Hour	800 hours	
8	Compute [Linux] +MSSQL	16	128	10	Per VM per Hour	800 hours	
9	Compute [Windows] +postgresql	16	128	10	Per VM per Hour	800 hours	
10	Compute [Linux] +postgresql	16	128	10	Per VM per Hour	800 hours	

S.No	Description	Specification	Quantity	Unit of Measurement	Indicative Duration of Usage (Not to be considered in unit price)	Unit Price (inclusive of all taxes)	Total Price (inclusive of all taxes)
			A		B	C	D=A*C
11	Block Storage (in TB)	200 TB	2	Per GB per Month	5 Years		
12	Object Storage (in TB)	200 TB	2	Per GB per Month	5 Years		
13	Virtual Load Balancer	1	2	Per VLB per Month	5 Years		
14	Content Delivery Network	300 GB	1	Per GB per Month	5 Years		
15	Anti-virus	1 VM	50	Per VM per Month	5 Years		
16	Host Intrusion Detection System / Network Intrusion Prevention System	1 VM	50	Per VM per Month	5 Years		
17	Web Application Firewall (Layer 7)	1	2	Per Month	5 Years		
18	DDoS Protection Service (Layer 3 & 4)	1	2	Per Month	5 Years		
19	Identity and Access Management	1	2	Per Month	5 Years		
20	Security Incident Monitoring Services	1	2	Per Month	5 Years		
21	Cloud management & monitoring tool	1	1	Per Month	5 Years		
22	CPU, memory, and disk I/O metrics Utilization Monitoring Dashboards	1	1	Per Month	5 Years		
23	Configuration Management	1	1	Per Month	5 Years		
24	Cloud Optimization Advisor	1	1	Per Month	5 Years		
25	Site Recovery Services	1	1	Per Month	5 Years		
26	Dedicated 1 Gbps connectivity/link between CGSDC and DR site with unlimited upload & download	1	1	Per Month	5 Years		



S.No	Description	Specification	Quantity	Unit of Measurement	Indicative Duration of Usage (Not to be considered in unit price)	Unit Price (inclusive of all taxes)	Total Price (inclusive of all taxes)
			A		B	C	D=A*C
<b>One time Setup and Managed Services Cost</b>							
27	One time cost of setting up cloud infrastructure and Replication tool	1	1	Lot	One Time		
28	Cost for Managed Services for the period of Five (5) Years for providing complete management with Helpdesk tool, support & SLA monitoring for provisioned cloud infrastructure covering, not limited to VMs, Storage, OS & DBs, Backup Network & security components for the proposed DR Site	1	1	Lot	5 Years		
<b>Total Cost for Cloud Hosting for 5 Years</b>							

**Note :**

- Payments shall be made to be the bidder on an quarterly equated basis as per the actual consumption of resources as mentioned for the entire contract duration**
- Line-Item Cost quoted by Bidder for the entire Bill of Material (BoM) shall be valid for the entire contract duration**
- Bidder is mandatorily required to put cost/value against each of the Line Item; in absence of any value against the specific Line Item then the Cost for that specific line item shall be considered as Zero which shall be applicable for the entire contract duration**
- Bidder shall quote one time cost and managed services cost considering scope document of the RFP and any additional Tool/Software required to deliver the ask, then the respective Cost should be included into, either one time cost or Managed services cost head**

## Selection of Master System Integrator for Technology Refresh of CGSDC CHiPS

### Annexure-13: Format for Performance Bank Guarantee

(To be issued by a Bank)

This Deed of Guarantee executed at ----- by ----- (Name of the Bank) having its Head/ Registered office at ----- (hereinafter referred to as "the Guarantor") which expression shall unless it be repugnant to the subject or context thereof include its heirs, executors, administrators, successors and assigns;

In favour of CEO, Chhattisgarh Infotech & Promotion Society (hereinafter called "CHiPS" which expression shall unless it be repugnant to the subject or context thereof include its heirs, executors, administrators, successors and assigns);

<Organization name > a company registered in India under the Companies Act, 1956 or Companies Act 2013 or as amended and having its Registered Office at -----, India (herein referred to as the "MSI" for CGSDC 2.0, for Chhattisgarh, for the work order number ---- dated --- - issued by CHiPS and selected < Organization name > (hereinafter referred to as the MSI) for the Contract by CHiPS as more specifically defined in the aforementioned Document including statement of work and the Contract executed between the CHiPS and MSI. The Contract requires the MSI to furnish an unconditional and irrevocable Bank Guarantee for an amount of INR ----/- (Rupees -----) by way of security for guaranteeing the due and faithful compliance of its obligations under the Contract.

Whereas, the MSI approached the Guarantor and the Guarantor has agreed to provide a Guarantee being these presents:

Now this Deed witnessed that in consideration of the premises, we, ----- Bank hereby guarantee as follows:

1. The MSI shall implement the Project, in accordance with the terms and subject to the conditions of the Contract, and fulfil its obligations there under
2. We, the Guarantor, shall, without demur, pay to CHiPS, an amount not exceeding of INR ----/- (Rupees ----) within 21(Twenty One) days of receipt of a written demand therefore from CHiPS stating that the MSI has failed to fulfil its obligations as stated in Clause 1 above
3. The above payment shall be made by us without any reference to the MSI or any other person and irrespective of whether the claim of the CHiPS is disputed by the MSI or not
4. The Guarantee shall come into effect from ----- (Start Date) and shall continue to be in full force and effect till the earlier of its expiry at 1700 hours Indian Standard Time on (Expiry Date) (both dates inclusive) or till the receipt of a claim, from Chhattisgarh Infotech & Promotion Society under this Guarantee, whichever is earlier. Any demand received by the Guarantor from CHiPS prior to the Expiry Date shall survive the expiry of this Guarantee till such time that all the moneys payable under this Guarantee by the Guarantor to CHiPS.
5. In order to give effect to this Guarantee, CHiPS shall be entitled to treat the Guarantor as the principal debtor and the obligations of the Guarantor shall not be affected by any variations in the terms and conditions of the Contract or other documents by CHiPS or by the extension of time of performance granted to the MSI or any postponement for any time of the power exercisable by CHiPS against the MSI or forbear or enforce any of the terms and conditions of the Contract and we shall not be relieved from our obligations under this Guarantee on account of any such variation, extension, forbearance or omission on the part of MSI or any indulgence by CHiPS to the MSI to give such matter or thing whatsoever which under the law relating to sureties would but for this provision have effect of so relieving us.
6. This Guarantee shall be irrevocable and shall remain in full force and effect until all our obligations under this guarantee are duly discharged
7. The Guarantor has power to issue this guarantee and the undersigned is duly authorized to execute this Guarantee pursuant to the power granted under -----

In witness, whereof the Guarantor has set its hands hereunto on the day, month and year first here-in-above written.

Signed and Delivered by ----- Bank by the hand of Shri ----- its ----- and authorised office.

Authorised Signatory ----- Bank

#### Annexure-14: Format for Manufacturer Authorization Letter (on OEM's Letterhead)

To,  
Chief Executive Officer  
Chhattisgarh Infotech Promotion Society (CHiPS)  
SDC Building, 02nd floor, Near Police Control Room,  
Civil Lines, Raipur, Chhattisgarh-492001

Subject: Manufacturer Authorization Letter for Selection of Master System Integrator (MSI) for CGSDC2.0 Project in the State of Chhattisgarh with Tender Reference No.

.....  
Sir,  
We, <OEM Name> having our registered office at <OEM address>, hereinafter referred to as OEM are an established manufacturer of the following items quoted by <MSI Name> having their registered office at <MSI address>, hereinafter referred to as MSI.

We <OEM Name> authorize <MSI's name> to quote our product for above mentioned tender as our Authorized Indian Agent.

We confirm that we have understood the delivery & installation time lines defined in the tender. We confirm that we have worked out all necessary logistics and pricing agreement with <MSI name>, and there won't be any delay in delivery, installation and support due to any delay from our side. Our full support as per pre-purchased support contract is extended in all respects for supply and maintenance of our products. We also ensure to provide the required spares and service support as pre-purchased for the supplied equipment for entire contract. In case of any difficulties in logging complaint at MSI end, user shall have option to log complaint at our call support centre.

We also undertake that in case of default in execution of this Contract by MSI, we shall provide necessary extended support to the new partner in accordance with the Contract Terms in identifying another authorized partner with similar certifications/capabilities and extend support to the new partner in accordance with OEM's agreement with the new partner. In case MSI is unable to fulfil the obligations given under this Contract, OEM shall be responsible to replace the MSI with an alternate Indian Authorized agent to facilitate to get the requisite work done. OEM shall also ensure that the alternate Indian Authorized Agent in this case shall abide by all the terms & conditions laid down under the Contract and during the Award of Work to the MSI for the quoted OEM products.

If any product is declared end of sale, we shall proactively ensure that a suitable equivalent or higher roll over product is offered through the existing MSI to CHiPS for due approval, contract and order executions thereafter.

We understand that any false information/commitment provided here may result in <OEM's Name> getting blacklisted/debarred from doing business with CHiPS.

Yours sincerely,  
Authorized Signature [In full and initials]: \_\_\_\_\_  
Name and Title of Signatory: \_\_\_\_\_  
Name of Firm: \_\_\_\_\_  
Address: \_\_\_\_\_  
Location: \_\_\_\_\_ Date: \_\_\_\_\_

**NOTE:**

- i. The letter should be submitted on the letter head of the manufacturer / OEM and should be signed by the authorized signatory.
- ii. Any deviation would lead to summarily rejection of bid

## Annexure-15: Non-Disclosure Agreement (NDA)

### **NON- DISCLOSURE AGREEMENT FOR EXCHANGE OF CONFIDENTIAL INFORMATION**

This Non-Disclosure Agreement for Exchange of Confidential Information (the “Agreement”) is entered into as of \_\_\_\_\_ DD, 2024 (the “Effective Date”) by and between Chhattisgarh Infotech Promotion Society (CHiPS), hereinafter referred to as ‘**Nodal Agency**’ referred as the Nodal Agency company having its registered office at SDC Building, 02nd floor, Near Police Control Room, Civil Lines, Raipur, Chhattisgarh–492001

And

<\*\*\*>, a Company incorporated under the Companies Act, 1956, having its registered office at <\*\*\*> (hereinafter referred to as ‘**the Master System Integrator**’ (**MSI**) which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the ‘Parties’ and individually as a ‘Party’.

Whereas:

1. Nodal Agency is desirous to implement the project of “SDC Upgrade in the State of Chhattisgarh”
  2. The Nodal Agency and Implementation Agency have entered into a Master Services
  3. Agreement dated <\*\*\*> (the “MSA”) as well as a Service Level Agreement dated <\*\*\*> (the “SLA”) in furtherance of the Project.
  4. Whereas in pursuing the Project (the “Business Purpose”), a Party (“Disclosing Party”) recognizes that they will disclose certain Confidential Information (as defined hereinafter) to the other Party (“Receiving Party”).
  5. Whereas such Confidential Information (as defined hereinafter) belongs to Receiving Party as the case may be and is being transferred to the Disclosing Party to be used only for the
  6. Business Purpose and hence there is a need to protect such information from unauthorized use and disclosure.
1. Term: This Agreement shall have a term of five (8) years from the Effective Date. Either Party may request for an extension of the Term by giving a renewal notice to the other Party. The Parties may agree to extend the Term of Agreement by an instrument in writing.

#### **2. SCOPE OF THE AGREEMENT**

- a. *This Agreement shall apply to all confidential and proprietary information disclosed by Disclosing Party to the Receiving Party and other information which the disclosing party identifies in writing or otherwise as confidential before or within (30) thirty days after disclosure to the Receiving Party (“Confidential Information”). Such Confidential Information consists of certain specifications, documents, software, prototypes and/or technical information, and all copies and derivatives containing such Information that may be disclosed to the Disclosing Party for and during the Business Purpose, which a party considers proprietary or confidential.*
  - b. *Such Confidential Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to the Receiving Party.*
3. Purpose: The Parties intend to share Confidential Information for a potential business relationship with respect to implementation of “SDC Upgrade project in the State of Chhattisgarh”. (“Purpose”).
  4. Discloser & Recipient: Either Party, including its Affiliates, may disclose Confidential Information under this Agreement for the Purpose and shall be referred to as “Discloser” hereunder. The other Party, including its Affiliates, receiving Confidential Information hereunder shall be referred to as “Recipient”. For the purpose of this Agreement, “Affiliates” shall mean any legal entity which, is directly or indirectly controlling, controlled by or under the common control of the Party.

5. Confidential Information: The information disclosed by Discloser to Recipient hereunder relating to Discloser's business, including, without limitation, computer programs, technical drawings, algorithms, know-how, processes, designs, reports, specifications, ideas, trade secrets, inventions, schematics, pricing information, and other technical, business, financial, customer and product development plans, strategies or any other information which is reasonably understood to be confidential or proprietary based on the circumstances of disclosure or the nature of the information itself, such information is hereinafter referred to as "Confidential Information" of the Discloser.
6. Information which is orally or visually disclosed, or is disclosed in writing without being marked as confidential, shall constitute Confidential Information, if Discloser within seven (7) days after such disclosure, delivers to Recipient, a written document(s) describing such Information and referencing the place and date of such oral or visual disclosure and the names of the employees or officers of the Recipient to whom such disclosure was made.
7. Confidential Information shall not include any information that is a) lawfully known by the Recipient at the time of disclosure without any obligation to keep the same confidential; b) or becomes, through no fault of the Recipient, known or available to the public; c) independently developed by the Recipient without use or reference to such Confidential Information; or d) rightfully disclosed to Recipient by a third party without any restrictions on disclosure.
8. Confidentiality Obligation: Discloser shall observe the duty of reasonable care while disclosing any Confidential Information to the Recipient. Recipient agrees that it shall a) not use any such Confidential Information except for the Purpose of this Agreement; b) hold the Confidential Information in confidence and shall take all reasonable precautions to protect such Confidential Information from unauthorized disclosure including all precautions that Recipient employs to protect its own confidential material; c) not divulge any such Confidential Information to any third party without prior approval of Discloser; and d) not copy or reverse engineer any such Confidential Information. Recipient may permit access to Confidential Information to its employees, consultants, vendors and agents, on a need to know basis and to the extent required to meet the Purpose, and shall ensure that they are bound to maintain confidentiality of such Confidential Information to the same extent as provided under this Agreement.
9. Survival, Exception & Return: Confidentiality obligations under this Agreement shall survive for a period of five (5) years following the expiry of this Agreement, provided that the obligations shall be perpetual with regard to any source code or trade secret that may be disclosed hereunder.
10. Recipient may make disclosures to the extent required by law or by order of any court or regulatory body, provided the Recipient promptly notifies the Discloser in writing about such requirement to disclose.
11. Recipient will return to Discloser, upon request, any Confidential Information under its possession or control and/or destroy all documents or media containing any such Confidential Information provided that Recipient may retain a copy of Confidential Information to the extent necessary to meet any statutory requirements.
12. Disclaimer: Parties acknowledges that providing or receiving Confidential Information under this Agreement shall not constitute an offer, acceptance, or promise to enter into or amend any other contract.
13. To the extent permitted by law, Confidential Information is disclosed on "as is" basis, without any express or implied warranties and in particular, without any limitation, as to fitness for the intended Purpose.
14. The ownership of all intellectual property rights (IPRs) in Confidential Information disclosed hereunder shall remain with its original owner and no grant of license or conveyance of any IPRs in such Confidential Information is to be implied from exchange or sharing of any such information under this Agreement.
15. Injunctive Relief: Recipient acknowledges that due to the unique nature of the Discloser's Confidential Information, any breach of its obligations hereunder will result in irreparable harm to the Discloser, and therefore, upon any such breach or threat thereof, the Discloser shall be entitled to appropriate equitable relief including the relief of injunction and/or specific performance, in addition to any other remedies available at law.

- 
16. General: The Parties agree to be bound by any applicable export control regulations while sharing Confidential Information hereunder.
  17. This Agreement shall be governed by the laws of India and shall be subject to the exclusive jurisdiction of courts in Chhattisgarh.

Neither party may assign or transfer any rights or obligations arising out of this Agreement without the prior written consent of the other party.

No failure or delay in enforcing any right will be deemed a waiver unless made in writing and signed by a duly authorized representative of such Party.

Any notice under this Agreement shall be in writing and shall be sent at the registered addresses of the Parties specified in this Agreement.

This Agreement may be modified only by an amendment executed in writing by a duly authorized representative of both Parties.

This Agreement constitutes the entire agreement between the Parties and supersedes all prior discussions or agreements relating to subject matter hereof.

For [Chhattisgarh Infotech Promotion Society \(CHiPS\)](#),

Signature: \_\_\_\_\_  
Name: \_\_\_\_\_  
Designation: \_\_\_\_\_  
Date: \_\_\_\_\_

For [Master System Integrator' \(MSI\)](#)

Signature: \_\_\_\_\_  
Name: \_\_\_\_\_  
Designation: \_\_\_\_\_  
Date: \_\_\_\_\_

\*\*\*\* End of Document \*\*\*\*

---

## Annexure -16: Compliance to Technical Specifications on OEM Letterhead

To,  
Chief Executive Officer  
Chhattisgarh Infotech Promotion Society (CHiPS)  
SDC Building, 02nd floor, Near Police Control Room,  
Civil Lines, Raipur, Chhattisgarh-492001

Subject: Compliance to Technical Specifications of IT & Non-IT Components mentioned in this  
RFP - Tender Reference No. ....

Sir,  
We, <OEM Name> having our registered office at <OEM address>, hereinafter referred to as OEM  
are an established manufacturer of the following items quoted by <MSI Name> having their  
registered office at <MSI address>, hereinafter referred to as MSI.

We <OEM Name> authorize <MSI's name> to quote our product for above mentioned tender as  
our Authorized Indian Agent.

We confirm that we have understood the delivery & installation time lines defined in the tender. We  
confirm that we have worked out all necessary logistics and pricing agreement with <MSI name>,  
and there won't be any delay in delivery, installation and support due to any delay from our side.  
Our full support as per pre-purchased support contract is extended in all respects for supply and  
maintenance of our products. We also ensure that all the components to be supplied as per scope  
of this tender fully comply with the technical specifications mentioned in the Technical Specification  
section (Annexure 17).

We understand that any false information/commitment provided here may result in <OEM's Name>  
getting blacklisted/debarred from doing business with CHiPS.

Yours sincerely,  
Authorized Signature [In full and initials]: \_\_\_\_\_  
Name and Title of Signatory: \_\_\_\_\_  
Name of Firm: \_\_\_\_\_  
Address: \_\_\_\_\_  
Location: \_\_\_\_\_ Date: \_\_\_\_\_

### NOTE:

- i. The letter should be submitted on the letter head of the manufacturer / OEM and should be  
signed by the authorized signatory.
- ii. Any deviation would lead to summarily rejection of bid

## Annexure-17: Technical Specifications

### A. IT Components

#### 17.1 "Technical Requirements Specifications - Hardware-Rack Server"

Product Name: Rack Server

Sr. No.	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
RS.REQ.001	2U rack server with rail-kits for 19" industry standard racks		
RS.REQ.002	Server should have 2 socket, proposed processor should be with at least 2.8 GHz or better, 64-bit x86 latest generation processor with 24 Core each socket. (MSI may size CPU cores based on the server roles and meeting SLA)		
RS.REQ.003	Should be populated with at least populated with at least 512 GB latest DDR RAM memory in balanced/near-balanced memory mode. Offered server must support features like ECC & memory mirroring		
RS.REQ.004	4 x 960 GB drives or higher.		
RS.REQ.005	2x1/10G Ethernet ports 2x 10G/25G SFP fibre ports 2 x 32G Fiber Channel Ports with Transceivers		
RS.REQ.006	Must be certified under Windows Server 2019, RHEL, SLES, Oracle Linux, VMware ESXi		
RS.REQ.007	Proposed server should be IPv6 Compliant.		
RS.REQ.008	All the accessories required for installation of configuration of the servers like Cables, Rails of installations, Cable Manager, PDUs etc. must be supplied with the servers.		
RS.REQ.009	Cryptographically signed firmware, UEFI Secure Boot, Chassis intrusion detection		
RS.REQ.010	Redundant hot-swappable dual power supplies and Fan		
RS.REQ.011	24x7 single point of OEM support for hardware & associated software for a period of 5 years. Any issues reported must be resolved within the same business day.		
RS.REQ.012	Integrated RAID controller offering Striping, Mirroring (RAID 0, 1, 5 and 6)		
RS.REQ.013	Server should support upto eight PCI Express slots		
RS.REQ.014	Equipment should be best in class about cooling and power efficiency		
RS.REQ.015	Proposed server should support pre-failure alert i.e., should provide predictive failure monitoring & proactive alerts of actual or impending component failure like fan, power supply, etc.		
RS.REQ.016	Proposed server should be better in terms of capacity performance, and features with latest offering from the proposed OEM.		



## 17.2 "Technical Requirements Specifications - HCI Node"

Product Name: HCI Node & HCI Software

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>HCIS.REQ.001</b>	The proposed HCI solution shall support scalability up to 8/16/64 hyper converged nodes (Compute + Storage) or more in a single cluster. N+1 redundant power supplies & cooling fans. Solution shall support intel latest processor of 2x24 Core @2.8Ghz or better processor with 512GB RAM and 2x32Gbps HBA. The HCI cluster should have 500 usable cores and 500TB SSD/NVME Storage capacity.		
<b>HCIS.REQ.002</b>	Bidder need to consider minimum 24x10Gbps SFP + port (fully Loaded) Switches in HA		
<b>HCIS.REQ.003</b>	The solution should include bare metal hypervisor with functionality of HA, Zero Downtime & Zero Data-loss without any clustering solution, encrypted live migration of VMs, inbuilt distributed switch, VM level encryption, Network and Storage I/O Control, VM based replication.		
<b>HCIS.REQ.004</b>	Virtualization solution should have heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Oracle Linux, Ubuntu and CentOS, Solaris x86)		
<b>HCIS.REQ.005</b>	The solution should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.		
<b>HCIS.REQ.006</b>	The solution should provide proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs		
<b>HCIS.REQ.007</b>	Should provide a centralized virtual switch which span across a virtual data-centre and multiple hosts should be able to connect to it. This should simplify and enhance virtual-machine networking in virtualized environments.		
<b>HCIS.REQ.008</b>	The solution should provide capabilities of Hot Add (CPU, Memory & devices) to virtual machines when needed, without disruption or downtime in working for both windows and Linux based VMs		
<b>HCIS.REQ.009</b>	Virtualization manager should be highly available with out of box HA without any dependency on external shared storage or load balancer.		
<b>HCIS.REQ.010</b>	The solution should provide integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware solutions without the need for agents inside the virtual machines.		
<b>HCIS.REQ.011</b>	The solution should enforce security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	address changes, and forged source MAC transmits.		
HCIS.REQ.012	The solution should provide solution to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers.		
HCIS.REQ.013	The solution should be able to create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.		
HCIS.REQ.014	The solution should provide with adequate licenses to meet solution requirement.		
HCIS.REQ.015	The solution should automate and provision data-centre services such as compute, storage, networking, backup, replication, load balancing, NAT, fault tolerance, security, stateful firewall, etc.		
HCIS.REQ.016	The solution should have a capability to extend to public cloud platforms.		
HCIS.REQ.017	The solution should provide creation of services such as 'Single VM' and a 'multi-tier application infrastructure (including software based constructs such as load balancers)' as part of a standard template with constructs like virtual switch, virtual router, firewall, load balancer etc.		
HCIS.REQ.018	The solution should provide multiple levels of approval with E-mail notifications with ability to automate manual provisioning and deprovisioning of the tasks and policies embedded in each layer of their application.		
HCIS.REQ.019	The solution should allow administrators to manage and reserve (allocate a share of the memory, CPU and storage) resources for a group of virtual machines to use.		
HCIS.REQ.020	The solution should integrate with software defined networking for auto provisioning of networks including ability to automate delivery of virtual networking & virtual security services such as switching, routing, stateful firewalling, VPN, NAT, DHCP and load-balancing.		
HCIS.REQ.021	The solution should provide horizontal and vertical scaling.		
HCIS.REQ.022	The solution should provide intent based workload balancing across clusters and ability to automatically take corrective action or call to external systems to effect change (workflow), open/close tickets or wait for approvals etc.		
HCIS.REQ.023	The solution should have inbuilt orchestrator platform to build the custom workflow for complex tasks and Day-2 operations and also integrated configuration management capabilities to build the custom states for complex tasks for OS and Applications.		
HCIS.REQ.024	The solution should enforce IT regulatory standards with integrated compliance and		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	automated drift remediation and adherence to common requirements out-of-the box compliance templates and also create own custom templates.		
<b>HCIS.REQ.025</b>	Should allow connecting to data-center ecosystem components e.g., operating systems, applications, servers, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyse logs at scale.		
<b>HCIS.REQ.026</b>	Should provide intelligent log analytics to be able to bring unstructured and structured data together, for enhanced end-to-end operations management, collect and analyse all types of machine-generated log data, for example, network traces, configuration files, messages, performance data, system state dumps, and more.		

### 17.3 "Technical Requirements Specifications - Hyper Converged Infrastructure"

Product Name: HCI Cluster

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>HCIC.REQ.001</b>	The proposed solution should be a Hyper Converged infrastructure which should come preinstalled with all software required to meet the requirement mentioned in RFP including SDS (Software Defined Storage), replication with management and associated hypervisor. It should include all hardware and software necessary to ensure high availability mode of operation. The proposed hyper converged system should have Single Management Console to manage integrated Compute, Storage, Hypervisor & Cluster. All nodes must be HCI nodes.		
<b>HCIC.REQ.002</b>	Technology must be software defined and the solution should provide enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network & associated components such as SAN Switches & HBAs		
<b>HCIC.REQ.003</b>	The storage solution with the HCI should either have inbuilt software defined storage capability integrated within the Hypervisor kernel itself or should use a virtual storage controller architecture.		
<b>HCIC.REQ.004</b>	Hypervisor layer should directly sit on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability and security. It should be Industry Standard software and no special purpose software is allowed.		
<b>HCIC.REQ.005</b>	The HCI solution should be able to scale by adding additional nodes to the cluster at a later point of time to handle compute, Memory & Storage requirements. Solution should support cluster expansion with zero down time.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
HCIC.REQ.006	Data compression, deduplication, erasure coding techniques should be available with licenses in the Software Defined Storage (SDS) layer for use without additional cost.		
HCIC.REQ.007	The HCI solution should provide seamless upgrade for Firmware, Hypervisor, Storage OS, SDS software, BIOS and other such functions which are required in the HCI platform. The upgrade should be online and should not mandate any kind of OEM engagement		
HCIC.REQ.008	The HCI solution should support 3rd party Enterprise Backup Solution of all leading OEMs.		
HCIC.REQ.009	The HCI Solution should provide a backup catalogue to allow any Virtual Server to be recovered to any specific point-in-time.		
HCIC.REQ.010	The HCI solution must provide the following Disaster Recovery features and all licenses should be included from day 1. 1. The solution must provide a simple failover operation 2. The solution must allow creation of a Run book to automate recovery of Virtual Servers		
HCIC.REQ.011	Should be compatible with Disaster Recovery solutions (DR on Cloud)		
HCIC.REQ.012	The HCI solution should support to connect external storage devices (like NAS/ SAN etc.) and should be useable as part of the HCI Solution, for the purpose of Backup.		
HCIC.REQ.013	HCI solution should provide High Availability & It should support features like snapshots & cloning of individual virtual machines.		
HCIC.REQ.014	HCI solution should support live migration of running virtual machines from one physical node to another with zero downtime, continuous service availability, and complete transaction integrity transparent to users.		
HCIC.REQ.015	Dashboard to manage and provision virtual machines, network, storage, monitor performance and manage events & alerts. It should also contain a dashboard for monitoring & generate reports.		
HCIC.REQ.016	The HCI solution should have a single management console for managing compute, Network, Storage and Clustering. The HCI Solution should be able to give insight of underlying infrastructure like compute, storage and network.		
HCIC.REQ.017	In the event of a node failure, virtual machines should automatically run on another node.		
HCIC.REQ.018	HCI solution should include Redundant 10G switches providing minimum 48 ports (referred as Leaf Switch') with minimum 4 uplink ports of 10G & 2 uplink ports of 40Gper switch.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
HCIC.REQ.019	All the required cables & modules for connecting all HCI nodes to HCI switch should be configured with redundancy in order to ensure HA.		
HCIC.REQ.020	Bidder must quote appropriate license to enable and meet mentioned features in the infrastructure automation architecture.		
HCIC.REQ.021	All licenses required for Memory and Storage upgradation with-in the provided solution should be included from Day-1		
HCIC.REQ.022	HCI solution has to integrate with active directory (AD) /open LDAP to allow importing existing users and groups in addition to creation of local users.		
HCIC.REQ.023	HCI solution should include an application and infrastructure performance management tool quoted as part of the solution to improve operations and provide insight deep infrastructure performance.		
HCIC.REQ.024	Solution should support with Active-Active stretch cluster to support even near zero for future purposes. Should have redundancy within site and across site without any extra cost.		
HCIC.REQ.025	The proposed HCI solution must have capability to provide 80% of the IOPS of respective node to any single VM.		
HCIC.REQ.026	Hypervisor should support both features like Network Virtualization Generic Routing Encapsulation (NVGRE) and Virtual Extensible LAN (VXLAN).		
HCIC.REQ.027	Humidity: 10% to 85% non-condensing & Operating temperature: 0 to 40 degrees		

#### 17.4 "Technical Requirements Specifications - Enterprise Storage "

Product Name: Enterprise Storage

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
ES.REQ.001	The storage should have Symmetric Active-Active Controller architecture where a LUN should be accessible by all the offered controllers simultaneously.		
ES.REQ.002	The proposed storage should be enterprise class having Dual controller and scalable upto 8 controllers.		
ES.REQ.003	The Storage Systems should be Enterprise Class Storage System and supplied with usable capacity, with TLC/MLC NVMe Drives in RAID 6		
ES.REQ.004	The proposed storage should support 7.6TB, 15TB TLC/MLC NVMe Drives.		
ES.REQ.005	The proposed storage should be configured with 500TB total usable capacity with RAID 6		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
ES.REQ.006	Solution should have De-Duplication functionality min 2.0 x, so that there is no performance impact. It should be possible to enable or disable data reduction functionality on volumes for specific applications or group of volumes as and when required.		
ES.REQ.007	The supported Storage should have NVMe Back-End Disk Interface and Links. The Storage should be End-to-End NVMe ready. Any additional hardware or licenses required for End-to-End NVMe should be supplied with day 1.		
ES.REQ.008	Storage should be capable of dedupe and compression to avail at least twice of the effective capacity for configured physical usable capacity.		
ES.REQ.009	The storage model offered should be capable of supporting upto 3 Lakhs or above IOPS		
ES.REQ.010	Storage System should have multiple Hot Spares. At least One Hot spare disk should be provided		
ES.REQ.011	Storage should Support 16x16Gbps/32Gbps FC ports for host connectivity and also 8x25/10 Gbps ethernet ISCSI or equivalent as per the solution requirement		
ES.REQ.012	The storage system should have minimum 1024 GB of DRAM Cache. DRAM cache should be scalable upto 6 TB. Only write cache must be mirrored. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache.		
ES.REQ.013	The storage should be with No Single Point of Failure (SPOF). All the components should be redundant and hot swappable including power supply, fans, etc.		
ES.REQ.014	The storage system should have support for multi-path configuration for redundant path to connected hosts. Any Licenses required for this should be provided with Storage.		
ES.REQ.015	The storage should have protection of cache data during a power failure by destaging the data in cache to non-volatile Memory or Disk. This memory should be equivalent to proposed as per DRAM. Adequate battery backup should be provided to destage the data from cache to non-volatile Memory or Disk.		
ES.REQ.016	The storage should be able to generate audit logs to record activities including host-initiated actions, physical component changes, attempts blocked by security control.		
ES.REQ.017	The storage should support multiple operating systems and clusters such as Windows, Unix, Linux, Solaris etc. on a single port		
ES.REQ.018	Storage should support virtual Storage APIs for Array Integration for offloading the storage tasks, including but not limited to VMWare, Microsoft, Containers, Open Stack, etc.		
ES.REQ.019	The storage should be supplied with Storage management, virtual/thin provisioning, snapshot,		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	clone and other required software to meet the technical requirements. Licenses to be supplied for Unlimited capacity.		
ES.REQ.020	The storage should be able to provide Quality or Service (QOS) to ensure bandwidth is allocated to desired servers or ports, storage should be capable of restricting IOs or throughput to LUNs or Volumes.		
ES.REQ.021	The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at least 1000.Solution should support application consistent point in time copies for MS SQL, PostgreSQL or equivalent databases etc		
ES.REQ.022	Vendor shall offer encryption and shall meet FIPS 140-2 – Level 2 security requirements.		
ES.REQ.023	The proposed solution should support public cloud API to tier or Disaster recovery on public cloud.		
	<b>Storage Management Features</b>		
ES.REQ.024	Centralized Storage management software should be browser based/ web enabled accessible over IP		
ES.REQ.025	Storage management software should have roles-based access for user accounts to manage and monitor the storage system		
ES.REQ.026	Storage management software should provide simplified user interface and wizards to perform configuration operations like create LUNs, Pools, Tiers, present LUNs to host, etc.		
ES.REQ.027	Storage management software should be able to Orchestrate and Automate storage configuration operations		
ES.REQ.028	Storage Management software should be able to define storage-centric data replication policies and automate the storage-based replications		
ES.REQ.029	Storage management software should be able to monitor alerts for automated or manually set performance thresholds		
ES.REQ.030	Storage solution shall support data at rest encryption as well as data in flight encryption.		
ES.REQ.031	5 years on-site comprehensive OEM Warranty with 24X7 access to OEM product support.		

### 17.5 "Technical Requirements Specifications - Virtualisation Software and Management Solution for Rack server Cluster - Software"

Product Name: Virtualisation Software and Management Solution for Rack server Cluster for Rack Server Cluster



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>VSMS.REQ.001</b>	Virtualisation software and management console shall provide a single view of all virtual machines, allow monitoring of system availability and performance and automated notifications with email alerts.		
<b>VSMS.REQ.002</b>	Virtualisation software and management should provide the core administration interface. This interface should be flexible and robust and should simplify the virtualisation control through shortcut navigation, custom tagging, enhanced scalability, and the ability to manage from any web browser enabled devices.		
<b>VSMS.REQ.003</b>	The management software should provide means to perform quick, as-needed deployment of additional hypervisor hosts.		
<b>VSMS.REQ.004</b>	The software should have capability to simplify host deployment and compliance by creating virtual machines from configuration templates.		
<b>VSMS.REQ.005</b>	Power, storage related, and OS cluster related information has to initiate from the relevant sources and can be integrated through RESTful APIs or equivalent.		
<b>VSMS.REQ.006</b>	The console shall provide reports for performance and utilization of Virtual Machines.		
<b>VSMS.REQ.007</b>	The console shall provide capability to monitor and analyze virtual machines, and server utilization and availability with detailed performance graphs.		
<b>VSMS.REQ.008</b>	The console shall maintain a record of configuration changes and the administrator who initiated them.		
<b>VSMS.REQ.009</b>	The console shall provide the Manageability of the complete inventory of virtual machines, and physical servers with greater visibility into object relationships.		
<b>VSMS.REQ.010</b>	The software should provide a search function to access the entire inventory of multiple instances of virtualisation management server, including virtual machines, hosts, data stores and networks, anywhere from within virtualisation management server.		
<b>VSMS.REQ.011</b>	The software should support user role and permission assignment (RBAC).		
<b>VSMS.REQ.012</b>	The software should allow to deploy and export virtual machines, virtual appliances in Open Virtual Machine Format (OVF).		
<b>VSMS.REQ.013</b>	The software should allow reliable and non-disruptive migrations for Physical/ Virtual machines running Windows or Linux (any flavour) based operating systems to virtual environment.		
<b>VSMS.REQ.014</b>	The software should include provision for host patch management with no VM downtime.		
<b>VSMS.REQ.015</b>	The software should support both features like Network Virtualization Generic Routing		



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	Encapsulation (NVGRE) and Virtual Extensible LAN (VXLAN).		
<b>VSMS.REQ.016</b>	The software shall provide a virtualisation layer that sits directly on the quoted hardware with no dependence on a general-purpose OS for greater reliability and security		
<b>VSMS.REQ.017</b>	The software shall have High Availability capabilities for the virtual machines if in case one server/Node fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualisation software		
<b>VSMS.REQ.018</b>	The software should support for increasing capacity by adding CPU, Memory or any other devices to virtual machines on an as needed basis without any disruption in working VMs running Windows and Linux operating system.		
<b>VSMS.REQ.019</b>	The software shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines		

## 17.6 "Technical Requirements Specifications - Backup Hardware & Software"

Product Name: Backup Hardware & Software

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>A</b>	<b>Hardware</b>		
<b>BKHW.REQ.001</b>	<b>Capacity:</b> Proposed backup solution should be sized appropriately for backup of <b>500TB</b> Hardware. <b>Scalability:</b> The appliance should be quoted with adequate provision for future capacity expansion of minimum <b>1000TB</b> .		
<b>BKHW.REQ.002</b>	Proposed appliance should be able to interface with various industry leading server platforms, operating systems and must support LAN/SAN based backup via FC, and iSCSI protocols.		
<b>BKHW.REQ.003</b>	Proposed appliance should support integration with quoted backup software and should support source side deduplication so that only changed blocks travel through network from source host to backup device.		
<b>BKHW.REQ.004</b>	Proposed appliance should support retention lock feature which ensures that no data is deleted accidentally or deliberately. Even Administrator should not be able to delete the data deliberately & accidentally.		
<b>BKHW.REQ.005</b>	The proposed storage array must support data-at-rest encryption.		
<b>BKHW.REQ.006</b>	Backup solution should have security feature which ensures that even administrator is not able		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	to delete the backup data deliberately or accidentally till the retention period of the backup data is expired in backup appliance. The security feature should also protect against NTP hacking/compromise.		
<b>BKHW.REQ.007</b>	The backup solution should support for ease of user rights management along with role-based access control to regulate the level of management in multi-tenant environment		
<b>BKHW.REQ.008</b>	The Proposed hardware should have 4 x 10 Gbps, 8x32Gbps ports, support LACP/aggregation of LAN ports, RAID 6 . Dual Controller/Engine/Node, Cache - Min. 512 GB.		
<b>BKHW.REQ.009</b>	Proposed backup software should be available on various OS platforms like Windows, Linux, HP-UX, IBM AIX, Solaris etc. The backup server should be compatible to run on Windows/ Linux OS platforms.		
<b>BKHW.REQ.010</b>	The proposed backup software should support restore a single VM, single file from a VM, a VMDK restore from the same management console for ease of use.		
<b>BKHW.REQ.011</b>	The proposed backup solution should have in-built feature for extensive alerting and reporting with pre- configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.		
<b>BKHW.REQ.012</b>	The proposed backup software should have the capability for block-based backups with granular recovery capability for Windows, Linux, Hyper-V, VMWARE and Exchange for faster backups on supported Disk platforms.		
<b>BKHW.REQ.013</b>	The proposed backup solution should provide search capability from a web portal to allow search for a single file from complete backup store.		
<b>BKHW.REQ.014</b>	The proposed backup solution should support completing backup speed of 10TB/hour.		
<b>BKHW.REQ.015</b>	Operating temperature: 0 to 40 degrees		
<b>BKHW.REQ.016</b>	Humidity: 10% to 85% Non-condensing		
<b>B</b>	<b>Backup Software (500 TB front end capacity or 500 VM)</b>		
<b>BKSW.REQ.001</b>	Backup software should support for Virtual machine and volume backup		
<b>BKSW.REQ.002</b>	Bidder need to provide the 500 front end capacity or 500 VM license		
<b>BKSW.REQ.003</b>	Integrates in Cloud platform for Tenant self-service		
<b>BKSW.REQ.004</b>	Supports application awareness		
<b>BKSW.REQ.005</b>	Protects VMs and volumes		
<b>BKSW.REQ.006</b>	Tenants can recover single files from backups		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>BKSW.REQ.007</b>	Supports need for full workload restore to other Tenants/Clouds for test/dev refresh		
<b>BKSW.REQ.008</b>	Multi tenancy support		
<b>BKSW.REQ.009</b>	Backup scheduler		
<b>BKSW.REQ.010</b>	Supports workload re-configuration		
<b>BKSW.REQ.011</b>	Support for backup of boot and data volumes (boot and data) for VMs		
<b>BKSW.REQ.013</b>	Backups can be full or incremental		
<b>BKSW.REQ.014</b>	Can roll through a full retention period		
<b>BKSW.REQ.015</b>	Role based permissions		
<b>BKSW.REQ.016</b>	Integration with Dashboard with Role-based actions and self-service		
<b>BKSW.REQ.017</b>	Support for backup and restore part of a cluster by using namespaces or label selectors.		
<b>BKSW.REQ.018</b>	The Backup software should support integration and connectivity with Tape Library and any 3rd Party disk-based storage solution for the long-term backup.		
<b>BKSW.REQ.019</b>	Redeployment Method: Manual, Scripted, Automated		

## 17.7 "Technical Requirements Specifications – SDN Controller"

Product Name: SDN Controller

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SDNCTR.REQ.001</b>	The overall System network design & operations must be based on Open Standards' implementation for Networking, with the minimum of eBGP underlay, eBGP/MP-BGP/EVPN overlay and VXLAN H/W VTEP where required.		
<b>SDNCTR.REQ.002</b>	The overall System must not be based on Proprietary & Closed (ie. Vendor-specific) Technology implementations for Networking.		
<b>SDNCTR.REQ.003</b>	The overall System must provide the capability to build both simple and complex analytics, against the context of the reference design and network topology.		
<b>SDNCTR.REQ.004</b>	Interaction between the Central Server and the switching fabric must be held on the management plane only.		
<b>SDNCTR.REQ.005</b>	The system must provide open APIs to enable an automated system wide build of the DC		
<b>SDNCTR.REQ.006</b>	The interaction must not be held on the Control Plane or Data Plane of the Fabric.		
<b>SDNCTR.REQ.007</b>	The deployed network must be able to operate and run without interruption, in case the Central Server is not present for any reason. There must not be any relationship between the Central Server and the operational running of the Fabric.		
<b>SDNCTR.REQ.008</b>	The System must enable integration between physical and virtualised infrastructures.		
<b>SDNCTR.REQ.009</b>	The System must provide Spine & Leaf Fabric design capability.		
<b>SDNCTR.REQ.010</b>	The System must provide a web-based UI to design, build and deploy Spine & Leaf Fabric.		
<b>SDNCTR.REQ.011</b>	The System must provide network abstraction simplifying the design and implementation of the Fabric.		
<b>SDNCTR.REQ.012</b>	The System must generate configuration files which can be easily viewed via the web front-end, for both the full running configuration and any pre-staged configuration.		
<b>SDNCTR.REQ.013</b>	For a fixed Fabric Design, the configuration files must reflect the precise running-config to be deployed on target OS Fabric switches.		
<b>SDNCTR.REQ.014</b>	The System must provide the capability to create a graphical representation of all Network and Compute Elements in the design.		
<b>SDNCTR.REQ.015</b>	The System must provide an open API that enables the networking Fabric to be built to the very same level as the UI.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SDNCTR.REQ.016</b>	The System must not be constructed of separate sub-systems stitched together by one overarching UI, which independently serve design, build, deploy and operations' capabilities.		
<b>SDNCTR.REQ.017</b>	The System must provide the capability to build a complete network representation in which logical layers can be applied, with a minimum of all addressing information (IP / ASNs / VNIs), VRFs and the overlay.		
<b>SDNCTR.REQ.018</b>	The System must provide continuous, closed-loop validation of the desired Fabric state (as declared in design, build or deploy phase) against the actual operational state of the physical network, and alert when the two states do not match.		
<b>SDNCTR.REQ.019</b>	The System must be able to interface through open APIs with external ticketing systems or centralised alerting NMS systems as used in a NOC.		
<b>SDNCTR.REQ.020</b>	The System must provide the capability to build complex analytics out of telemetry collected from the Fabric switches - analytics with context.		
<b>SDNCTR.REQ.021</b>	The System must integrate with 3rd-party systems through open APIs for additional reporting, with the minimum of time series databases and graphing applications.		
<b>SDNCTR.REQ.022</b>	The System must support multiple switching hardware.		
<b>SDNCTR.REQ.023</b>	The System must provide an easily exportable Cabling Map or topology Map for the completed Fabric.		
<b>SDNCTR.REQ.024</b>	The System must deliver a single source-of-truth and an accurate representation of all deployed systems within a dashboard for network, security, virtualization.		
<b>SDNCTR.REQ.025</b>	The System must support multiple switching hardware vendors.		
<b>SDNCTR.REQ.026</b>	The Should should provide active-active EVPN ESI multihoming to the connected end-points has context menu		

## 17.8 "Technical Requirements Specifications - Hardware-Spine Switch"

Product Name: Spine Switch

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SPINES.REQ.001</b>	Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing		
<b>SPINES.REQ.002</b>	Solution Requirement	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy		
<b>SPINES.REQ.003</b>	Hardware and Interface Requirement	Switch should have 32 x 40/100G QSFP28 Ports fully loaded with required optics transceiver as per solution design		
<b>SPINES.REQ.004</b>	Hardware and Interface Requirement	Switch should have 16GB DRAM and 16GB internal Flash/Storage		
<b>SPINES.REQ.005</b>	Hardware and Interface Requirement	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc.		
<b>SPINES.REQ.006</b>	Hardware and Interface Requirement	The switch should support hardware based load sharing at wire speed using LACP and multi chassis ether channel/LAG		
<b>SPINES.REQ.007</b>	Hardware and Interface Requirement	Switch should support minimum 6.4 Tbps of switching capacity		
<b>SPINES.REQ.008</b>	Layer2 Features	Switch should support minimum 280,000 no. of MAC addresses		
<b>SPINES.REQ.009</b>	Layer2 Features	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S)		
<b>SPINES.REQ.010</b>	Layer2 Features	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 32 number of Link Aggregation Group.		
<b>SPINES.REQ.011</b>	Layer2 Features	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SPINES.REQ.012</b>	Layer2 Features	The Switch should Multihoming ESI-LAG or equivalent		
<b>SPINES.REQ.013</b>	Layer3 Features	The switch should support 1.8 Million IPv4 routes (RIB) and 400k IPv6 routes (RIB) entries in the routing table including 100,000 multicast routes		
<b>SPINES.REQ.014</b>	Layer3 Features	Switch should support static and dynamic routing like Static, OSPF and BGP		
<b>SPINES.REQ.015</b>	Layer3 Features	Should support BGP, MBGP, IS-IS for IPv4 and IPv6		
<b>SPINES.REQ.016</b>	Layer3 Features	Switch should support multicast traffic reachability using PIM-SM and SSM		
<b>SPINES.REQ.017</b>	Layer3 Features	Switch should support RSVP/LDP/6PE and L3 VPN		
<b>SPINES.REQ.018</b>	Virtualization Features	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN/ NVGRE		
<b>SPINES.REQ.019</b>	Virtualization Features	Switch should support VXLAN & EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center		
<b>SPINES.REQ.020</b>	Availability	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/ VRRP		
<b>SPINES.REQ.021</b>	Availability	Switch should support for BFD For Fast Failure Detection		
<b>SPINES.REQ.022</b>	Quality of Service	Switch system should support 802.1P classification and marking of packet CoS, DSCP etc.		
<b>SPINES.REQ.023</b>	Quality of Service	Switch should support for different type of QoS features for real time traffic differential treatment using WRED/SP Queuing		
<b>SPINES.REQ.024</b>	Quality of Service	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SPINES.REQ.025</b>	Security	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy		
<b>SPINES.REQ.026</b>	Security	Switch should support for external database for AAA using TACACS+ / Radius		
<b>SPINES.REQ.027</b>	Security	Switch should support for Role Based access control (RBAC)		
<b>SPINES.REQ.028</b>	Manageability	Switch should support for embedded RMON for central NMS management and monitoring		
<b>SPINES.REQ.029</b>	Manageability	Switch should provide remote login for administration Telnet, SSHv2		
<b>SPINES.REQ.030</b>	Manageability	Switch should support for basic administrative tools like Ping and traceroute		
<b>SPINES.REQ.031</b>	Manageability	Switch should support central time server synchronization using Network Time Protocol NTP		
<b>SPINES.REQ.032</b>	Certification	The Switch should be IPv6 Certified (IPv6 Logo ready or USGv6)		
<b>SPINES.REQ.033</b>	Certification	The Switch should be EAL 3/NDPP/ NDcPP certified under Common Criteria.		
<b>SPINES.REQ.034</b>	General	System should be sized to meet requirement of CHiPS data centre		
<b>SPINES.REQ.035</b>	Environment	Operating temperature: 0 to 40 degrees		
<b>SPINES.REQ.036</b>	Environment	Humidity: 10% to 85% non-condensing		

## 17.9 "Technical Requirements Specifications - Hardware-Leaf Switch OFC"

Product Name: Leaf Switch OFC

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>LSWO.REQ.001</b>	Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>LSWO.REQ.002</b>	Solution Requirement	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy		
<b>LSWO.REQ.003</b>	Hardware and Interface Requirement	Switch should have the 48 x 1/10G/25G SFP fibre ports and should have 6 x 40G/100G QSFP28 ports (Fully populated). MSI to provision all the transceivers required to meet the solution design		
<b>LSWO.REQ.004</b>	Hardware and Interface Requirement	Switch should have 16GB DRAM and 16GB internal Flash/Storage		
<b>LSWO.REQ.005</b>	Hardware and Interface Requirement	Switch should support Configuration roll-back		
<b>LSWO.REQ.006</b>	Hardware and Interface Requirement	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc.		
<b>LSWO.REQ.007</b>	Hardware and Interface Requirement	The switch should support hardware-based load sharing at wire speed using LACP and multi chassis ether channel/LAG		
<b>LSWO.REQ.008</b>	Hardware and Interface Requirement	Switch should support minimum 3.6 Tbps of switching capacity and 2Bpps Forwarding		
<b>LSWO.REQ.009</b>	Layer2 Features	Switch should support minimum 200,000 no. of MAC addresses		
<b>LSWO.REQ.010</b>	Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)		
<b>LSWO.REQ.011</b>	Layer2 Features	Switch should support 8Nos. of link or more per Port channel (using LACP) and support 48 number of Link Aggregation Group.		
<b>LSWO.REQ.012</b>	Layer2 Features	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
<b>LSWO.REQ.013</b>	Layer2 Features	The Switch should Multihoming ESI-LAG or equivalent		
<b>LSWO.REQ.014</b>	Layer3 Features	The switch should support 1.8 million IPv4 routes (RIB) and 400k IPv6 routes (RIB) entries in the routing table including 100,000 multicast routes		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
LSWO.REQ.015	Layer3 Features	Switch should support static and dynamic routing like Static, OSPF and BGP		
LSWO.REQ.016	Layer3 Features	Should support BGP, MBGP, IS-IS for IPv4 and IPv6		
LSWO.REQ.017	Layer3 Features	Switch should support multicast traffic reachability using PIM-SM and SSM		
LSWO.REQ.018	Layer3 Features	Switch should support RSVP/LDP/6PE and L3 VPN		
LSWO.REQ.019	Virtualization Features	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN/ NVGRE		
LSWO.REQ.020	Virtualization Features	Switch should support VXLAN & EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center		
LSWO.REQ.021	Availability	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/ VRRP		
LSWO.REQ.022	Availability	Switch should support for BFD For Fast Failure Detection		
LSWO.REQ.023	Quality of Service	Switch system should support 802.1P classification and marking of packet CoS, DSCP etc.		
LSWO.REQ.024	Quality of Service	Switch should support for different type of QoS features for real time traffic differential treatment using WRED/SP Queuing		
LSWO.REQ.025	Quality of Service	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x		
LSWO.REQ.026	Security	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy		
LSWO.REQ.027	Security	Switch should support for external database for AAA using TACACS+ / Radius		
LSWO.REQ.028	Security	Switch should support for Role Based access control (RBAC)		
LSWO.REQ.029	Manageability	Switch should support for embedded RMON for central NMS management and monitoring		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>LSWO.REQ.030</b>	Manageability	Switch should provide remote login for administration Telnet, SSHv2		
<b>LSWO.REQ.031</b>	Manageability	Switch should support for basic administrative tools like Ping and traceroute		
<b>LSWO.REQ.032</b>	Manageability	Switch should support central time server synchronization using Network Time Protocol NTP		
<b>LSWO.REQ.033</b>	Certification	The Switch should be IPv6 Certified (IPv6 Logo ready or USGv6)		
<b>LSWO.REQ.034</b>	Certification	The Switch should be EAL 3/NDPP/ NDcPP certified under Common Criteria.		
<b>LSWO.REQ.035</b>	Environment	Operating temperature: 0 to 40 degrees		
<b>LSWO.REQ.036</b>	Environment	Humidity: 10% to 85% non-condensing		

#### 17.10 "Technical Requirements Specifications - Hardware-Router"

Product Name: Core Router – Internet

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>INTRTR.REQ.001</b>	Architecture	Should be chassis based/ Modular router.		
<b>INTRTR.REQ.002</b>	Architecture	The Router should have 32GBRAM and 64GB internal flash/ storage from Day 1		
<b>INTRTR.REQ.003</b>	Architecture	The Router should have redundant Control Plane/ Redundant Routing Engine		
<b>INTRTR.REQ.004</b>	Architecture	Should have N+1 power supply redundancy. There should not be any impact on The Router performance in case one of the power supplies fails		
<b>INTRTR.REQ.005</b>	Architecture	All power supplies should be hot swappable for high availability		
<b>INTRTR.REQ.006</b>	Architecture	The Router shall support active - active high availability using vPC or Virtual Chassis or Multi-chassis or EVPN LAG		
<b>INTRTR.REQ.007</b>	Architecture	The Router should have a non-blocking throughput of at least 3Tbps ( Half Duplex) or 1.5Tbps (Full Duplex)		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>INTRTR.REQ.008</b>	Architecture	The Router should provide min 6 x 100G and 16 x 10G (NATive or using Breakout) Interfaces loaded with required optics from Day 1.		
<b>INTRTR.REQ.009</b>	Architecture	The Router should support following minimum MAC Address, Routes and other scale		
<b>INTRTR.REQ.010</b>	Architecture	MAC Address - 1Million, IPv4 FIB- 8 million, IPv6 FIB - 8 million		
<b>INTRTR.REQ.011</b>	Architecture	The Router should support minimum VRF - 8000 and 1 Million - MPLS Labels		
<b>INTRTR.REQ.012</b>	Architecture	The Router should support minimum Multicast 120k		
<b>INTRTR.REQ.013</b>	Architecture	The operating system shall be modular and run all critical functions (Eg; Routing protocols, Forwarding plane, management tasks) in separate memory protected modules.		
<b>INTRTR.REQ.014</b>	Architecture	Shall support link aggregation using LACP as per IEEE 802.3ad min 32 bundles with min 8 member ports per bundle		
<b>INTRTR.REQ.015</b>	Protocol Support	IPv4 Routing, IPv6 Routing Border Gateway Protocol, Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF], IGMP, PIM SSM, OSPFv3 for IPv6,		
<b>INTRTR.REQ.016</b>	Protocol Support	MPLS TE (Fast re-route), DiffServ-Aware TE, Inter-AS VPN, Resource Reservation Protocol (RSVP), VPLS, BGP-LU, LDP, EVPN-VxLAN, L2VPN, L3VPN, Segment Routing and DCI		
<b>INTRTR.REQ.017</b>	QOS Features	IP Precedence, 802.1p, MPLS EXP, DSCP, Priority queuing, Traffic Conditioning: Committed Access Rate/Rate limiting		
<b>INTRTR.REQ.018</b>	QOS Features	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter		
<b>INTRTR.REQ.019</b>	QOS Features	Should support at least 256k Hardware queues per system.		
<b>INTRTR.REQ.020</b>	Security	Support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc.), Port Range		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
INTRTR.REQ.021	Security	Support per-user Authentication, Authorization and Accounting through RADIUS or TACACS, enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration		
INTRTR.REQ.022	Security	Authentication, Authorization and Accounting through RADIUS or TACACS		
INTRTR.REQ.023	Security	The Router shall support MD-5 route authentication for RIP, OSPF and BGP		
INTRTR.REQ.024	Security	The Router must support multiple multi-level privilege levels for remote access (e.g. console or telnet)		
INTRTR.REQ.025	Security	Should support URPF, DHCP snooping, control plane policing, SNMPv3 authentication		
INTRTR.REQ.026	Security	Multiple privilege level authentications for console and telnet access through Local database or through an external AAA Server		
INTRTR.REQ.027	Debug, Alarms & Diagnostics	The Router shall support for monitoring of Traffic flows		
INTRTR.REQ.028	Debug, Alarms & Diagnostics	Display of input and output error statistics on all interfaces		
INTRTR.REQ.029	Debug, Alarms & Diagnostics	Display of Input and Output data rate statistics on all interfaces		
INTRTR.REQ.030	Debug, Alarms & Diagnostics	The Router must support Telnet, Trace-route, Ping and extended Ping		
INTRTR.REQ.031	Debug, Alarms & Diagnostics	The Router shall have Debugging features to display and analyse various types of packets		
INTRTR.REQ.032	Management	Shall support latest version of Secure Shell for secure connectivity		
INTRTR.REQ.033	Management	The Router should support Netconf interface for device configuration		
INTRTR.REQ.034	Management	The solution should support the network configuration protocol (NETCONF) and YANG models		
INTRTR.REQ.035	Management	Embedded RMON support for four groups – history, statistics, alarms and events.		
INTRTR.REQ.036	Management	Should have to support Out of band management through		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		Ethernet or should have Console port		
<b>INTRTR.REQ.037</b>	Management	Event and system history logging functions shall be available		
<b>INTRTR.REQ.038</b>	Environment	Operating temperature: 0 to 40 degrees		
<b>INTRTR.REQ.039</b>	Environment	Humidity: 10% to 85% non-condensing		

## 17.11 "Technical Requirements Specifications - Hardware-Router"

Product Name: Intranet Router

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CORRTR.REQ.001</b>	Architecture	Should be chassis based/ Modular router.		
<b>CORRTR.REQ.002</b>	Architecture	The Router should have 32GBRAM and 64GB internal flash/ storage from Day 1		
<b>CORRTR.REQ.003</b>	Architecture	The Router should have redundant Control Plane/ Redundant Routing Engine		
<b>CORRTR.REQ.004</b>	Architecture	Should have N+1 power supply redundancy. There should not be any impact on The Router performance in case one of the power supplies fails		
<b>CORRTR.REQ.005</b>	Architecture	All power supplies should be hot swappable for high availability		
<b>CORRTR.REQ.006</b>	Architecture	The Router shall support active - active high availability using vPC or Virtual Chassis or Multi-chassis or EVPN LAG		
<b>CORRTR.REQ.007</b>	Architecture	The Router should have a non-blocking throughput of at least 3Tbps (Half Duplex) or 1.5Tbps (Full Duplex)		
<b>CORRTR.REQ.008</b>	Architecture	The Router should provide min 6 x 100G and 16 x 10G (native or using Breakout) Interfaces loaded with required optics from Day 1.		
<b>CORRTR.REQ.009</b>	Architecture	The Router should support following minimum MAC Address, Routes and other scale		
<b>CORRTR.REQ.010</b>	Architecture	MAC Address - 1Million, IPv4 FIB- 8 million, IPv6 FIB - 8 Million		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CORRTR.REQ.011</b>	Architecture	The Router should support minimum VRF - 8000 and 1 million - MPLS Labels		
<b>CORRTR.REQ.012</b>	Architecture	The Router should support minimum Multicast 120k		
<b>CORRTR.REQ.013</b>	Architecture	The operating system shall be modular and run all critical functions (Eg; Routing protocols, Forwarding plane, management tasks) in separate memory protected modules.		
<b>CORRTR.REQ.014</b>	Architecture	Shall support link aggregation using LACP as per IEEE 802.3ad min 32 bundles with min 8 member ports per bundle		
<b>CORRTR.REQ.015</b>	Protocol Support	IPv4 Routing, IPv6 Routing Border Gateway Protocol, Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF]), IGMP, PIM SSM, OSPFv3 for IPv6,		
<b>CORRTR.REQ.016</b>	Protocol Support	MPLS TE (Fast re-route), DiffServ-Aware TE, Inter-AS VPN, Resource Reservation Protocol (RSVP), VPLS, BGP-LU, LDP, EVPN-VxLAN, L2VPN, L3VPN, Segment Routing and DCI		
<b>CORRTR.REQ.017</b>	QOS Features	IP Precedence, 802.1p, MPLS EXP, DSCP, Priority queuing, Traffic Conditioning: Committed Access Rate/Rate limiting		
<b>CORRTR.REQ.018</b>	QOS Features	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter		
<b>CORRTR.REQ.019</b>	QOS Features	Should support at least 256k Hardware queues per system.		
<b>CORRTR.REQ.020</b>	Security	Support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc.), Port Range		
<b>CORRTR.REQ.021</b>	Security	Support per-user Authentication, Authorization and Accounting through RADIUS or TACACS, enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CORRTR.REQ.022</b>	Security	Authentication, Authorization and Accounting through RADIUS or TACACS		
<b>CORRTR.REQ.023</b>	Security	The Router shall support MD-5 route authentication for RIP, OSPF and BGP		
<b>CORRTR.REQ.024</b>	Security	The Router must support multiple multi-level privilege levels for remote access (e.g. console or telnet)		
<b>CORRTR.REQ.025</b>	Security	Should support URPF, DHCP snooping, control plane policing, SNMPv3 authentication		
<b>CORRTR.REQ.026</b>	Security	Multiple privilege level authentications for console and telnet access through Local database or through an external AAA Server		
<b>CORRTR.REQ.027</b>	Debug, Alarms & Diagnostics	The Router shall support for monitoring of Traffic flows		
<b>CORRTR.REQ.028</b>	Debug, Alarms & Diagnostics	Display of input and output error statistics on all interfaces		
<b>CORRTR.REQ.029</b>	Debug, Alarms & Diagnostics	Display of Input and Output data rate statistics on all interfaces		
<b>CORRTR.REQ.030</b>	Debug, Alarms & Diagnostics	The Router must support Telnet, Trace-route, Ping and extended Ping		
<b>CORRTR.REQ.031</b>	Debug, Alarms & Diagnostics	The Router shall have Debugging features to display and analyse various types of packets		
<b>CORRTR.REQ.032</b>	Management	Shall support latest version of Secure Shell for secure connectivity		
<b>CORRTR.REQ.033</b>	Management	The Router should support Netconf interface for device configuration		
<b>CORRTR.REQ.034</b>	Management	The solution should support the network configuration protocol (NETCONF) and YANG models		
<b>CORRTR.REQ.035</b>	Management	Embedded RMON support for four groups – history, statistics, alarms and events.		
<b>CORRTR.REQ.036</b>	Management	Should have to support Out of band management through Ethernet or should have Console port		
<b>CORRTR.REQ.037</b>	Management	Event and system history logging functions shall be available		
<b>CORRTR.REQ.038</b>	Environment	Operating temperature: 0 to 40 degrees		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CORRTR.REQ.039</b>	Environment	Humidity: 10% to 85% non-condensing		

## 17.12 "Technical Requirements Specifications - Hardware-Out of Band Management Switch"

Product Name: Out of Band Management Switch

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>MGMTSW.REQ.001</b>	Minimum 48 x 10/100/1000 Base-T and 4 x 10G ports (with required transceiver modules)		
<b>MGMTSW.REQ.002</b>	Minimum 1 U Rack mountable		
<b>MGMTSW.REQ.003</b>	The Switch should have 4GB DRAM and 8GB internal Flash/ SSD		
<b>MGMTSW.REQ.004</b>	176Gbps or higher Backplane capacity and minimum 130Mpps of forwarding rate (excluding the stacking bandwidth and forwarding)		
<b>MGMTSW.REQ.005</b>	Should support non-blocking hardware architecture		
<b>MGMTSW.REQ.006</b>	Support for at least 1000 VLANs & 64k MAC address		
<b>MGMTSW.REQ.007</b>	It should support IGMP snooping v1/v2 & v3		
<b>MGMTSW.REQ.008</b>	It should have static IP routing from Day 1 and should be upgradable to support OSPF, PIM, EVPN-VxLAN and BGP		
<b>MGMTSW.REQ.009</b>	The switch should support 32k IPv4/ 16k IPv6 and 16k Multicast Routes		
<b>MGMTSW.REQ.010</b>	Switch should support 8 hardware queues per port		
<b>MGMTSW.REQ.011</b>	Dynamic Host Configuration Protocol (DHCP) snooping and MLD snooping		
<b>MGMTSW.REQ.012</b>	Switch should support LLDP capabilities		
<b>MGMTSW.REQ.013</b>	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection		
<b>MGMTSW.REQ.014</b>	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).		
<b>MGMTSW.REQ.015</b>	Switch needs to have console port for administration & management		
<b>MGMTSW.REQ.016</b>	Management using CLI/GUI using Web interface should be supported		
<b>MGMTSW.REQ.017</b>	FTP/TFTP for upgrading the operating System		
<b>MGMTSW.REQ.018</b>	Should support Energy Efficient Ethernet		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>MGMTSW.REQ.019</b>	IEEE 802.1x support, IEEE 802.1D Spanning-Tree Protocol, IEEE 802.1p class-of-service (CoS) prioritization, IEEE 802.1Q VLAN, IEEE 802.3 10BASE-T specification, IEEE 802.3u 100BASE-TX		
<b>MGMTSW.REQ.020</b>	Switch should have internal redundant power supply and Hot swappable fans		
<b>MGMTSW.REQ.021</b>	Switch should be UL-UL60950-1,FCC Part 15, VCCI Class A, EN 55022/550032, EN 55024, EN 300386, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous Substances (ROHS) certified		
<b>MGMTSW.REQ.022</b>	The Switch should be EAL 3/NDPP/ NDcPP certified under Common Criteria.		
<b>MGMTSW.REQ.024</b>	Operating temperature: 0 to 40 degrees		
<b>MGMTSW.REQ.025</b>	Humidity: 10% to 85% non-condensing		

### 17.13 Technical Requirements Specifications - Hardware-L2 Managed Access Switch for NOC

Product Name: L2 Managed Access Switch for NOC

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>L2SW.REQ.001</b>	General Features	Switch should be minimum 1U and rack mountable. Switch should have 48 x 1G Copper Ports and 4 X 10 G loaded with required optics SFP/SFP+.		
<b>L2SW.REQ.002</b>	General Features	Support for external redundant power supply, if required.		
<b>L2SW.REQ.003</b>	General Features	Switch support online hot insertion and removal of different parts like modules/power supplies/fan tray etc. should not require switch reboot and disrupt the functionality of the system		
<b>L2SW.REQ.004</b>	General Features	Switch should be supplied with the all-necessary hardware accessories like Power cord, Rack-mount bracket, Installation Guide, necessary software image file, licenses etc.		
<b>L2SW.REQ.005</b>	Performance	Switch shall have minimum 88 Gbps of switching fabric.		
<b>L2SW.REQ.006</b>	Performance	Switch shall have minimum 16K MAC Addresses and minimum 256 VLAN IDs.		
<b>L2SW.REQ.007</b>	Performance	Switch should support Spanning Tree Protocol		
<b>L2SW.REQ.008</b>	Performance	The Switch should support minimum Access Control lists		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>L2SW.REQ.009</b>	Functionality	Switch should support management features like SSHv2, SNMPv1/SNMPv2c/SNMPv3, NTP, RADIUS or TACACS+		
<b>L2SW.REQ.010</b>	Functionality	Switch should support for external database to AAA using Tacacs or equivalent.		
<b>L2SW.REQ.011</b>	Functionality	Switch should support IPv4 AND IPv6 from day 1		
<b>L2SW.REQ.012</b>	Functionality	Switch should have management interface for Out of Band Management		
<b>L2SW.REQ.013</b>	Functionality	Switch should support Jumbo Frames up to 9K Bytes.		
<b>L2SW.REQ.014</b>	Environment	Operating temperature: 0 to 40 degrees		
<b>L2SW.REQ.015</b>	Environment	Humidity: 10% to 85% non-condensing		

#### 17.14 "Technical Requirements Specifications - Link Load Balancer"

Product Name: Link Load Balancer

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>LINKLDBR.REQ.001</b>	The proposed appliance should provide functionalities of Link Load Balancer		
<b>LINKLDBR.REQ.002</b>	The Appliance should have minimum 4x1GbE copper ports, 4x10GbE SFP+ ports fully populated, and dedicated out of band management port.		
<b>LINKLDBR.REQ.003</b>	Should be intelligent to handle multiple link of different capacity and able to utilize the same accordingly		
<b>LINKLDBR.REQ.004</b>	System should support dynamically redirecting traffic via the best performing link.		
<b>LINKLDBR.REQ.005</b>	System should support setting a priority for each type of traffic.		
<b>LINKLDBR.REQ.006</b>	Support for multiple internet links in Active-Active load balancing and active standby failover mode.		
<b>LINKLDBR.REQ.007</b>	Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, target proximity and dynamic detect.		
<b>LINKLDBR.REQ.008</b>	Should support inbound load balancing algorithms like round robin, Weighted round robin, target proximity & dynamic detect.		
<b>LINKLDBR.REQ.009</b>	Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>LINKLDBR.REQ.010</b>	In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.		
<b>LINKLDBR.REQ.011</b>	Shall provide individual link health check based on physical port, ICMP Protocols, user defined ports and destination path health checks.		
<b>LINKLDBR.REQ.012</b>	Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.		
<b>LINKLDBR.REQ.013</b>	Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation.		
<b>LINKLDBR.REQ.014</b>	System should support setting a priority for each type of traffic.		
<b>LINKLDBR.REQ.015</b>	The solution should support Domain name support for outbound link selection for FQDN based load balancing.		
<b>LINKLDBR.REQ.016</b>	the solution should support Stateful session failover with N+1 clustering support when deployed in HA mode.		
<b>LINKLDBR.REQ.017</b>	The solution shall provide individual link health check based on physical port, ICMP Protocols, user defined I4 ports and destination path health checks.		
<b>LINKLDBR.REQ.018</b>	The appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback. The system should support led warning and system log alert for failure of any of the power and CPU issues		
<b>LINKLDBR.REQ.019</b>	The solution should be dual stack support IPv4 & Ipv6.		
<b>LINKLDBR.REQ.020</b>	Should Support integration with SIEM and other Monitoring and Reporting solution		
<b>LINKLDBR.REQ.021</b>	Operating temperature: 0 to 40 degrees		
<b>LINKLDBR.REQ.022</b>	Humidity: 10% to 85% non-condensing		

## 17.15 "Technical Requirements Specifications - Server Load Balancer"

Product Name: Server Load Balancer

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SRLDBR.REQ.001</b>	Device to have capabilities to support ADC as independent Network Function and not an integrated solution to ensure required performance.		
<b>SRLDBR.REQ.002</b>	It shall support built-in failover decision/health-check conditions. It shall also support failover and High Availability (HA) requirements. It shall have redundant power supplies. Shall support script-based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS		
<b>SRLDBR.REQ.003</b>	Should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode. Should support both device level and VA level High availability for using standard VRRP protocol.		
<b>SRLDBR.REQ.004</b>	24 x 7 OEM support with 5 years warranty		
<b>SRLDBR.REQ.005</b>	The appliance should be modular based high performance purpose built next generation multi-tenant hardware with Network function virtualization . The Appliance should support multiple network functions virtualization with dedicated hardware resources for each virtual instance.		
<b>SRLDBR.REQ.006</b>	The Appliance should have dedicated 1x1Gb port for management and 8x10/25 GbE SFP+ ports.		
<b>SRLDBR.REQ.007</b>	The appliance should have multicore CPU, minimum 64 GB RAM,minimum 2TB SSD and dual power supply.		
<b>SRLDBR.REQ.008</b>	The device should support minimum 8 virtual instances from Day1.		
<b>SRLDBR.REQ.009</b>	The solution should support minimum 5 million L7 RPS and 2.5 million L4 Connections per second.		
<b>SRLDBR.REQ.010</b>	The solution should support negative and positive security model The positive security recognizes the characteristics of normal application traffic by automatic traffic learning in order to form the positive security model (whitelist model), which allows only traffic matching these whitelists to pass.		
<b>SRLDBR.REQ.011</b>	The solution should respectively support working modes and protocol detection based on IPv4 and IPv6 environments, and be able to		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	support IPv4 and IPv6 dual-stack environments.		
<b>SRLDBR.REQ.012</b>	The solution should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.		
<b>SRLDBR.REQ.013</b>	The solution should support for policy nesting at layer7 and layer4. it should able to combine layer4 and layer7 policies to address the complex application integration.		
<b>SRLDBR.REQ.014</b>	The solution using e-policy then should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash ip and snmp		
<b>SRLDBR.REQ.015</b>	The solution should provide Dua Stack IPv4 and IPv6 support .		
<b>SRLDBR.REQ.016</b>	The solution should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.		
<b>SRLDBR.REQ.017</b>	It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.		
<b>SRLDBR.REQ.018</b>	The solution should provide comprehensive and reliable support for high availability and N+1 clustering through VRRP on Per VIP based Active-active & active standby unit redundancy mode.		
<b>SRLDBR.REQ.019</b>	Operating temperature: 0 to 40 degrees		
<b>SRLDBR.REQ.020</b>	Humidity: 10% to 85% non-condensing		

## 17.16 "Technical Requirements Specifications - Hardware-Core SAN Switch"

Product Name: Core San Switch

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CSANSW.REQ.001</b>	Proposed switch should be best in terms of capacity performance, features and latest offering from the proposed OEM.		
<b>CSANSW.REQ.002</b>	SAN Switch should supports standard SAN protocols, and should be provided with the licences from Day-1		
<b>CSANSW.REQ.003</b>	SAN Switch shall have support for web-based management or CLI Based Management		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CSANSW.REQ.004</b>	The fibre switch should be quoted with minimum 24 FC ports (fully populated) of 16/32/64 Gbps speed with all supported Licenses from day one. It shall be along with requisite SFP module. The switch should be scalable up to 48 ports.		
<b>CSANSW.REQ.005</b>	The switch should have support for 16/32/64Gbps		
<b>CSANSW.REQ.006</b>	The switch should have auto sensing, Zoning, Integrated Ethernet and Serial Port for communication.		
<b>CSANSW.REQ.007</b>	Switch should be rack mountable 1 or 2RU size and should be supplied with mounting kit.		
<b>CSANSW.REQ.008</b>	The switch should be equipped with redundant hot swap power supply and Fan and allow hot swap ability without resetting the switch, or affecting the coperations of the switch		
<b>CSANSW.REQ.009</b>	The switch should be backward compatible		
<b>CSANSW.REQ.010</b>	The switch should be capable for non-disruptive firmware /microcode upgrade and hot code activation.		
<b>CSANSW.REQ.011</b>	The switch should be capable of End-to-end performance monitoring		
<b>CSANSW.REQ.012</b>	The switch should be capable to interface with host- based adapters (HBA) of multiple OEM, supporting multiple Operating Systems		
<b>CSANSW.REQ.013</b>	SAN Switch should have management access through 10/100Mbps Ethernet (RJ-45), serial port or equivalent		
<b>CSANSW.REQ.014</b>	The switch should have following Zoning and security features -		
<b>CSANSW.REQ.015</b>	Support for hardware and software zoning Policy based security and centralized fabric management. Support for secure access. Support for RADIUS, SSH, SNMP Support for Switch linking / trunking.		
<b>CSANSW.REQ.016</b>	Switch shall support alert based on threshold value for temperature, fan status, power supply status and port status.		
<b>CSANSW.REQ.017</b>	The switch shall support different port type such as FL port, F port, M port(mirror port), and E port ; self- discovery based on switch type (U port); optional port type control in access gateway mode F port and NPIV- Enabled N port or provide equivalent functionality with any relevant technology to achieve solution requirement.		
<b>CSANSW.REQ.018</b>	All relevant licenses for all the above features and scale should be quoted along with switch		
<b>CSANSW.REQ.019</b>	Operating temperature: 0 to 40 degrees		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>CSANSW.REQ.020</b>	Humidity: 10% to 85% non-condensing		

#### 17.17 "Technical Requirements Specifications - Next generation Firewall"

Product Name: Next Generation Firewall - Internet

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>NEXGENFWALL.REQ.001</b>	The appliance based security platform shall be capable of providing firewall, IPS and VPN (IPSec) functionality simultaneously.		
<b>NEXGENFWALL.REQ.002</b>	FCC Class A, CE Class A, VCCI Class A, CB, and Common Criteria Certified.		
<b>NEXGENFWALL.REQ.003</b>	The offered firewall must be provided with redundant Fan Trays and redundant power supplies		
<b>NEXGENFWALL.REQ.004</b>	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane		
<b>NEXGENFWALL.REQ.005</b>	The proposed firewall must have min 32 physical cores with x86 processor and minimum 128GB RAM from day 1		
<b>NEXGENFWALL.REQ.006</b>	The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support. Also, the device should have capability to provide detailed information about dependent applications to securely enable an application		
<b>NEXGENFWALL.REQ.007</b>	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration		
<b>NEXGENFWALL.REQ.008</b>	Should have protocol decoder-based analysis which can state fully decodes the protocol and then intelligently applies signatures to detect network and application exploits		
<b>NEXGENFWALL.REQ.009</b>	The Firewall should have Application visibility and control/ AVC from Day 1.		
<b>NEXGENFWALL.REQ.010</b>	The Firewall should have Advanced Threat Protection like malware and zero-day threats from Day 1		
<b>NEXGENFWALL.REQ.011</b>	HA configuration that uses dedicated HA/ Control interfaces apart from the mentioned traffic interfaces		
<b>NEXGENFWALL.REQ.012</b>	Should provide active/active and active/standby failover		



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
NEXGENFWALL.REQ.013	The Firewall should support MACsec and should have TPM2.0		
NEXGENFWALL.REQ.014	Should support upto 750,000 connections per second and at least 10 million concurrent sessions per second		
NEXGENFWALL.REQ.015	Should provide 70 Gbps Firewall Throughput		
NEXGENFWALL.REQ.016	Should provide 40 Gbps IPSec throughput (large packet)		
NEXGENFWALL.REQ.017	Should provide 20 Gbps NextGen firewall throughput including firewall, Application Security/ AVC, IPS and URL filtering		
NEXGENFWALL.REQ.018	The NGFW should have two 400GB solid-state drives for System storage in RAID 1 or minimum 800 GB SSD based storage		
NEXGENFWALL.REQ.019	<b>Support:</b> - IKEv1 and v2, IPSec VPN standards, 56-bit DES, 168-bit 3DES, 256-bit AES.		
NEXGENFWALL.REQ.020	<b>Authentication, Authorization and Accounting (AAA) support:</b> RADIUS/TACACS		
NEXGENFWALL.REQ.021	<b>Support for:</b> Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256		
NEXGENFWALL.REQ.022	<b>Provides:</b>		
NEXGENFWALL.REQ.023	NAT44, NAT64, NAT46 and NAT66		
NEXGENFWALL.REQ.024	Stateful and stateless and Zone-based firewall		
NEXGENFWALL.REQ.025	Traffic anomaly protection		
NEXGENFWALL.REQ.026	<b>Management</b>		
NEXGENFWALL.REQ.027	Web based management to support for remote monitoring		
NEXGENFWALL.REQ.028	Accessible through variety of methods including Telnet, Console Port, SSH		
NEXGENFWALL.REQ.029	Dedicated Out-of-Management interface		
NEXGENFWALL.REQ.030	Support SNMPv1/v2, v3 & Support for syslog		
NEXGENFWALL.REQ.031	<b>Software features</b>		
NEXGENFWALL.REQ.032	support for IPv4,IPv6, OSPF, BGP, VLAN, DHCP, Support for IPv6 RIPng.		
NEXGENFWALL.REQ.033	<b>Power Supply</b>		
NEXGENFWALL.REQ.034	Internal Redundant Power supply and Redundant fans		
NEXGENFWALL.REQ.035	<b>Minimum Interfaces Required</b>		
NEXGENFWALL.REQ.036	8 x 1/10G SFP+, 4 x 10G/25G and 4 x 40/100G Ports (loaded with required optics)		
NEXGENFWALL.REQ.037	Operating temperature: 0 to 40 degrees		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>NEXGENFWALL.REQ.038</b>	Humidity: 10% to 85% non-condensing		
<b>NEXGENFWALL.REQ.039</b>	MSI shall propose Internet and Intranet Firewall from two different OEMs.		

## 17.18 "Technical Requirements Specifications - Web application Firewall"

Product Name: Web application firewall

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>WAPPFWALL.REQ.001</b>	The proposed appliance should provide integrated functionalities of Web application Firewall		
<b>WAPPFWALL.REQ.002</b>	The proposed device should support ICASA certified WAF functionality covering all the OWASP Top 10 attack categories, WAF should be ICASA/ NDPP/NSS/ etc. Lab certified.		
<b>WAPPFWALL.REQ.003</b>	The proposed appliance must provide 4 x 1G ports and 8 x 10 SFP+ ports		
<b>WAPPFWALL.REQ.004</b>	The proposed appliance should provide minimum throughput of minimum 25 Gbps		
<b>WAPPFWALL.REQ.005</b>	The solution should support minimum 5 million L7 RPS and 2.5 million L4 Connections per second.		
<b>WAPPFWALL.REQ.006</b>	The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, hardware-based compression, caching etc. in active-passive mode.		
<b>WAPPFWALL.REQ.007</b>	Proposed solution should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover for all connections which are offloaded on the device so that existing SSL connections are not lost during a failover event		
<b>WAPPFWALL.REQ.008</b>	The proposed appliance should support centralized Security policies enforcement, SSL Certificates management for workloads		
<b>WAPPFWALL.REQ.009</b>	The solution must support automatic updation of certificate bundles of CA installed on it to reduce administrative workload and simply SSL certificate management.		
<b>WAPPFWALL.REQ.010</b>	Device should support File Upload Violation & scanning for malicious content in Uploads.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>WAPFWALL.REQ.011</b>	Should Support integration with SIEM and other Monitoring and Reporting solution		
<b>WAPFWALL.REQ.012</b>	The solution should have script-based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. It should support ePolicies to customize new features/rules to re-direct the traffic on specific parameters.		
<b>WAPFWALL.REQ.013</b>	The solution should support for policy nesting at layer7 and layer4. it should able to combine layer4 and layer7 policies to address the complex application integration.		
<b>WAPFWALL.REQ.014</b>	The solution should support Web Anti-Defacement (WAD) function to detect and prevent the defaced web pages from being returned to the client.		
<b>WAPFWALL.REQ.015</b>	The solution should detect and block SQL injection attacks, support injection detection based on get, post, cookie, etc., and support the detection of code bypassing SQL injection.		
<b>WAPFWALL.REQ.016</b>	The solution should respectively support working modes and protocol detection based on IPv4 and IPv6 environments and be able to support IPv4 and IPv6 dual-stack environments.		
<b>WAPFWALL.REQ.017</b>	The solution should support negative and positive security model The positive security recognizes the characteristics of normal application traffic by automatic traffic learning in order to form the positive security model (whitelist model), which allows only traffic matching these whitelists to pass.		
<b>WAPFWALL.REQ.018</b>	Operating temperature: 0 to 40 degrees		
<b>WAPFWALL.REQ.019</b>	Humidity: 10% to 85% non-condensing		

#### 17.19 "Technical Requirements Specifications - IDAM"

Product Name: IDAM

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>IDAM.REQ.001</b>	Solution should be platform independent and can be deployed across on-premises Data Centre and in cloud environment.		
<b>IDAM.REQ.002</b>	Solution should sized for minimum 1000 Users.		
<b>IDAM.REQ.003</b>	Solution should have the ability to configure and connect to various database targets.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
IDAM.REQ.004	Solution should have the ability to reconcile with connected/ disconnected targets.		
IDAM.REQ.005	Solution should have the ability to configure and connect to Active Directory target.		
IDAM.REQ.006	Solution should support creation and management of identity of users; groups and other objects present in CHIPS system along with their respective attributes and associated identifiers. All the solution components (IDAM, SSO, MFA & PAM) shall have integration.		
IDAM.REQ.007	Solution should support automated account creation, modification, suspension, and deletion across systems and applications based on changes in the roles and entitlements of a user.		
IDAM.REQ.008	Solution should provide the capability to manage profiles and privileges of all users and groups across all application services and components through a single management interface.		
IDAM.REQ.009	Solution should provide capability to authenticate the user at the time of login and provide access to only those applications/resources/services that the user is authorized to after successful authentication.		
IDAM.REQ.010	Solution should support sending OTP on e-Mail/SMS/any other messaging platform, etc. (through multiple service providers) simultaneously.		
IDAM.REQ.011	Solution should be able to create a Group of synthetic users which will be allowed to access the application without Multi Factor Authentication (MFA).		
IDAM.REQ.012	Solution should support self-service password resets and identity proofing capability.		
IDAM.REQ.013	Solution should support account reconciliation.		
IDAM.REQ.014	Solution should support automatic failover to other IDAM instance in case of disaster at primary instance.		
IDAM.REQ.015	Solution should provide API/Services that support workflow capabilities.		
IDAM.REQ.016	Solution should support access request management with ability to provide a consistent and auditable process for requesting and approving access privileges.		
IDAM.REQ.017	Solution should have robust reporting capability to include ad hoc reporting.		
IDAM.REQ.018	Solution should ensure that the identity information and all user credentials are encrypted in storage as well as in transit between all components of the system.		
IDAM.REQ.019	Solution should support context specific step-up from password authentication to multi factor token authentication when more sensitive data or functions are requested by a user.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	Administrator should be able to control the priority / method of authentication through configurations.		
<b>IDAM.REQ.020</b>	Risk Based Authentication - Risk-based authentication uses real-time intelligence to gain a holistic view of the context behind each login. When a user attempts to sign in, a risk-based authentication solution analyses factors such as: Device, Network, Sensitivity		
<b>IDAM.REQ.021</b>	Solution must have support during review of user access rights. Users' access rights will be reviewed at regular interval.		
<b>IDAM.REQ.022</b>	Solution should detect orphaned accounts (accounts that have no associated record in a specified authoritative data source) and perform an action such as "suspend" or "notify"		
<b>IDAM.REQ.023</b>	The system shall provide comprehensive reporting such as —who has access to what, —who approved what, —orphaned accounts found and these reports should be available online or can be exported for distribution.		
<b>IDAM.REQ.024</b>	The system should have the ability to apply and evaluate identify compliance policies/rules on access privileges across multiple systems		
<b>Single Sign-On (SSO)</b>			
<b>IDAM.REQ.025</b>	Solution should support Single Sign-On (SSO) Transparent User Identification with zero impact for enterprise users.		
<b>IDAM.REQ.026</b>	Solution's SSO Portal based authentication with tracking widgets to reduce the need for repeated authentications.		
<b>IDAM.REQ.027</b>	Solution should support SAML SP/IdP Web SSO.		
<b>IDAM.REQ.028</b>	Solution should include Single Sign-on Functionality		
<b>IDAM.REQ.029</b>	Solution should provide risk-based access control, authentication and authorization of users based on different attributes		
<b>IDAM.REQ.030</b>	Solution should have its own user store or should leverage existing directories such as Active Directory or LDAP directories.		
<b>IDAM.REQ.031</b>	Solution should provides strong authentication and multi-factor authentication to web and federated applications		
<b>IDAM.REQ.032</b>	Solution should maintain logs for user access without exposing passwords		
<b>IDAM.REQ.033</b>	The solution shall provide out-of-the-box integration to the following directories for authentication		
<b>IDAM.REQ.034</b>	a. Active Directory,		
<b>IDAM.REQ.035</b>	b. LDAP Directory		
<b>IDAM.REQ.036</b>	c. AAA Server		
<b>IDAM.REQ.037</b>	The solution shall support strong (two-factor) authentication technologies at least with the following:		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
IDAM.REQ.038	a. Dynamic/One Time Password		
IDAM.REQ.039	b. Two-Factor Token		
IDAM.REQ.040	c. Digital Certificates		
IDAM.REQ.041	The solution shall support integration to various security repositories (eg. Active Directory, LDAP, Database, etc) to achieve Single Sign-On.		
<b>Multi Factor Authentication</b>			
IDAM.REQ.042	The Multi Factor Authentication solution shall support authentication mechanism like Hardware USB Token/Hardware Token/ Mobile Token/ email Token /SMS Token.		
IDAM.REQ.043	Every token shall have unique identity & shall be unique to user.		
IDAM.REQ.044	The Multi Factor Authentication solution shall support authentication mechanisms OAUTH, SAML & OpenID Connect		
IDAM.REQ.045	Solution should be Standards-based secure authentication which works in conjunction with soft tokens to deliver secure two-factor authentication to any third-party device capable of authentication via RADIUS or LDAP.		
<b>Privilege Access Management (PAM)</b>			
IDAM.REQ.046	Solution should be platform independent and can be deployed across on-premises Data Centre and in cloud environment.		
IDAM.REQ.047	Solution should be supported on the hyperconverged infrastructures.		
IDAM.REQ.048	Solution should support IPV6 enabled endpoints like Web SSH, SSH Relay, Web RDP etc. The security level of the information system being connected should not be downgraded upon any such interconnect of systems.		
IDAM.REQ.049	User access to the solution should be via encrypted channel only.		
IDAM.REQ.050	Solution should allow access of only authorized application/component/service functionalities based on the privileges provided to the logged in user. The system should be based on zero trust.		
IDAM.REQ.051	At the time of Login, the solution should provide access to the users based on zero trust.		
IDAM.REQ.052	Solution should allow to secure, manage, automate and log all activities associated with the privileged accounts for audit trail purpose.		
IDAM.REQ.053	Solution should support password management as per data center security policy and requirements.		
IDAM.REQ.054	Solution should include handling access permissions based on roles and policies.		
IDAM.REQ.055	Solution should have the ability to define a fixed number of parameters that control administrative access with limited access to specific functions and resources.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>IDAM.REQ.056</b>	Administrator should be able to create authorization policy for any User, Group (including dynamic groups), Role, or ad-hoc user(s) etc.		
<b>IDAM.REQ.057</b>	Solution should share a common infrastructure for managing, securing, and tracking shared privileged accounts.		
<b>IDAM.REQ.058</b>	Solution should enforce users to specify reason when requesting access for a privileged account.		
<b>IDAM.REQ.059</b>	Solution should have the facility to generate new password automatically every time the user tries to login.		
<b>IDAM.REQ.060</b>	Solution should be policy based and should be used to configure different policies for privileged accounts on different platforms and components.		
<b>IDAM.REQ.061</b>	Solution should provide web browser-based UI for users to perform activities such as account management, privilege request, approval, viewing audit trail, etc.		
<b>IDAM.REQ.062</b>	Solution should have the capability to enforce time-limited secure remote access of data center environments without having to expose credentials to external users e.g., providing guest login to 3rd party vendor staff etc.		
<b>IDAM.REQ.063</b>	Solution should enable archival of audit logs.		
<b>IDAM.REQ.064</b>	Solution should generate audit trail reports for reviews and analysis.		
<b>IDAM.REQ.065</b>	Solution should have session timeout capabilities, when session remains idle, and this parameter should be configurable.		
<b>IDAM.REQ.066</b>	Solution should have capability of integration with SIEM for log forwarding.		
<b>IDAM.REQ.067</b>	Solution should create isolation between the privileged user's desktop and the target system, which eliminates the risk of planting malware on critical systems.		
<b>IDAM.REQ.068</b>	Solution should control, monitor, and record all privileged sessions.		
<b>IDAM.REQ.069</b>	Solution should be able to map local drive or directory during an RDP session.		
<b>IDAM.REQ.070</b>	Solution should provide full session recording.		
<b>IDAM.REQ.071</b>	Solution should have the ability to perform SHA (Secure Hash Algorithms) verification every time the session recording is being played or provide tamper proof session recordings features to ensure the session recording integrity is not compromised.		
<b>IDAM.REQ.072</b>	Solution should provide facility to monitor in real time and video recording of the privileged sessions for all the integrated devices, users and applications.		
<b>IDAM.REQ.073</b>	There should be no mechanism to export any password from the PAM vault under any circumstances.		



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>IDAM.REQ.074</b>	The proposed solution should support integration with enterprise infrastructure including strong authentication such as 2-factor & Radius		

## 17.20 "Technical Requirements Specifications - Network Access Control"

Product Name: Network Access control

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>NAC.REQ.001</b>	Proposed Network Access Control solution (NAC) should Control access of end points with defined policies, Also it should provide quarantine, remediation and orchestration to maintain the security infrastructure		
<b>NAC.REQ.002</b>	A captive portal intercepts HTTP access to web pages, redirecting users to a web application that provides instructions and tools for updating their computer. Until their computer passes automated inspection, no network usage besides the captive portal should be allowed		
<b>NAC.REQ.003</b>	The proposed NAC Solution should be offered with all supported features for all Data Center I.T devices.		
<b>NAC.REQ.004</b>	Solution should be able to detect, classify and restrict all endpoints based on various parameters.		
<b>NAC.REQ.005</b>	NAC solution should authenticate each user and machine connecting/accessing the network through any authentication server as RADIUS, LDAP, Active Directory, etc. The solution should support inbuilt and Integrated scalable AAA services (authentication, authorization, and accounting) for endpoints including access policy management.		
<b>NAC.REQ.006</b>	NAC solution should assess whether the connecting endpoint complies with the defined security policy.		
<b>NAC.REQ.007</b>	NAC solution should have the ability to automatically quarantine/block an endpoint that does not comply with the defined security policy until the issues causing it to be non-compliant are fixed.		
<b>NAC.REQ.008</b>	NAC solution should verify user's access to the network according to an authorization scheme defined in in-built or an existing authorization system, such as Active Directory, etc. allowing the enforcement of identity-based policies after an endpoint is allowed on the network.		
<b>NAC.REQ.009</b>	The proposed solution should support vendor agnostic infrastructure and operate in a heterogeneous environment from multiple OEMs		
<b>NAC.REQ.010</b>	The proposed NAC solution should have the capability to provide visibility for all endpoints .		



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>NAC.REQ.011</b>	Solution should be deployable in both 802.1x and non 802.1x environment and should support hybrid integration for managing the endpoint with all functionalities available in NAC.		
<b>NAC.REQ.012</b>	The proposed solution must support both agent based & Agentless deployment and provide complete posture analysis.		
<b>NAC.REQ.013</b>	The Solution should support all the features& Functionalities like Profiling, Compliance check, Remediation, Blocking, reporting, alerting the device admin, notifying the end user etc.		
<b>NAC.REQ.014</b>	The propose solution should support Guest users on-boarding through self-register web portal and provide access of network as per the policy defined to limit access to specific resources, length of connections and set automatic account expiry after a specified number of hours or days. User Credentials should be delivered through SMS or email.		
<b>NAC.REQ.015</b>	The propose solution should support exception in policies for endpoints based on various parameters viz. hostname, IP address, MAC address, identity group, type of assets location, etc.		
<b>NAC.REQ.016</b>	Solution should maintain detailed information and up-to-date/centralized inventory of endpoints		
<b>NAC.REQ.017</b>	The solution should verify endpoint posture assessment for PCs connecting to the network		
<b>NAC.REQ.018</b>	The proposed solution should be deployed in a cluster environment with at least N+ 1 redundancy to ensure system availability in the event of any component failure.		
<b>NAC.REQ.019</b>	The proposed solution able to support both IPv4 and IPv6 dual stack deployments.		
<b>NAC.REQ.020</b>	Solution should have a Centralized Management for managing, monitoring & controlling for all the features of the NAC.		
<b>NAC.REQ.021</b>	Centralized Management solution must have executive, detail and customizable dashboard and support role-based users/admins.		
<b>NAC.REQ.022</b>	The solution should able to categorize the alerts on the basis of risk (high, medium and low), type of devices, location etc.		
<b>NAC.REQ.023</b>	The solution should offer a built-in alerting mechanism through email & SMS based on the categorization of alerts.		
<b>NAC.REQ.024</b>	The solution should have a single web-based or client based. GUI console for admin users for managing the full functionalities of NAC solution.		
<b>NAC.REQ.025</b>	The solution must allow user's access to the network in a worst case scenario in case of AAA server outages or any other reasons like WAN failure.		
<b>NAC.REQ.026</b>	Solution should log each & every session/all important events and parameters for forensic and statistical reports. Logs should be exportable to external log server in readable formats.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>NAC.REQ.027</b>	The proposed solution must be able to generate/customized reports from logs available online and offline on different parameters		

## 17.21 "Technical Requirements Specifications - EMS,NMS and ITSM"

Product Name: EMS , NMS, ITSM

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>a</b>	<b>EMS, NMS, ITSM and Patch Management General Software Specifications</b>		
<b>EMS.REQ.001</b>	The proposed EMS solution should be an integrated and scalable solution		
<b>EMS.REQ.002</b>	It should have single pane of glass visibility across multiple areas of monitoring & management.		
<b>EMS.REQ.003</b>	The proposed monitoring solution deployment shall support latest version of Window/ Linux Operating Systems		
<b>EMS.REQ.004</b>	The proposed EMS solution must have the Integration capability using REST API and/or SNMP or any equivalent solution.		
<b>b</b>	<b>Server Fault and Performance Monitoring Management</b>		
<b>EMS.REQ.005</b>	The proposed Enterprise Management tools must be able to monitor end to end performance of Server Operating Systems and database, system should be able to manage distributed heterogeneous systems – Windows, LINUX from a single management station.		
<b>EMS.REQ.006</b>	The solution should support Agent-based and Agent less Monitoring .		
<b>EMS.REQ.007</b>	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS.		
<b>EMS.REQ.008</b>	It should have capability to perform correlation from Network Monitoring tool, Systems monitoring and other domain monitoring tools.		
<b>EMS.REQ.009</b>	The solution should have ability to track status of its critical components & parameters such as Up/Down status of its services, servers CPU utilization, Memory capacity, synchronization status between systems and event processing etc. It should provide this information in real-time through graphical dashboards, events/alarms as well as in the form of historical reports.		
<b>EMS.REQ.010</b>	It should create topology maps containing devices discovered in different physical, virtual servers and select multiple devices discovered in different physical, virtual servers while generating the reports.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>EMS.REQ.011</b>	The Stakeholder Dashboard should be able to provide reports across domains.		
<b>EMS.REQ.012</b>	The solution also must have the capability to build and generate the custom reports and dashboards.		
<b>EMS.REQ.013</b>	The solution must be able to collect following minimum Server Monitoring Parameters:		
	a. Disk failure		
	b. CPU Failure		
	c. Memory/ RAM failure & utilization		
	d. Event logs		
	e. OS Monitoring		
	f. CPU Utilization		
	g. Disk Utilization		
	h. Cluster Monitoring		
<b>c</b>	<b>Alarm Correlation and Root Cause Analysis Capabilities</b>		
<b>EMS.REQ.014</b>	Solution should provide alarm correlation and facilitate reduction of total number of alarms displayed . The system must ensure reduction in MTTR by means of advanced event correlation, filtering ,root cause analysis or using any other technique.		
<b>EMS.REQ.015</b>	The proposed Alarm Correlation and Root Cause Analysis system shall integrate performance information. The current performance state of the entire network & system infrastructure shall be visible.		
<b>EMS.REQ.016</b>	The proposed solution should provide root cause analysis functionality		
<b>EMS.REQ.017</b>	solution should provide functionalities to convert critical Alarms into Incidents for auto ticket generation into proposed Helpdesk tool.		
<b>EMS.REQ.018</b>	It should also provide an intuitive interface for designing, creating, customized flows , reports and dashboards to monitor the flow in the operations.		
<b>EMS.REQ.019</b>	The proposed solution should provide various workflows to automate use cases.		
<b>d</b>	<b>Network Fault Monitoring &amp; Performance Management with Reporting</b>		
<b>EMS.REQ.020</b>	The Network Management function must monitor performance of SNMP enabled network devices across heterogeneous networks .		
<b>EMS.REQ.021</b>	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, discovering devices and interfaces.		
<b>EMS.REQ.022</b>	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, Firewalls etc.) and map the connectivity between them with granular visibility.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
EMS.REQ.023	It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across data center infrastructure.		
EMS.REQ.024	The proposed solution must support discovery mechanisms and should discover new devices using mechanisms such as SNMP discovery or any other mechanism. It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms		
EMS.REQ.025	The solution must provide reports to identify unused/dormant Network ports in order to facilitate capacity planning		
e	<b>Network Configuration Automation</b>		
EMS.REQ.027	The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-vendor network tool.		
EMS.REQ.028	The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “start-up” configurations and alert the administrators.		
EMS.REQ.029	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements: a) Capture running configuration, b) Capture start-up configuration, c) Upload configuration, d) Write start-up configuration, e) Upload firmware Etc.		
EMS.REQ.030	The proposed solution should provide Dashboards of network infrastructure. With this dashboard, operator should be able to see the most offending devices in the group along with the non-compliant devices.		
EMS.REQ.031	The solution should focus on all dimensions of network compliance including but not limited to defining configuration policies and tracking OS versions and patches.		
EMS.REQ.032	The proposed solution should be highly scalable as per solution requirements		
EMS.REQ.033	The propose solution should have diagnostic analytics capability that able to visually correlate performance and configuration changes of all network issues.		
EMS.REQ.034	NMS should support out of the monitoring of all the IT devices of all OEM,s/vendors in the Data Center		
f	<b>Consolidated Dashboard</b>		
EMS.REQ.035	The platform must provide complete cross-domain visibility of IT infrastructure issues.		
EMS.REQ.036	The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database and cloud.		
EMS.REQ.037	The solution should support dynamic discovery to maintains Run-time Service Model accuracy e.g. virtualization and cloud.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
EMS.REQ.038	The solution must support custom dashboards for different role users such as Management, admin and report users.		
EMS.REQ.039	The solution must allow creating custom data widget to visualize data with user preferences.		
EMS.REQ.040	The solution must support multiple visualization methods.		
EMS.REQ.041	The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console.		
EMS.REQ.042	The solution should allow for customizable operator perspectives.		
EMS.REQ.043	The solution must have role based access to the dashboards.		
g	<b>IT Service Management/Helpdesk Systems</b>		
EMS.REQ.044	Should able to support and handle a large volume of the incident, service requests, changes, etc via concurrent operators.		
EMS.REQ.045	Should able to integrate with third-party IVR or CTI.		
EMS.REQ.046	The Helpdesk solution should allow Multi-Tenancy.		
EMS.REQ.047	Auto allocation of incidents: Solution should provide the flexibility of automated incident assignment based on multiple metrics		
EMS.REQ.048	Incident Categorization: Solution should provide multi-level ticket category classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, Business Urgency levels and Business impact levels.		
EMS.REQ.049	The proposed IT Service Management solution should be certified by Pink Elephant PINK VERIFY /ITIL V4 certified for minimum 9 ITIL processes		
EMS.REQ.050	The solution should support SLA violations alerts during the tracking period.		
EMS.REQ.051	The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators measured across infrastructure and vendors		
EMS.REQ.052	MSI shall propose a full-fledged Service Level Management Solution that allows for tracking of various service level performances of IT Infrastructure.		
EMS.REQ.053	Proposed ITSM solution should have mobile app for Android and iPhone users and Request and Incident management features should be available on the mobile app.		
h	<b>Auto-Discovery and Asset Inventory Management</b>		
EMS.REQ.054	Should use Industry-standard protocols such as SNMP to perform discovery.		
EMS.REQ.055	Proposed Tool should support both Hybrid Discovery (both agent based and agent less discovery).		
EMS.REQ.056	Asset Management Proposed Tool should support Asset portfolio management.		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
EMS.REQ.057	Proposed Solution must support multi tenant architecture.		
EMS.REQ.058	The ITSM & ITAM should have Integration capability		
i	<b>Patch Management</b>		
EMS.REQ.059	The proposed solution should provide lifecycle management across heterogeneous virtual and physical servers including patching, compliance, audit and remediation.		
EMS.REQ.060	The proposed solution should provide dynamic, real-time, and historical reports into hardware, software, patches, and operations activities in complex and heterogeneous data centres.		
EMS.REQ.061	The proposed solution should support audit and remediation .		
EMS.REQ.062	The proposed solution should provide remediation with maintenance windows and exception management.		
EMS.REQ.063	The proposed solution should provide redundancy, resiliency and scalability .		
EMS.REQ.064	The proposed solution should provide role-based access control (RBAC) to manage user authentication and authorization.		
EMS.REQ.065	The system should support manual and scheduled triggering of patch scans.		
EMS.REQ.066	The system should support custom actions as part of end-to-end scan and patching.		
EMS.REQ.067	The system should support manual and scheduled triggering of compliance scans.		
EMS.REQ.068	The system should provide a dashboard to display the top non-compliant resources in the data-centre .		
EMS.REQ.069	System should maintain a patch repository.		
EMS.REQ.070	System should allow for patch policies to be set, enforced, and applied.		

## 17.22 "Technical Requirements Specifications - Hardware Security Module(HSM)"

Product Name: Hardware Security Module(HSM)

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
HSM.REQ.001	General Aspects	HSM should have dual power , dual TCP/IP interface and dual connectivity support. Speed: Minimum 5000 TPS/ CPS (Transactions per second/ Commands per second )		
HSM.REQ.002	General Aspects	Should support SHA-256 RSA 2048 Format or above. Capable to support 3DES KEY lengths 112bit		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		&168 bit and AES key lengths 128, 192 & 256 bits.		
<b>HSM.REQ.003</b>	General Aspects	Support multi-threading & multi-client so as maximum performance can be achieved.		
<b>HSM.REQ.004</b>	General Aspects	Should support algorithms AES & 3DES		
<b>HSM.REQ.005</b>	Management facilities	Support SNMP V2 and V3		
<b>HSM.REQ.006</b>	Management facilities	Utilization statistics - Health check diagnostic and error logs		
<b>HSM.REQ.007</b>	Management facilities	FIPS complaint HSM should have dedicated management Ethernet port with minimum 2X1G & 2X10G network interface.		
<b>HSM.REQ.008</b>	Security Certification	Cryptographic module certified to FIPS:140-2 Level 3		
<b>HSM.REQ.009</b>	Security Certification	FIPS 140-2 level 3 (Device should be FIPS certified and proof must be submitted as a part of compliance)		
<b>HSM.REQ.010</b>	Security Certification	SP800-90B/SP800-90C/BSI DRG.4		
<b>HSM.REQ.011</b>	Security Certification	FIPS compliant Random number generator		
<b>HSM.REQ.012</b>	Security Certification	FIPS approved algorithms		
<b>HSM.REQ.013</b>	Security features	Tamper resistance meeting requirements of FIPS 140-2 Level 3		
<b>HSM.REQ.014</b>	Security features	Detection of cover removal in addition to Alarm triggers as per FIPS Standard		
<b>HSM.REQ.015</b>	Security features	Multiple alarm triggers for motion, voltage and temperature as per FIPS Standard		
<b>HSM.REQ.016</b>	Security features	Device hardening as per FIPS Standard		
<b>HSM.REQ.017</b>	Security features	Triple-DES key lengths 112 & 168 bit		
<b>HSM.REQ.018</b>	Security features	AES key lengths 128, 192 & 256 bit		
<b>HSM.REQ.019</b>	Security features	RSA (up to 4096 bit)		
<b>HSM.REQ.020</b>	Security features	HMAC, MD5, SHA-1, SHA-2		
<b>HSM.REQ.021</b>	Key Features	Secure Key Storage and Generation for all key types used		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
HSM.REQ.022	Key Features	Secure Host communication using TLS or SSL		
HSM.REQ.023	Key Features	Remote management and monitoring options.		
HSM.REQ.024	Key Features	Safety and environmental compliances certifications as per BIS standard		
HSM.REQ.025	Other Features	Must support cryptographic offloading and acceleration		
HSM.REQ.026	Other Features	Should provide authenticated multi-role access control		
HSM.REQ.027	Other Features	Must have strong separation of administration and operator roles		
HSM.REQ.028	Other Features	Must have secure key wrapping, backup, replication and recovery		
HSM.REQ.029	Other Features	Must support 2048, 4096 and 2048 bit RSA private keys, 256 bit AES keys on FIPS 140-2 Level 3		
HSM.REQ.030	Other Features	Must support clustering and load balancing		
HSM.REQ.031	Other Features	Should support cryptographic separation of application keys using logical partitions		
HSM.REQ.032	Other Features	Minimum 2X1G & 2X10G with Port Bonding		
HSM.REQ.033	Other Features	Asymmetric public key algorithms: RSA, Diffie Hellman, DSA, ECDSA, ECDH,ECIES.		
HSM.REQ.034	Other Features	Symmetric algorithms: AES, HMAC, Triple DES		
HSM.REQ.035	Other Features	Hash/message digest: SHA-1,SHA-2(224,256,384,512 bit)		
HSM.REQ.036	Other Features	Support remote administration – including adding applications, updating firmware, and checking status from centralized Location		
HSM.REQ.037	Other Features	Syslog diagnostics support		
HSM.REQ.038	Other Features	HSM should have Dual Physical lock		
HSM.REQ.039	Other Features	Should have ability to regularly expand functionality via firmware or application upgrades.		
HSM.REQ.040	Other Features	Should have physical and logical security features.		
HSM.REQ.041	Other Features	Should adhere to all major industry standards, including FIPS-140-2 level 3.		
HSM.REQ.042	Other Features	Should have multiple, redundant power supplies and ethernet ports to maintain functionality in the event that one of the either sources should fail.		
HSM.REQ.043	Other Features	Should support remote access technology with encrypted connection to maintain security in		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		all configuration and remote key loading processes.		
<b>HSM.REQ.044</b>	Other Features	Must maintain compatibility with wide range of host applications		

### 17.23 "Technical Requirements Specifications - Host Intrusion Prevention System(HIPS)"

Product Name: Host Intrusion Prevention System(HIPS)

Sr. No	Host Intrusion Prevention System(HIPS)	Compliance (Yes / No)	Reference (Document /Page no)
<b>HIPS.REQ.001</b>	The solution should enable threat detection, identification, and prevention		
<b>HIPS.REQ.002</b>	The solution should analyses all packets to and from the server for intrusion attempts and propagation		
<b>HIPS.REQ.003</b>	The solution should encompasses host-based firewall capability. Must allow definition of		
<b>HIPS.REQ.004</b>	The solution should encompasses host-based firewall capability. Must allow definition of network-level filtering rules based on source and destination IP/network address, protocol, and source and destination ports in support of organizational security policy to allow/disallow specific types of activity between hosts		
<b>HIPS.REQ.005</b>	The solution should combine NIPS (network) and HIPS (host) based signature to proactively protect against intrusion targeted at the servers or provide attack prevention using the least privilege containment approach		
<b>HIPS.REQ.006</b>	The solution should support adaptive mode to automatically learn rules or have integrated approach to block inbound and outbound TCP/UDP traffic		
<b>HIPS.REQ.007</b>	The solution should use vulnerability based and not exploit based signatures or prevent intrusions by using the least privilege containment approach. It should detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability)		
<b>HIPS.REQ.008</b>	The solution should use vulnerability based and not exploit based signatures or prevent intrusions by using the least privilege containment approach. It should detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).		
<b>HIPS.REQ.009</b>	The solution should provide protection for Web Server and Database Server		
<b>HIPS.REQ.010</b>	The solution should have provision to protect Web applications by inspecting SSL-encrypted		
<b>HIPS.REQ.011</b>	HTTP traffic streams before they reach the application		

Sr. No	Host Intrusion Prevention System(HIPS)	Compliance (Yes / No)	Reference (Document /Page no)
<b>HIPS.REQ.012</b>	The solution should protect against SQL injection attacks		
<b>HIPS.REQ.013</b>	The solution should have provision to protect against cross-site scripting (XSS) attacks		
<b>HIPS.REQ.014</b>	The solution should support system lock-down by blocking all the applications to run on the system. The administrator can create a white list of application so that only those applications are allowed to be executed		
<b>HIPS.REQ.015</b>	The solution should encompass a wide array of built-in alerting, blocking, and logging responses for each event.		
<b>HIPS.REQ.016</b>	The solution should support response adjustment on a per signature/policy basis.		
<b>HIPS.REQ.017</b>	The solution should have the option to block intruder for a particular period of time or should have targeted		
<b>HIPS.REQ.018</b>	prevention policy to respond to server incursion		
<b>HIPS.REQ.019</b>	The agents shall be managed by a central administration system designed for large-scale enterprise deployments		
<b>HIPS.REQ.020</b>	The solution should support a wide variety of reports.		

#### 17.24 "Technical Requirements Specifications - Network Detection response (NDR)"

Product Name: Network Detection response (NDR)

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
<b>NDR.REQ.001</b>	General Requirement	Proposed NDR Systems should be hardware-based appliances.		
<b>NDR.REQ.002</b>	General Requirement	All systems / subsystems of proposed NDR systems should have dual redundant hot swappable internal power supply.		
<b>NDR.REQ.003</b>	General Requirement	Proposed NDR systems should have adequate inbuilt storage for retaining minimum 30 days data from day 1.		
<b>NDR.REQ.004</b>	General Requirement	The solution should be sized as per the inventory details shared in RFP considering 30 % escalation from day 1.		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
<b>NDR.REQ.005</b>	General Requirement	Bidder is to quote hardware appliances (i.e., Compute, Memory, storage, Operating Systems, DB, replication and corresponding licenses etc.). Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. In case of any shortfall in hardware and software, the OEM will be responsible to supply additional hardware and software without any financial cost to User to ensure successful deployment of the NDR solution. All hardware and software components of appliance-based solutions must be hardened to ensure security of the system and all versions of OS/firmware/patch update schedule/ best practices must be shared by OEM with User.		
<b>NDR.REQ.006</b>	Visibility & Identity Awareness	The NDR tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.		
<b>NDR.REQ.007</b>	Visibility & Identity Awareness	The NDR solution should also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		or resource misuse or misconfiguration.		
<b>NDR.REQ.008</b>	Visibility & Identity Awareness	The Solution should be able to detect Malwares on both encrypted and non-encrypted payloads.		
<b>NDR.REQ.009</b>	Visibility & Identity Awareness	By collecting, analysing and storing available log information from various sources, NDR System should provide a full audit trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.		
<b>NDR.REQ.010</b>	Functional Requirements	The solution should be able to provide real-time monitoring and visibility into all network traffic, using machine learning, context-aware analysis, and on-premise threat detection and analytics.		
<b>NDR.REQ.011</b>	Functional Requirements	Network Detection and Response (NDR) solutions take advantage of the flow technologies built into network devices. NDR tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs data into meaningful analytics data like numbers charts and tables that quantify exactly how the network is being used, by whom and for what purpose.		
<b>NDR.REQ.012</b>	Functional Requirements	Unsupervised and supervised machine learning along with probabilistic mathematics without predefined rules and signatures should be employed by the solution to detect significant anomalies and drifts in user,		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		device or network activities and traffic that signal an attack		
<b>NDR.REQ.013</b>	Functional Requirements	The solution should provide contextual network-wide visibility via an agentless approach.		
<b>NDR.REQ.014</b>	Functional Requirements	NDR solution should be able to use the existing network environment as a sensor grid to analyse traffic flow across the across the existing network and security solutions in a non-disruptive manner		
<b>NDR.REQ.015</b>	Functional Requirements	The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.		
<b>NDR.REQ.016</b>	Functional Requirements	The solution should identify the source of an attack and should not block legitimate users.		
<b>NDR.REQ.017</b>	Functional Requirements	The solution should allow analysis by grouping of network segments such as user VLAN, management VLAN, server farms etc.		
<b>NDR.REQ.018</b>	Functional Requirements	The system should be able to monitor flow data between various VLANs.		
<b>NDR.REQ.019</b>	Functional Requirements	The solution should have the capability of application profiling in the system and also support custom applications present or acquired by the end user.		
<b>NDR.REQ.020</b>	Functional Requirements	The solution should have the capability to enrich flow records with additional fields including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviours.		
<b>NDR.REQ.021</b>	Functional Requirements	The solution must be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.		
<b>NDR.REQ.022</b>	Functional Requirements	The solution should support all forms of flows including but not limited to NetFlow, IPFIX, sFlow, Jflow, cFlowd, NSEL.		
<b>NDR.REQ.023</b>	Functional Requirements	The solution should be able to combine/stitch the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation and present them as a single bi-directional flow record.		
<b>NDR.REQ.024</b>	Functional Requirements	The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.		
<b>NDR.REQ.025</b>	Functional Requirements	The solution must provide an application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.		
<b>NDR.REQ.026</b>	Functional Requirements	The solution must probe the network in a manner so that impact on network performance is minimal.		
<b>NDR.REQ.027</b>	Functional Requirements	The solution must be an out of band analytics engine from the primary data path.		
<b>NDR.REQ.028</b>	Functional Requirements	The system should provide detailed visibility to identify devices/servers/subnet		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		information within a network automatically.		
<b>NDR.REQ.029</b>	Functional Requirements	The solutions should provide the capability of behavioural analysis on a user-defined relationship between groups of network assets based on certain parameters like services, protocols and tolerance.		
<b>NDR.REQ.030</b>	Functional Requirements	The solution should have capability to assign risk and credibility rating to alerts and hosts and present critical high-fidelity alerts prioritized based on threat severity with contextual information on the dashboard.		
<b>NDR.REQ.031</b>	Functional Requirements	The solution should provide use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.		
<b>NDR.REQ.032</b>	Functional Requirements	The solution should provide the capability to define custom policies to evaluate flow attributes such as byte ratios, services, process, name and more.		
<b>NDR.REQ.033</b>	Functional Requirements	The tool should have capability for interactive event identification and creating business logic and policies for threat detection.		
<b>NDR.REQ.034</b>	Functional Requirements	The solution must have the capability to identify network traffic from high-risk applications such as file sharing, peer-to-peer communications.		
<b>NDR.REQ.035</b>	Threat Detection Capabilities	The NDR solution should provide enterprise-wide network visibility and apply advanced security analytics to detect and respond to threats in real time. NDR solutions must be able to detect threats such as reconnaissance, data hoarding/exfiltration, distributed-denial-of- service		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		(DDoS) attacks and insider threats.		
<b>NDR.REQ.036</b>	Threat Detection Capabilities	The solution shall use behavioural technology and machine learning and advanced entity modelling to reduce false positives. Solution should detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.		
<b>NDR.REQ.037</b>	Threat Detection Capabilities	Mathematical modelling to create statistically significant views of user, device and network behaviours and detecting attacks that are already within the enterprise.		
<b>NDR.REQ.038</b>	Threat Detection Capabilities	Detect in-progress attacks as they evolve and true 360o view in the networks like whom and what is really using your data or facilities.		
<b>NDR.REQ.039</b>	Threat Detection Capabilities	Assess weak links (Inside users) of the network as an early indicator to determine the target threats.		
<b>NDR.REQ.040</b>	Threat Detection Capabilities	Must automatically learn a normal pattern of life" for every user, device and network and is capable of detecting the most subtle cyber- threats within the network, including insider threat.		
<b>NDR.REQ.041</b>	Threat Detection Capabilities	The solution must detect anomalous data transfer from/to the corporate network or within the network.		
<b>NDR.REQ.042</b>	Threat Detection Capabilities	The solution must detect unusual, unauthorized behavior within the network. This includes but is not restricted to unusual RDP, port scanning, unauthorized new devices plugged in, unauthorized use of access		



Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		credentials to internal resources.		
<b>NDR.REQ.043</b>	Threat Detection Capabilities	Systems can produce detailed visibility to identify devices/servers/subnet information within a network automatically.		
<b>NDR.REQ.044</b>	Threat Detection Capabilities	System monitors traffic passively without being invasive on the network with the ability to send alerts in real time.		
<b>NDR.REQ.045</b>	Threat Detection Capabilities	System has the capability to historically track the location, dates first/last seen and summary of malicious activity.		
<b>NDR.REQ.046</b>	Threat Detection Capabilities	System uses mathematical algorithms to assess model breaches with a rating based on level of anomaly to the specific network which allows alerts to be raised on a percentile basis.		
<b>NDR.REQ.047</b>	Threat Detection Capabilities	The solution should perform analysis on network data all the way up to the Layer 7 and provide complete application visibility		
<b>NDR.REQ.048</b>	Threat Detection Capabilities	The solution should be able to detect command and control and bot communication based on the domain/URL the user is trying to access.		
<b>NDR.REQ.049</b>	Threat Detection Capabilities	The solution should have DNS Threat Analytics Capability to detect the threat present in DNS traffic.		
<b>NDR.REQ.050</b>	Threat Detection Capabilities	The solution should be able to detect vertical and horizontal scans within the environment		
<b>NDR.REQ.051</b>	Threat Detection Capabilities	The solution should highlight weak ciphers being used in the network by hosts or applications. The solution should search and monitor cipher suites and report on which ones are used on the network.		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
<b>NDR.REQ.052</b>	Threat Detection Capabilities	The solution should be able to analyse SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese).		
<b>NDR.REQ.053</b>	Threat Detection Capabilities	Ability to detect ransomwares and profiling malwares such as Troldeh, Dridex, Quakbot, TrickBot, Gootkit, Adware, TorrentLocker, Adwind, Tofsee, Gozi, Jbifrost, Dyre, Zeus, Gameover, chinad, bamital, Post Tovar GOZ, corebot, cryptominers, etc		
<b>NDR.REQ.054</b>	Threat Detection Capabilities	The solution must support VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions.		
<b>NDR.REQ.055</b>	Threat Detection Capabilities	The solution must support port-agnostic protocol detection. The solution should be capable of detecting protocols and applications despite them using non-standard TCP/UDP ports.		
<b>NDR.REQ.056</b>	Threat Detection Capabilities	NDR solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish "normal" traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
<b>NDR.REQ.057</b>	Threat Detection Capabilities	The solution should detect events of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including network flood events of ICMP, UDP, TCP SYN, TCP NULL, IP NULL, identify the presence of botnets in the network, etc. and detect long-lived connections that may be associated with data-exfiltration.		
<b>NDR.REQ.058</b>	Threat Detection Capabilities	The solution must utilize anomaly detection methods to identify attacks such as self-propagating malware and worms/viruses, lateral movement, resource misuse or mis-configuration.		
<b>NDR.REQ.059</b>	Integration	Solution shall support NTP server time synchronization.		
<b>NDR.REQ.060</b>	Integration	The NDR solution must be able to interoperate with the Data center, Core and Campus network to track endpoints and provide end-to-end visibility and control.		
<b>NDR.REQ.061</b>	Integration	The solution must integrate with existing security solutions like Security Information and Event Management (SIEM), Next-generation Firewalls, Router, Switches, NAC, SOAR, Proxy, WAF, mail gateway etc. Necessary applicable licenses for integration with other security devices must be supplied from day one.		
<b>NDR.REQ.062</b>	Integration	The solution should integrate with Open LDAP, Microsoft Active Directory, RADIUS and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & provides full historical mapping of User Name to IP		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		address logins in a searchable format.		
<b>NDR.REQ.063</b>	Reporting	Solution should have built-in various reports and can create custom reports like Executive report, detection life cycle report and Health reports etc.		
<b>NDR.REQ.064</b>	Reporting	The solution should have the ability to generate reports in different formats, such as html, excel, csv and pdf. Reports should be available in real time on demand and should automatically be generated on a scheduled basis. Should support scheduled reports to be delivered via email automatically.		
<b>NDR.REQ.065</b>	Reporting	Solution should come with predefined & customizable reports and should have ability to run certain reports based on security role.		
<b>NDR.REQ.066</b>	Reporting	The system should have the capability to historically track the dates first/last seen, and summary of malicious activity.		
<b>NDR.REQ.067</b>	Management	The proposed solution should have Centralized Management systems supporting role-based administration		
<b>NDR.REQ.068</b>	Management	The solution must be deployed in Centralized mode with central management and reporting from the single dashboard for the entire deployment.		
<b>NDR.REQ.069</b>	Management	Enables administrators to centrally configure		
<b>NDR.REQ.070</b>	Management	The solution should support the backup and recovery of policies/configuration.		
<b>NDR.REQ.071</b>	Management	The solution should support the capability to alert the admin and provide mitigation action like quarantine or		

Sr. No	Parameter	Network Detection response (NDR)	Compliance (Yes / No)	Reference (Document /Page no)
		block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm.		
<b>NDR.REQ.072</b>	Management	The solution should have capability to categorize hosts into logical groups by observing traffic to achieve smarter segmentation. Admin may confirm, exclude or ignore any suggestion based on the network architecture.		

## 17.25 "Technical Requirements Specifications – EDR"

Product Name: (EDR)

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.001</b>	General Requirements	Single lightweight agent for endpoint protection, detection, and response		
<b>EDR.REQ.002</b>	General Requirements	Protection against malware, ransomware, and fileless attacks		
<b>EDR.REQ.003</b>	General Requirements	Zero-delay signatures to rapidly deliver protection and share threat intelligence		
<b>EDR.REQ.004</b>	General Requirements	Solution should support Behaviour-based threat prevention for dynamic analysis of running processes and Exploit prevention by exploit technique		
<b>EDR.REQ.005</b>	General Requirements	Solution should support known threat prevention based on threat intelligence, such as file hashes		
<b>EDR.REQ.007</b>	General Requirements	Network inspection engine to stop network-based attacks		
<b>EDR.REQ.009</b>	General Requirements	Ad hoc and scheduled scanning of endpoints		
<b>EDR.REQ.010</b>	General Requirements	Solution should support Machine learning-based local analysis and threat prevention		
<b>EDR.REQ.011</b>	General Requirements	Single lightweight agent for endpoint protection, detection, and response		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.012</b>	General Requirements	Protection against malware, ransomware, and fileless attacks		
<b>EDR.REQ.013</b>	General Requirements	Zero-delay signatures to rapidly deliver protection and share threat intelligence		
<b>EDR.REQ.014</b>	General Requirements	Solution should support Behaviour-based threat prevention for dynamic analysis of running processes and Exploit prevention by exploit technique		
<b>EDR.REQ.015</b>	General Requirements	Solution should support known threat prevention based on threat intelligence, such as file hashes		
<b>EDR.REQ.016</b>	General Requirements	Automated integration with a cloud-based malware prevention service, with analysis reports and minimum 50 MB file size support		
<b>EDR.REQ.017</b>	General Requirements	Network inspection engine to stop network-based attacks		
<b>EDR.REQ.018</b>	General Requirements	Reverse shell protection capability		
<b>EDR.REQ.019</b>	General Requirements	Ad hoc and scheduled scanning of endpoints		
<b>EDR.REQ.020</b>	General Requirements	Solution should support Machine learning-based local analysis and threat prevention		
<b>EDR.REQ.021</b>	Endpoint Protection Requirements	Host firewall		
<b>EDR.REQ.022</b>	Endpoint Protection Requirements	Disk encryption		
<b>EDR.REQ.023</b>	Endpoint Protection Requirements	USB device control		
<b>EDR.REQ.024</b>	Endpoint Protection Requirements	Customizable prevention rules		
<b>EDR.REQ.025</b>	Visibility and Detection Requirements	Behavioural analytics to profile behaviour and detect anomalies indicative of attack by analysing network traffic, endpoint events, and user events over time		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.026</b>	Visibility and Detection Requirements	Identity analytics to detect user-based threats such as lateral movement		
<b>EDR.REQ.027</b>	Visibility and Detection Requirements	Predefined and customizable behaviour-based detection rules		
<b>EDR.REQ.028</b>	Visibility and Detection Requirements	Custom correlation rules that can retroactively detect attacks		
<b>EDR.REQ.029</b>	Visibility and Detection Requirements	Granular alert exclusions for optional tuning of endpoint, network, cloud, or third-party alerts		
<b>EDR.REQ.030</b>	Visibility and Detection Requirements	Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services		
<b>EDR.REQ.031</b>	Visibility and Detection Requirements	Ability to consume threat intelligence feeds from third-party sources in JSON and CSV formats		
<b>EDR.REQ.032</b>	Visibility and Detection Requirements	Detection of attack techniques across the attack lifecycle including discovery, lateral movement, command and control, and exfiltration		
<b>EDR.REQ.033</b>	Visibility and Detection Requirements	Demonstrated ability to detect attacker tactics and techniques through MITRE ATT&CK Evaluations		
<b>EDR.REQ.034</b>	Visibility and Detection Requirements	Tagging of MITRE ATT&CK tactics and techniques in alerts, detection rules, and incidents		
<b>EDR.REQ.035</b>	Visibility and Detection Requirements	Asset management with rogue device discovery		
<b>EDR.REQ.036</b>	Investigation Requirements	AutB33:B48 of any alert, including network alerts, if endpoint data is available		
<b>EDR.REQ.037</b>	Investigation Requirements	Visualization of the chains of execution leading up to an alert		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.038</b>	Investigation Requirements	Timeline analysis view to see all actions and alerts on a timeline		
<b>EDR.REQ.039</b>	Investigation Requirements	A 360-degree user view with user risk scores		
<b>EDR.REQ.040</b>	Investigation Requirements	A cloud investigation view with cloud-specific events and artifacts		
<b>EDR.REQ.041</b>	Investigation Requirements	Querying for indicators of compromise (IOCs) and endpoint behaviours		
<b>EDR.REQ.042</b>	Investigation Requirements	Querying for online and offline hosts		
<b>EDR.REQ.043</b>	Investigation Requirements	Querying of log data from any source, including network, cloud, endpoint, identity & forensics data		
<b>EDR.REQ.044</b>	Investigation Requirements	Advanced querying language with support for wildcards, regular expressions, JSON, data aggregating, field and value manipulation, merging of data from disparate sources, and visualization of data		
<b>EDR.REQ.045</b>	Investigation Requirements	Granular filtering and sorting of query results		
<b>EDR.REQ.046</b>	Investigation Requirements	In-context wizard that lets you search for information, perform common investigation tasks, or initiate response actions from anywhere in the management console		
<b>EDR.REQ.047</b>	Investigation Requirements	Automatic aggregation of relevant IP or hash information, including threat intelligence, events, and related incidents in a single view to simplify investigations		
<b>EDR.REQ.048</b>	Investigation Requirements	Identification of whether an event was blocked by an endpoint agent, firewall, or another prevention technology		
<b>EDR.REQ.049</b>	Investigation Requirements	Automated stitching of endpoint, network, cloud and identity data, including security alerts & events		
<b>EDR.REQ.050</b>	Investigation Requirements	Noise cancellation; removal of non-		



S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
		significant binaries and DLLs from chain		
<b>EDR.REQ.051</b>	Investigation Requirements	SOC analyst context of TTPs to utilize knowledge gained to help in future investigations		
<b>EDR.REQ.052</b>	Incident Management Requirements	Automated grouping of related alerts from various sources into a single incident		
<b>EDR.REQ.053</b>	Incident Management Requirements	Intuitive incident view with an incident overview and MITRE tactics and key incident information.		
<b>EDR.REQ.054</b>	Incident Management Requirements	Customizable incident scoring		
<b>EDR.REQ.055</b>	Incident Management Requirements	Listing of notable artifacts from alerts and their threat intelligence information		
<b>EDR.REQ.056</b>	Incident Management Requirements	Listing of user and hosts involved in incidents to quickly determine the scope of an incident		
<b>EDR.REQ.057</b>	Incident Management Requirements	Ability to assign incidents to team members		
<b>EDR.REQ.058</b>	Incident Management Requirements	Automated notifications on incident assignment		
<b>EDR.REQ.059</b>	Incident Management Requirements	End-to-end management of the incident lifecycle (new, investigation, closed, handled, etc.)		
<b>EDR.REQ.060</b>	Incident Management Requirements	Optional merging of incidents		
<b>EDR.REQ.061</b>	Incident Management Requirements	Ability to send incident data to third-party case management		
<b>EDR.REQ.062</b>	Threat Intelligence Requirements	Ability to alert on known malicious objects on endpoints with IOC rules		
<b>EDR.REQ.063</b>	Threat Intelligence Requirements	Ability to automatically scan historic data for IOCs as they are added to the system and raise alerts		
<b>EDR.REQ.064</b>	Threat Intelligence Requirements	Out-of-the box integration with one or more threat intelligence services for threat		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
		intelligence tags and additional context on key artifacts		
<b>EDR.REQ.065</b>	Threat Intelligence Requirements	Ingestion of threat intelligence feeds from third-party sources in JSON and CSV formats		
<b>EDR.REQ.066</b>	Threat Intelligence Requirements	IOC creation using APIs		
<b>EDR.REQ.067</b>	Threat Intelligence Requirements	IOC creation from the management console		
<b>EDR.REQ.068</b>	Threat Intelligence Requirements	Ability to import multiple IOCs using APIs		
<b>EDR.REQ.069</b>	Threat Intelligence Requirements	Ability to import multiple IOCs from a CSV file using the management console		
<b>EDR.REQ.070</b>	Threat Intelligence Requirements	Configurable severity level of an IOC		
<b>EDR.REQ.071</b>	Response Requirements:	Remote terminal capability		
<b>EDR.REQ.072</b>	Response Requirements:	Full CMD, PowerShell, and Python commands and scripts on Windows 7, 8, and 10		
<b>EDR.REQ.073</b>	Response Requirements:	Full Bash and Python commands on macOS and Linux		
<b>EDR.REQ.074</b>	Response Requirements:	Ability to execute custom Python scripts across multiple endpoints simultaneously on Windows, macOS, and Linux		
<b>EDR.REQ.075</b>	Response Requirements:	Pre-defined scripts to allow analysts of all experience levels to easily collect data and investigate and respond to threats		
<b>EDR.REQ.076</b>	Response Requirements:	Status window that displays script results, confirming whether scripts executed successfully		
<b>EDR.REQ.077</b>	Response Requirements:	Remote isolation of a single endpoint or multiple endpoints		
<b>EDR.REQ.078</b>	Response Requirements:	Remote file deletion of a single endpoint or multiple endpoints		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.079</b>	Response Requirements:	Automatic and manual collection or retrieval of quarantined files and objects		
<b>EDR.REQ.080</b>	Response Requirements:	Ability to view, suspend, or terminate running processes or download binaries with a graphical task manager for Windows, macOS, and Linux		
<b>EDR.REQ.081</b>	Response Requirements:	Graphical file manager with ability to view, download, rename, or move files for Windows, macOS, and Linux		
<b>EDR.REQ.082</b>	Response Requirements:	Remediation suggestions to restore hosts to their original state		
<b>EDR.REQ.083</b>	Response Requirements:	Search and destroy to swiftly sweep across endpoint and eradicate threats		
<b>EDR.REQ.084</b>	Response Requirements:	Integration with proposed firewalls to block access to malicious IP addresses or domains		
<b>EDR.REQ.085</b>	Response Requirements:	Integration with proposed security orchestration, automation, and response (SOAR) solution for incident analysis		
<b>EDR.REQ.086</b>	Response Requirements:	Integration with proposed security information and event management (SIEM) solutions		
<b>EDR.REQ.087</b>	Data Collection and Data Integration Requirements	Ability to ingest logs from virtually any data source, including network, endpoint, cloud, identity, application, HR, and any other data source for threat hunting, correlation and detection including below		
<b>EDR.REQ.088</b>	Data Collection and Data Integration Requirements	User, Device and Process information for analytics		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.089</b>	Data Collection and Data Integration Requirements	File information for file create, write, access, open, rename, or delete for analytics		
<b>EDR.REQ.090</b>	Data Collection and Data Integration Requirements	Network activity, including outgoing, incoming, and failed connections for analytics		
<b>EDR.REQ.091</b>	Data Collection and Data Integration Requirements	Registry activities, such as create, modify, delete and rename key for analytics		
<b>EDR.REQ.092</b>	Data Collection and Data Integration Requirements	System events and Security alerts for analytics		
<b>EDR.REQ.093</b>	Data Collection and Data Integration Requirements	Option should be provided to establish a secure connection for critical endpoints (without internet access) to route endpoints and collect and forward logs and files for analysis.		
<b>EDR.REQ.094</b>	Endpoint Agent System Support and Resource Requirements	Support for all recent Windows versions, including Windows Server		
<b>EDR.REQ.095</b>	Endpoint Agent System Support and Resource Requirements	Support for all recent macOS and Mac OS X versions		
<b>EDR.REQ.096</b>	Endpoint Agent System Support and Resource Requirements	Support for Android and Chrome OS, non-persistent VDI		
<b>EDR.REQ.097</b>	Endpoint Agent System Support and Resource Requirements	Support for all major Linux distributions		
<b>EDR.REQ.098</b>	Endpoint Agent System Support and Resource Requirements	Full auditing for all actions in the system		
<b>EDR.REQ.099</b>	Endpoint Agent System Support and Resource Requirements	Low CPU usage with all services enabled		
<b>EDR.REQ.100</b>	Endpoint Agent System Support and Resource Requirements	Agent installation size less than 50 MB		
<b>EDR.REQ.101</b>	Endpoint Agent System Support and Resource Requirements	Ability to push agent updates from the management console		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
<b>EDR.REQ.102</b>	Endpoint Agent System Support and Resource Requirements	It should support automated agent upgrades & Peer-to-peer agent updates		
<b>EDR.REQ.103</b>	Endpoint Agent System Support and Resource Requirements	Granular control of agent controls and notifications, including tray icon visibility, custom end user notifications, and the option to restrict response options such as remote terminal access		
<b>EDR.REQ.104</b>	Deployment, Management and Security	Scalable, cloud-based management and agent deployment		
<b>EDR.REQ.105</b>	Deployment, Management and Security	Single, web-based management console for endpoint security as well as extended detection and response		
<b>EDR.REQ.106</b>	Deployment, Management and Security	Role-based access control (RBAC) for granular permissions		
<b>EDR.REQ.107</b>	Deployment, Management and Security	Multi-factor authentication (MFA) for management		
<b>EDR.REQ.108</b>	Deployment, Management and Security	Customizable dashboard for high-level status of security and operational information		
<b>EDR.REQ.109</b>	Deployment, Management and Security	Kubernetes integration for deployment and management in a container environment		
<b>EDR.REQ.110</b>	Deployment, Management and Security	Optional on-premises broker service to aggregate and manage communications between endpoints and a cloud-based management console		
<b>EDR.REQ.111</b>	Deployment, Management and Security	Standards-based APIs to allow third-party management tools to integrate and perform administrative actions		
<b>EDR.REQ.112</b>	Deployment, Management and Security	Best practices to ensure the entire solution and its infrastructure are secure, including hardening, encryption for data at rest and data in motion, network security, physical		

S No.	Parameter	Minimum Technical Specifications	Compliance (Yes / No)	Reference (Document /Page no)
		security, and regular assessment tests		
<b>EDR.REQ.113</b>	Deployment, Management and Security	SOC 2 Type II Plus certification		
<b>EDR.REQ.114</b>	Deployment, Management and Security	ISO 27001 certification		
<b>EDR.REQ.115</b>	Deployment, Management and Security	EDR data lake should be within country.		
<b>EDR.REQ.116</b>	Deployment, Management and Security	Solution should have a proxy or bridge like architecture so that critical systems which doesn't have direct internet access can connect through the bridge/Proxy to connect to console.		
<b>EDR.REQ.117</b>	Data Retention and Coverage Requirements	Visibility into lateral movement across the network and other parts of the infrastructure		
<b>EDR.REQ.118</b>	Data Retention and Coverage Requirements	Detection and response for threats involving managed and unmanaged endpoints		
<b>EDR.REQ.119</b>	Data Retention and Coverage Requirements	Detection and response for threats involving remote users		
<b>EDR.REQ.120</b>	Data Retention and Coverage Requirements	Detection and response for threats involving cloud servers		
<b>EDR.REQ.121</b>	Data Retention and Coverage Requirements	Continuous collection and centralized storage of all security data for behavioural analytics		
<b>EDR.REQ.122</b>	Data Retention and Coverage Requirements	Total data retention of 180 days to be included		
<b>EDR.REQ.123</b>	Data Retention and Coverage Requirements	One year of retention for audit logs of administrative and investigative activity		
<b>EDR.REQ.124</b>	Licensing & Support	500 Endpoint detection & response licenses with 5 year subscription		
<b>EDR.REQ.125</b>	Licensing & Support	License for EDR log retention for 5 years		
<b>EDR.REQ.126</b>	Licensing & Support	5 Years support bundle with 24x7x365 days TAC support,		

## 17.26 "Technical Requirements Specifications - Anti DDoS Appliance"

Product Name: Anti DDoS Appliance

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DDoS.REQ.001</b>	General Specifications	The Anti-DDoS solution should be a standalone purpose built appliance based solution for DDoS Detection and Mitigation.		
<b>DDoS.REQ.002</b>	General Specifications	The Anti-DDoS solution should ensure high availability with fail-open/fail-close bypass Kit.		
<b>DDoS.REQ.004</b>	General Specifications	The required solution must not be End of Life or End of Support for at least 5 years from the due date of submission of bid by the bidder.		
<b>DDoS.REQ.005</b>	Key features	The required DDoS Appliances must be rack mountable and rack mount kit and other required accessories must be supplied along.		
<b>DDoS.REQ.006</b>	Key features	The solution and all the components thereof must have provision for redundant/dual power supply		
<b>DDoS.REQ.008</b>	Key features	The proposed solution should support DDoS flood prevention rate of minimum 1 million packets per Second.		
<b>DDoS.REQ.009</b>	Key features	The solution should have SSL attack detection and mitigation capability for minimum 40000 SSL TPS with 2048 bit Keys.		
<b>DDoS.REQ.010</b>	Key features	Appliance should have at least 4 nos. of 1 GbE/SFP+ and 8 X 10G SFP+ Ports(fully populated)		
<b>DDoS.REQ.011</b>	Key features	Appliance Should have a dedicated out-of-band Ethernet management port.		
<b>DDoS.REQ.012</b>	Key features	Appliance should support minimum total 10 million concurrent sessions and scalable up to 20 million		
<b>DDoS.REQ.013</b>	Key features	Solution should detect and mitigate attacks at Layer 3 to Layer 7		
<b>DDoS.REQ.014</b>	Key features	The solution must be able to protect following UDP, TCP, DNS, HTTP, SSL and other network attack targets while delivering uninterrupted service for legitimate connections		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DDoS.REQ.015</b>	Key features	Should protect ICMP attack		
<b>DDoS.REQ.016</b>	Key features	Should protect DNS based attacks: DNS Cache Poisoning Defense, DNS Length Check Defense, DNS NXDomain Defense, DNS Query Flood Defense, DNS Reply Flood Defense, DNS TTL Check, DNS Source Authentication		
<b>DDoS.REQ.017</b>	Key features	The solution must be able to protect following TCP based - SYN, SYN-ACK, ACK and PUSH-ACK Flood, RST or FIN Flood, Fragmented ACK, Redirect Traffic Attack and Invalid TCP flags		
<b>DDoS.REQ.018</b>	Key features	The system must be regularly updated with new attack signatures that are maintained by the OEM's research team		
<b>DDoS.REQ.019</b>	Key features	DDoS Protection from active DDoS complainants based IP reputation, blacklisted hosts, country, domain		
<b>DDoS.REQ.020</b>	Key features	System must be able to detect, and block HTTP GET Flood and should support following mechanism to avoid False Positive prevention (or equivalent): a) TCP Authentication b) HTTP or JavaScript redirect		
<b>DDoS.REQ.021</b>	Key features	The solution must support to be deployable in inline mode		
<b>DDoS.REQ.022</b>	Key features	The solution should have the capability to be configured in detect as well as protect mode		
<b>DDoS.REQ.023</b>	Key features	Solution should support user customizable/ user definable signature/counter measures		
<b>DDoS.REQ.024</b>	Key features	The system must have connection limit option for new connection based on a) Source Basis. b) Destination Basis In IP wise or in range or equivalent		
<b>DDoS.REQ.025</b>	Key features	System should have Behavioural DoS approach/ Challenge response/countermeasure-based approach for immediate mitigation of flood attacks—protecting against zero-day DoS and DDoS attacks without manual intervention.		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DDoS.REQ.026</b>	Key features	The system must provide the ability to block bot-originated traffic according to system-supplied signatures and proposed solution should have the capability to challenge only the suspected attacker, legitimate user should not be challenged.		
<b>DDoS.REQ.027</b>	Key features	System must support concept of users / groups / roles and role-based access permission		
<b>DDoS.REQ.028</b>	Key features	The solution should provide historical dashboards or reports for at least 2 months. Dashboard should display real- time protection statistics on dropped and passed traffic in packets, with rate statistics in bps and pps.		
<b>DDoS.REQ.029</b>	Key features	Device should integrate seamlessly with SIEM solution.		
<b>DDoS.REQ.030</b>	Key features	The solution must support the generation of e-mail reports with the detailed statistics and graphs for any user defined entity from the solution		
<b>DDoS.REQ.031</b>	Key features	The system should support IPv4 and IPv6 dual-stack without deteriorating performance		
<b>DDoS.REQ.032</b>	Key features	The solution shall be able to support user authentication based on Local Password, RADIUS & TACACS+		
<b>DDoS.REQ.033</b>	Key features	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP		

**B. Non-IT Components****17.27 "Technical Requirements Specifications - UPS 300 KVA"**

Product Name: UPS 300 KVA

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
UPS300.REQ.001	Capacity	Adequate capacity to cover all IT equipment's like servers, important network and storage equipment, access control, Fire Detection and Suppression system, Surveillance system etc. UPS shall be of minimum 300KVa and upgradable to 400KVA		
UPS300.REQ.002	Technology	True ONLINE		
UPS300.REQ.003	Connector	SNMP Connectivity		
UPS300.REQ.004	Electrical Input	Single Phase, 230 V AC or better with an option to select three phase		
UPS300.REQ.005	Electrical Input	Voltage Range 155 – 280 V on Full Load or better		
UPS300.REQ.006	General Requirements	Voltage Range 110 – 280 V on less than 70% Load or better		
UPS300.REQ.007	Electrical Input	Frequency Range 45 – 55 Hz or better		
UPS300.REQ.008	Electrical Input	AC to AC efficiency of 85% or higher		
UPS300.REQ.009	Electrical Output	230V AC or higher		
UPS300.REQ.010	Electrical Output	Frequency: 50 Hz or better		
UPS300.REQ.011	Electrical Output	Overload Capacity: 110% for 5 to 10 mins or better .		
UPS300.REQ.012	Electrical Output	Pure sine wave output or equivalent		
UPS300.REQ.013	Protection	Electronic overload sensing and circuit breaker		
UPS300.REQ.014	Protection	Overheating, short-circuit, low battery, input over/under voltage.		
UPS300.REQ.015	Battery Type	Sealed maintenance-free Lithium ion battery only with necessary indicators, alarms, and protection, including battery storage.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
UPS300.REQ.016	Backup Time	Battery to be supplied to cater minimum 2 hours backup at rated load		
UPS300.REQ.017	DC Voltage	Minimum 240V.		
UPS300.REQ.018	Charging Features	1. Low battery protection to avoid deep discharging of batteries.		
UPS300.REQ.019	Charging Features	2. Self test diagnostic or equivalent feature		
UPS300.REQ.020	Other Features	UPS Bypass Automatic on Overload or UPS Failure		
UPS300.REQ.021	Other Features	Monitoring panel with LCD display to provide following information:-		
UPS300.REQ.022	Other Features	1. Input/output voltage		
UPS300.REQ.023	Other Features	2. Input/output frequency		
UPS300.REQ.024	Other Features	3. Load current		
UPS300.REQ.025	Other Features	4. Charging current		
UPS300.REQ.026	Other Features	LED display for:- UPS on, battery operation, bypass, alarm, battery charge level, etc.		
UPS300.REQ.027	Other Features	Alarms for :- Mains failure, low battery, overload etc.		
UPS300.REQ.028	Other Features	RS 232 Standard Interface or advanced protocol with equivalent port in conjunction with UPS		
UPS300.REQ.029	Other Features	monitoring software should provide information about UPS health, status, battery backup etc.		
UPS300.REQ.030	Environmental	Temperature 0 to + 55 deg C		
UPS300.REQ.031	Environmental	Humidity 0 – 95% RH non-condensing		
UPS300.REQ.032	Environmental	Audible noise < 50 dB (A) or better		
UPS300.REQ.033	Mandatory Compliance	Safety certified to IEC standards or as per applicable in Indian law		
UPS300.REQ.034	Mandatory Compliance	EMC certified to IEC standards.		
UPS300.REQ.035	Mandatory Compliance	ISO 9001:2000 certified		

## 17.28 "Technical Requirements Specifications - UPS 20 KVA"

Product Name: UPS 20KVA

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
UPS20.REQ.001	Technology	IGBT BASED DSP CONTROLLED		
UPS20.REQ.002	Rating	20 KVA/16 KW		
UPS20.REQ.003	Electrical Input	3 phase input and 3 phase output online UPS		
UPS20.REQ.004	Electrical Input	Input Voltage : 230 V or better		
UPS20.REQ.005	Electrical Input	Input Frequency : 50 HZ+/- 10% or equivalent		
UPS20.REQ.006	Electrical Input	Isolation Transformer: Inbuilt Isolation Transformer with 1:1 ratio at UPS Input to be provided at output		
UPS20.REQ.007	Electrical Output	Output Voltage: 230 V (adjustable to 220/230/240±10% or equivalent)		
UPS20.REQ.008	Electrical Output	Output Frequency: 50Hz+/- 10%		
UPS20.REQ.009	Electrical Output	Output Power Factor: 0.8		
UPS20.REQ.010	Other features	Crest Factor: up to 3:1 or better		
UPS20.REQ.011	Other features	Wave form: Pure sine wave or better		
UPS20.REQ.012	Connector	SNMP Connectivity		
UPS20.REQ.013	Battery Bank / Charger/ Rack	Backup Capacity - Battery should be provided with 120 min backup on Full load		
UPS20.REQ.014	Battery Bank / Charger/ Rack	cable with proper rating for interlink cables and battery input and necessary accessories.		
UPS20.REQ.015	Protection	Breakers, should provide Full Protection		
UPS20.REQ.016	Alarms	Audio Alarm, Mains Fail, Battery Low Pre-alarm,		
UPS20.REQ.017	Alarms	Graphical LCD display for Input & Output - Voltage		
UPS20.REQ.018	Alarms	Termination: Input, Battery, Output & Bypass		
UPS20.REQ.019	Working Condition	Operating Temp: 0 to 40 Deg C or better		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>UPS20.REQ.020</b>	Working Condition	Humidity: Upto 95%		
<b>UPS20.REQ.021</b>	Working Condition	Noise: < 55 dB or better		
<b>UPS20.REQ.022</b>	certifications	CE Certification:IEC/EN		

## 17.29 "Technical Requirements Specifications – AC”

Product Name: AC

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>AC.REQ.001</b>	AC Unit with wired remote & anti corrosion finish stand for outdoor unit. The AC units will be 3 Star rated for energy efficiency.		
<b>AC.REQ.002</b>	• 2 TR * 2 units Cassette AC in NOC Room.		
<b>AC.REQ.003</b>	• 1.5 TR * 3 Units (Split AC) for BMS Room, Staging Room & Conference Room		
<b>AC.REQ.004</b>	Copper refrigerant piping of required size with insulation making opening / cut-outs in partitions, brick walls as required complete.		
<b>AC.REQ.005</b>	Electrical Cabling for 2TR split unit indoor to outdoor making opening / cut-outs in brick walls, partitions as required complete.		
<b>AC.REQ.006</b>	Sequential Time controller for 2TR AC unit		
<b>AC.REQ.007</b>	Copper refrigerant piping with insulation making opening / cut-outs in brick masonry walls, partitions for 2 TR Split units		
<b>AC.REQ.008</b>	Electrical Cabling for 2 TR split unit indoor to outdoor making opening / cut-outs in brick masonry walls, partitions		
<b>AC.REQ.009</b>	Drain piping for all AC units making opening / cut-outs in brick masonry walls, partitions		

## 17.30 "Technical Requirements Specifications - Biometric card"

Product Name: Biometric card

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SC.REQ.001</b>	Card Type	Microprocessor based single chip contact less card with		
<b>SC.REQ.002</b>	Card Type	64Kbytes of available EEPROM		
<b>SC.REQ.003</b>	Compliance to	ISO 14443-1,2,3 A or B and SCOSTA – CL or (latest) platform		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SC.REQ.004</b>	Power	3 Volt or 5 Volt		
<b>SC.REQ.005</b>	Protocol	T = CL (Contact less)		
<b>SC.REQ.006</b>	Transmission Rate	100k Baud data transmission rate		
<b>SC.REQ.007</b>	Distance Range	10 cm operating distance range in case of Contact Less data		
<b>SC.REQ.008</b>	Distance Range	transfer as per ISO 14443 standard for Read/Write.		
<b>SC.REQ.009</b>	Retention Period	Minimum 5 years		
<b>SC.REQ.010</b>	Write Cycle	3,00,000		
<b>SC.REQ.011</b>	Chip Temperature	-4°C to +50°C		
<b>SC.REQ.012</b>	Operating Temperature	-4°C to +50°C		
<b>SC.REQ.013</b>	Construction	PVC or better		

### 17.31 "Technical Requirements Specifications - Biometric Controller and accessories"

Product Name: Biometric Controller

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>Smart Reader cum Controller</b>				
<b>SC.REQ.014</b>	Type	Capable of reading contactless smart card (ISO 14443 1/2/3/4 A and B). 64 Kbytes storage on smart card		
<b>SC.REQ.015</b>	Read Range	Up to 20 Cm (Maximum)		
<b>SC.REQ.016</b>	Memory	Hot List and Blacklist data		
<b>SC.REQ.017</b>	Memory	• Minimum 1000 and expandable up to 25000		
<b>SC.REQ.018</b>	Memory	• Entry / Exit data		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
SC.REQ.019	Memory	<ul style="list-style-type: none"> <li>Minimum 1000 and expandable up to 50,000</li> </ul>		
SC.REQ.020	Memory	Chip Serial No. (CSN) shall be used for hot listing & blacklisting. Entry/Exit data indicate Date & Time of Entry/Exit (Time stamp) corresponding to the card holder accessing the gate. Communication between Reader & Server shall be through SSL		
SC.REQ.021	RTC	Built in most accurate RTC (Real Time Clock) with Lithium Cell Backup		
SC.REQ.022	Communication	Ethernet (TCP/IP)		
SC.REQ.023	Outputs	Relay output		
SC.REQ.024	Cryptography	3DES/AES (with 128 bit encryption)/RSA Multiple Application Platforms should be supported by the Controller so as to avoid 'Proprietary Scenarios' . Application should support standard OS platforms such as Windows or UNIX or Linux etc		
<b>Biometric Reader</b>				
SC.REQ.025	Scanner Type	Optical		
SC.REQ.026	Sensing Area	As per ISO 19794-2		
SC.REQ.027	Setting Level	30 as defined in <a href="http://www.egovstandards.gov.in">www.egovstandards.gov.in</a> for fingerprints		
SC.REQ.028	Extractor & Minutia	for fingerprint Image Template. The algorithm used for Minutiae extraction must be Minax compliant/ Listed		
SC.REQ.029	Response Time	Less than 2 seconds for single transaction		
SC.REQ.030	Operating Temperature	0 to 45 degree Centigrade		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
SC.REQ.032	Storage Temperature	0 to 50 degree Centigrade		
SC.REQ.033	Humidity	10 to 90%		
SC.REQ.034	Reaction time	< 1.5 sec in 1:1 mode		
SC.REQ.035	Operating system	Application should support standard OS platforms such as Windows or UNIX or Linux etc		
SC.REQ.036	Keypad Reader type	Alphanumeric keys or touch screen		
SC.REQ.037	Screen Size	4x3 Inches Minimum		
SC.REQ.038	Display Type	LCD or equivalent		
SC.REQ.039	Network Controller	One controller can control a maximum of 4 card readers or and should Control 4 door locks.		
SC.REQ.041	Network Controller	Access decisions shall be made at each door controller, without reference to any other		
SC.REQ.042	Network Controller	control or monitoring equipment		
SC.REQ.043	Network Controller	The Access Controller shall continue to operate in the event of mains failure for not less than 4 hours.		
SC.REQ.044	Network Controller			
SC.REQ.045	Network Controller	Facility to open all the doors in case of fire is required.		
SC.REQ.039	Network Controller	One controller can control a maximum of 4 card readers or and should Control 4 door locks.		
SC.REQ.041	Network Controller	Access decisions shall be made at each door controller, without reference to any other		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SC.REQ.042</b>	Network Controller	control or monitoring equipment		
<b>SC.REQ.043</b>	Network Controller	The Access Controller shall continue to operate in the event of mains failure for not less than 4 hours.		
<b>SC.REQ.044</b>	Network Controller			
<b>SC.REQ.045</b>	Network Controller	Facility to open all the doors in case of fire is required.		

### 17.32 "Technical Requirements Specifications -Smart TV"

Product Name: Smart TV

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>STV.REQ.001</b>	Scope	The scope includes the supply, installation, testing & commissioning. The scope also includes LED TV system supply, installation work with all required accessories and other activities at site that are not specifically mentioned in the specifications but are required for successful commissioning of the project.		
<b>STV.REQ.002</b>	55" LED TV specifications	The product should match with below minimum criteria:		
<b>STV.REQ.003</b>	55" LED TV specifications	55" 4K Professional LED Display with Wall Mount, Incredible 4K picture quality, Resolution: 4K Ultra HD (3840x2160p)		
<b>STV.REQ.004</b>	55" LED TV specifications	Processor 4K, Built in Speaker (10W + 10W), Brightness control, Contrast Ratio 4000:1, Viewing Angle(H/V) 178/178, HDMI 2.0 (1), DVI, USB, Display, Display port connectivity, RJ45 external control		
<b>STV.REQ.005</b>	Accessories	HDMI cable, RJ 45 cable, power cable, LED mounting stand with installation accessories need to be consider by the bidder		
<b>STV.REQ.006</b>	Standards	It should be complied with electromagnetic compatibility (EMC) class B compliant for safety and reliability standards for operation.		
<b>STV.REQ.007</b>	75" LED TV specifications	The product should match with below minimum criteria:		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>STV.REQ.008</b>	75" LED TV specifications	75" 4K Professional LED Display with Wall Mount, Incredible 4K picture quality, Resolution: 4K Ultra HD (3840x2160p)		
<b>STV.REQ.009</b>	75" LED TV specifications	Processor 4K, Built in Speaker (10W + 10W), Brightness control, Contrast Ratio 4000:1, Viewing Angle(H/V) 178/178, HDMI 2.0 (1), DVI, USB, Display, Display port connectivity, RJ45 external control		
<b>STV.REQ.010</b>	Accessories	HDMI cable, RJ 45 cable, power cable, LED mounting stand with installation accessories need to be consider by the bidder		
<b>STV.REQ.011</b>	Standards	It should be complied with electromagnetic compatibility (EMC) class B compliant for safety and reliability standards for operation.		

### 17.33 "Technical Requirements Specifications -DCIM"

Product Name: DCIM

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DCIM.REQ.001</b>	Scope	The scope includes the supply, installation, testing & commissioning. The scope also includes DCIM software monitoring system installation work with all required accessories, hardware and other activities that are not specifically mentioned in the specifications but are required for successful commissioning of the project. The Bidder should supply and implement proposed DCIM solution including hardware/Virtual server, DCIM application/OS, DCIM DB, DCIM software licenses for successful installation of DCIM application.		
<b>DCIM.REQ.002</b>	General	The DCIM must be able to provides insights and drives performance throughout the Data Centre, including Data Centre assets and physical infrastructure. The management system		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		enables the monitoring and collection of low-level infrastructure data to enable intelligent analysis by individuals with domain expertise, as well as a holistic analysis of the overall infrastructure. The management system enables the integration of information technology (IT) and facility management to centralize monitoring and management of a Data Centre's critical devices. maintain, load management, space management, inventory, future projection and asset management within the Data Centre and provide visualization of the assets in floor layout, rack elevation, and individual asset views.		
<b>DCIM.REQ.003</b>	General	The DCIM system should be able to display energy efficiency information such as PUE, DCiE and trend them in real time on daily, monthly and yearly basis.		
<b>DCIM.REQ.004</b>	General	This specification describes the operation and functionality of a Data Centre Infrastructure Management system hereafter referred to as the management system. The management system is installed on a physical server or as a virtual appliance. The DCIM system should be able to create reports in at least .CSV formats.		
<b>DCIM.REQ.005</b>	General	The Proposed DCIM platform should also be capable of pushing		
<b>DCIM.REQ.006</b>	General	monitored device information using SNMP trap or restful API to any third-Party NMS system		
<b>DCIM.REQ.007</b>	General	By this the DCIM system should ensure it integrates back to commonly needed Infrastructure devices like in row cooling, CRAC,		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		Diesel Generators, Energy Meters, Branch Circuit Power meters, Rack mount Intelligent PDU and Rack Environmental Monitoring systems. To ensure a clear integration to the said devices is done as for Device connectivity is attached, please ensure that proposed DCIM covers licensing and integration requirements of all SNMP, Modbus, backnet and IP devices		
<b>DCIM.REQ.008</b>	General	The installed system shall be able to use web services to products and systems.		
<b>DCIM.REQ.009</b>	General	The DCIM shall be a web client architecture (web-based system that is accessed through a standard web browsing tool such as Internet Explorer, Chrome, or Firefox).		
<b>DCIM.REQ.010</b>	General	DCIM server / VM system should allow integration of client email server via SMTP channel as well as it should support integration to SMS Gateway servers by utilizing the HTTP post Method.		
<b>DCIM.REQ.011</b>	General	The DCIM must keep a log of all changes within the Data Centre including the changes made to the DCIM system and all IMAC workflow information.		
<b>DCIM.REQ.012</b>	General	All the features and functionalities or DCIM services mentioned		
<b>DCIM.REQ.013</b>	General	in this tender scope should be expandable to manage future requirement as well and provide us a simplified and unified view of all the DCs on future need basis.		
<b>DCIM.REQ.014</b>	General	Proposed DCIM system for present requirement should be modular in licensing Nature and provide us flexibility to purchase and expand enhanced modules according to our future need.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DCIM.REQ.015</b>	General	The DCIM should be able to run on a physical or virtualized server.		
<b>DCIM.REQ.016</b>	General	The DCIM software licensing should be Perpetual in NATure which means that license once bought for various polled devices/racks etc. never expire. However, the end client is free to buy		
<b>DCIM.REQ.017</b>	General	extension of software warranties on yearly basis to keep up to date with new releases as and when they are launched.		
<b>DCIM.REQ.018</b>	Visualization	A. It should provide diverse layout components to design the		
<b>DCIM.REQ.019</b>	Visualization	floor plans in a single project for both of the web and Windows application interfaces.		
<b>DCIM.REQ.020</b>	Visualization	B. It should be with the windows application interface which can help to switch to the full screen mode to let the layout plans fit		
<b>DCIM.REQ.021</b>	Visualization	in the different screen resolution automatically.		
<b>DCIM.REQ.022</b>	Visualization	C. The layout components include static/dynamic/boundary type of text, line, oval, rectangle, progress bar, linear/analogy		
<b>DCIM.REQ.023</b>	Visualization	meters, buttons, physical object, camera live streaming, history trend, pie chart, billboard, and other Data Centre components. The DCIM project designer needs not to write any program code		
<b>DCIM.REQ.024</b>	Visualization	to collect the data, design the plans and configure the system.		
<b>DCIM.REQ.025</b>	Visualization	D. The management system should be able to add devices to the Data Centre floor plan to represent the actual physical location		
<b>DCIM.REQ.026</b>	Visualization	in the Data Centre.		
<b>DCIM.REQ.027</b>	Visualization	E. The layout plans should be able to organize to		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		different layout groups for different login accounts. That means only the account with the privilege can see the plans in the layout groups.		
<b>DCIM.REQ.028</b>	Visualization	F. The layout plans can show where the physical devices are installed and identify where the problem is from the location and device.		
<b>DCIM.REQ.029</b>	Visualization	G. Users can look up more than 1 received data and show the history trend from the DCIM server. The searched history trend can be exported to as a .csv file or copy to the system clipboard.		
<b>DCIM.REQ.030</b>	Event Management	<p>A. The system provides a summary alarm toolbox for the users to understand the on-going event number and the level. Click on the tool box to pop up the monitoring device list to show all of the equipment operation status.</p> <p>B. The system also provides the event log query to search for the history event log.</p> <p>C. The history event log includes the device monitoring event, system operation event and the operators configure and control event.</p> <p>D. Event acknowledge: The system provides the event acknowledge button for the operator to acknowledge the on- going event. After the event is acknowledged then the system will not send any notification, but the layout plan still keeps the alarm until this event is complete recovered.</p> <p>E. Event escalation: Once the event is not recovered in a specified period of time then the system will escalate this event to</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		another assigned event level. The system will start to notify based on the new event level rule.		
<b>DCIM.REQ.031</b>	Protocol Management	<p>A. The management system can add, edit and remove Modbus, SNMP, OPC protocols to communicate with the devices.</p> <p>B. The implemented protocols can export to and be imported from files.</p> <p>C. All of the received data can be assigned to a transform formula to produce another value for the other application. And each received data can set more than 32 thresholds to trigger the notification event.</p> <p>D. The system protocol can be created off line or online for the DCIM engineer to well prepare in the office. And provide the design concept and simulate before the system install.</p>		
<b>DCIM.REQ.032</b>	Camera Management	<p>A. The management system can add, edit and remove an IP camera device.</p> <p>B. The management system enables you to watch the camera video in the layout plans directly without opening external applications.</p> <p>C. The management system can configure a trigger rule to record not only 1 camera video but also presents 3 types for recording: Full time, scheduling and event trigger. The event- triggered video files are integrated in the event log for you to play the video file at your fingertips.</p> <p>D. The trigger rule can combine any event in the management system.</p> <p>E. Provide the multiple video recorder's live show for you to trace the moving object between different cameras.</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		F. The management system is able to control the camera actions by pan, tile and zoom through the network.		
<b>DCIM.REQ.033</b>	User Management	A. The management system can add, edit and remove user accounts. B. The users can be assigned to any user group. C. The user or user group can be assigned to a privilege level. D. The login user can modify his own password. E. The system can logout the user automatically when the user idle for a period of time.		
<b>DCIM.REQ.034</b>	Privilege Management	A. The management system can add, edit and remove a privilege level. B. The management system can set unlimited number of privilege levels, and each privilege level includes the functions read/write permission, available layout groups and devices controlling.		
<b>DCIM.REQ.035</b>	Organization Management	A. An organization can be a department, a customer or a building. The organizational tree can be customized to reflect the actual enterprise structure. B. Each organization can assign its own team members, monitoring devices, asset and power meters and electricity tariff formula. Those configuration can only be modified by the team members. C. The roles of the team member are Designer, manager, device manager and general user.		
<b>DCIM.REQ.036</b>	Notification Management	A. The management system is able to notify the users through e-mail, SMS and audio. B. The non-notify time can be configured to not send notification in a specified period of time. C. The system can		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>configure up to 16 event levels with different title, color and icon.</p> <p>D. The system can define unlimited event tag, which associates with the notification method and whom should be notified.</p> <p>E. The first delay time and repeat interval time can be assigned for each notification method.</p> <p>F. The user can acknowledge the event to stop sending the notify message.</p> <p>G. The system can plan to report its own operating status to the administrator on daily basis.</p>		
<b>DCIM.REQ.037</b>	Scheduling Management	<p>A. The management system can assign holidays in the scheduling calendar.</p> <p>B. The scheduling action can be added, edited and deleted.</p> <p>C. The scheduling can be assigned by daily, per-N days, specific date, weekly and monthly.</p> <p>D. The scheduling action can send a control command through the protocol or popping out a message in the user interface.</p>		
<b>DCIM.REQ.038</b>	Reaction Management	<p>A. The management system can add, edit and remove a reaction rule.</p> <p>B. The reaction rule can be defined to check more than 1 condition and then base on the result to initiate not only 1 action.</p> <p>C. The condition check can be combined with logical and/or.</p>		
<b>DCIM.REQ.039</b>	Report Management	<p>A. The management system can add, edit and remove a report template.</p> <p>B. The report template can combine event log with history log value in one report file.</p> <p>C. The report template can integrate the date/time, text,</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>image, list and graphical chart into one template file.</p> <p>D. The management system can add, edit and delete scheduling report task.</p> <p>E. The scheduling report can be generated by daily, weekly, monthly, quarterly and annually.</p> <p>F. The type of file can be generated as .txt, .csv and .xls.</p> <p>G. The report template can be generated manually.</p>		
<b>DCIM.REQ.040</b>	PUE Energy Module	<p>The management system provides the following functionality from the point of view of Data Centre Energy Efficiency:</p> <p>A. The management system provides current and historical Power Usage Effectiveness (PUE) values and full insight into current and historical energy efficiency.</p> <p>B. The management system can design a dashboard view to display the PUE value on the layout plan.</p> <p>C. The PUE dashboard shows the current, this hour, today, month to date and year to date PUE value.</p> <p>D. It presents how much power is devoted to driving the installed IT-equipment compared with the total facility consumption.</p> <p>E. Provide insight into cost of energy at the subsystem level.</p> <p>F. The management system will have a dashboard view which includes efficiency data on current and historical PUE, as well as detailed subsystem cost analysis.</p>		
<b>DCIM.REQ.041</b>	Asset Module:	<p>The asset functional module is designed for the Data Centre application, which provides the device classification and looks for information about power, cooling, network, server, etc. Based on the asset</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		information, it can generate the power path and network topology map automatically. Furthermore, the rack detail view and 3D navigation feature which can automatically be built up based on the real environment provide a more comprehensive view of assets inside a rack:		
<b>DCIM.REQ.042</b>	Asset Module:	<p>A. The management system can add, edit and delete asset device. The asset information can be exported to and imported from a file.</p> <p>B. The management system can add, edit and delete device model information. The model information can be exported to and imported from a file.</p> <p>C. Users can classify or search the asset device by device type, asset ID, installation date, location, department, owner, dealer, etc. The result can be copied to the clipboard or saved as a file.</p> <p>D. The related asset document can be reserved in the system, such as specification, manual, purchase order and OI.</p>		
<b>DCIM.REQ.043</b>	Asset Module:	<p>E. The management system can analyze the device relationship in power and network connections.</p> <p>F. The management system has the ability to print the asset QR code and leverage the asset inspection functional module to manage the critical assets.</p> <p>G. The power path analysis function can trace back from the leaf device to list all of the power supply and power conversion nodes. This function can also list the impacted devices from one power supply or conversion device down to the related power</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		usage device. H. The network path analysis function displays the relationship among the network, patch panel and the terminal device. I. 3D navigation system can automatically generate a 3D view based on the real location of each device in a room. Users can rotate, pan, zoom in and zoom out the camera to navigate the room.		
<b>DCIM.REQ.044</b>	Asset Module:	J. Rack management: a. The rack can be grouped as a row, island and room. b. It can display images of the rack IT devices (e.g., server, switching hub) and power devices (e.g., PDU). c. User can easily configure the IT devices by dragging and dropping the asset component to the U position in a rack. d. The rack component can display the relative color based on the assigned temperature or humidity sensor.		
<b>DCIM.REQ.045</b>	Slide Show Module:	The management system provides the methodology to cooperate with the monitor screen, projector and video wall to project the designed layout plans to the assigned screens automatically: A. It provides transparency to Data Centre key performance indicators and business metrics, which displays customizable information for a high-level overview of Data Centre operations.  B. It can operate without user intervention. The slide show module starts up automatically when the system boots up and projects the layout plans alterNATively. C. It has the ability to run the slide show module in different PCs and project		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		the different layout plans for different management purposes.		
<b>DCIM.REQ.046</b>	Architecture	The Proposed DCIM should be created in separate installations to maintain sanctity of data as follows:		
<b>DCIM.REQ.047</b>		a. Gateway/Convertor Devices: Required for connecting to third party BMS/ third part etc.		
<b>DCIM.REQ.048</b>		b. Monitoring layer: Responsible for polling all Monitoring Points		
<b>DCIM.REQ.049</b>		c. Infra Mgmt. Layer: Responsible for Analytics and Insightful data analysis of DCIM data points.		
<b>DCIM.REQ.050</b>		d. Cooling optimization AI Layer for Control of Perimeter coolers		
<b>DCIM.REQ.051</b>	VLAN	For all Data Centre Infrastructure components including all Field level devices, Third Party BMS/BMS controllers, Rack Mount PDU, Energy meters, VESDA, Panel Meters etc. the Subnet should be the same so that all the devices are able to ping each other and are easily discovered. If possible, they should be in the same VLAN along with complete DCIM solution.		
<b>DCIM.REQ.052</b>	Gateway/Convert or	The Gateway/Convertor so proposed to integrate third party BMS/BMS controllers and Field devices over Modbus /Modbus TCP, BACNET/BACNET-IP and Lon.		
<b>DCIM.REQ.053</b>	Hardware Specification	The Gateway/Convertor should employ a modular I/O design to allow expansion of the unit to incorporate more Field devices if so, required in future for AI /AO /DI /DO. This input and output capacity is to be provided through plug-in modules of various types.		
<b>DCIM.REQ.054</b>	Hardware Specification	DCIM solution shall have an inherent multi-protocol conversion gateway or DCIM vendor should		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		provision for a similar hardware/software-based gateway as may be required as per client site requirements. To ensure no last-minute surprises and no cross-vendor device communication issues on site the gateway should be manufactured by same OEM whose DCIM is being proposed in this tender and integrated back to DCIM. The gateway so proposed should allow to run all protocols through it at the same time (through that one device the system should allow integration to a chain of LON devices, chain of Modbus Device and also a chain of BACNET devices at the same time).		
<b>DCIM.REQ.055</b>	Hardware Specification	The gateway so proposed has to be DIN Rail mounted device and not a Rack mountable design. The field level devices will terminate in panels not inside Racks inside the Data Centre hence the device has to be mounted inside wall mounted panel.		
<b>DCIM.REQ.056</b>	Hardware Specification	The Gateway shall support simultaneous exchanges on its various protocols, essentially meaning you can use all protocols at once and it should be able to run BACNET, LON and Modbus at the same time and also provide capability to convert BACNET to Modbus TCP which may be required for seamless Building side integrations.		
<b>DCIM.REQ.057</b>	Hardware Specification	Every hardware input and output point, hosted within the Gateway and attached I/O modules, shall be trended automatically without the requirement for manual creation, and each of these logs shall log values based upon a change-of-value and		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		store at least 500 trend samples before replacing the oldest sample with new data. The operating system of the NSC/AS, application programs, and all other portions of the configuration database, shall be stored in non-volatile, FLASH memory. AS/NSC shall contain enough memory for the current application, plus required history logging, plus a minimum of 20% additional free memory.		
<b>DCIM.REQ.058</b>	Hardware Specification	This Gateway will support both script text-based programming language as well as the graphical function block programming language. For both languages, the programmer will be able to configure application software for custom program development and write global control programs.		
<b>DCIM.REQ.059</b>	Hardware Specification	The Gateway so proposed should not have IPMI functionalities or IT Server access functionalities on the same box as that again contradicts the whole idea of having Field devices managed at Panel Level. Gateway so provided has to be dedicated for Field devices only.		
<b>DCIM.REQ.060</b>	Hardware Specification	The Gateway so provided has to be compliant with ASHRAE 135- 2004 and should be BTL-listed as a BACnet Building Controller (B- BC) at the least. The Gateway shall have a built in FTT-10 port to communicate to the TP/FT-10 Lon Works / SNMP / Mod-bus network.		
<b>DCIM.REQ.061</b>	Hardware Specification	The Gateway shall comply to Emission Norms: EN 61000-6-3; FCC Part 15, Sub-part B, Class B		
<b>DCIM.REQ.062</b>	Hardware Specification	The Gateway shall include a battery-backed, real-time clock, accurate to 10		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		seconds per day. The RTC shall provide the following: time of day, day, month, year, and day of week. Each Gateway will allow for its own UTC offset, depending upon the time zone. When the time zone is set, the Gateway will also store the appropriate times for daylight savings time.		
<b>DCIM.REQ.063</b>	Third Party system Integration	DCIM platform should also be capable of pushing monitored device information to any Third-Party NMS system using SNMP INFORM / REQUEST procedures and to third party BMS system using Modbus / SNMP / SNMP Trap TCP out channel and also support Web services programming interface.		
<b>DCIM.REQ.064</b>	Email Server Integration	DCIM Monitoring Layer server/VM system should allow integration of client email server via SMTP channel.		
<b>DCIM.REQ.065</b>	Alarm Status Tracking	DCIM Monitoring layer should have Alarm filters in the Monitoring dashboard. The solution provides alert compression and advanced alerting algorithms including deviation from normal and time over threshold to help reduce false positive alarms.		
<b>DCIM.REQ.066</b>	Trend Analysis	Should offer Graphical trending analysis for historical data pertaining to day, week, month, year and user defined durations.		
<b>DCIM.REQ.067</b>	Rule Creations for Threshold Alert	Proposed DCIM solution should allow for custom logics for creating Rules of Escalation and Email alerts for various devices based on alarm severity and priority.		
<b>DCIM.REQ.068</b>	Auto Timed Reporting	DCIM Monitoring Layer should allow for Auto Timed/Scheduled Report Emailing to selected audience on required key performance indicators.		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		These Reports should be mailed to relevant users as CSV format.		
<b>DCIM.REQ.069</b>	Low End UPS Monitoring	If in case client buys UPS from the DCIM OEM bidder which do not have SNMP cards but are managed through serial console cables connected directly to systems powered by the same UPS, the proposed DCIM shall allow integration of those devices as well. Any separate plugin so required shall be bought by client as and when required but DCIM should offer back integration to the same.		
<b>DCIM.REQ.070</b>	Virtual Machine Migration	DCIM should be scalable to offer plugins to allow safe shutdown for Virtual Machines and Virtual Machine Migration. The safe shutdown feature should support VMWARE and Microsoft HYPER- V formats. For sites where the UPS are also from the same OEM as the DCIM the functionality should be made available day one to the client. For sites where the UPS are not from the same OEM the functionality should be made available as and when client buys UPS from the same OEM for future integration. Non availability of such a capability will be considered as Non-Compliance as client reserves the right to opt for it or not (as per the availability and future scalability on UPS side)		
<b>DCIM.REQ.071</b>	Virtual Machine Migration	This Plugin for Safe shutdown of Virtualized Infrastructure should support the following UPS configurations for alerting: Single UPS, Redundant UPS and Parallel UPS.		
<b>DCIM.REQ.072</b>	Virtual Machine Migration	This Plugin for Safe shutdown of Virtualized Infrastructure should support Event logging -		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		Pinpoint the timing and sequence of events leading up to an incident with the event log.		
<b>DCIM.REQ.073</b>	Virtual Machine Migration	This Plugin for Safe shutdown of Virtualized Infrastructure should help prevent possible data corruption by performing graceful, unattended operating system shutdown in the event of an extended power outage or computer power problem.		
<b>DCIM.REQ.074</b>	Virtual Machine Migration	It should allow the operator to run command file - Run command file on network shutdown sequence as well as start-up sequence.		
<b>DCIM.REQ.075</b>	Virtual Machine Migration	It should facilitate Sequenced Server Shutdown - Sequences the shutdown of multiple servers powered by the same UPS to extend runtime for higher priority servers.		
<b>DCIM.REQ.076</b>	Converged management layer	<p>Converged Management Layer concept arise from the fact that irrespective of various underlying components like Power, Cooling, Network, U space all of them have to converge to a single unified system. This System should facilitate the complete Lifecycle approach for Data Centre involving:</p> <ul style="list-style-type: none"> <li>a. Analysis</li> <li>b. Design</li> <li>c. Implement</li> <li>d. Operate</li> <li>e. Evaluate</li> </ul> <p>DCIM Management Layer will have the capability to lay out in the Data Centre model accurately represents the real-world physical environment of the room. This includes any physical attributes of the room such as size, shape, doors, windows, aisles, containments, false floor creations, false ceiling creation and ability to duct</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		the Racks, Containments and CRAC units to False ceiling as per site requirements.		
<b>DCIM.REQ.077</b>	Converged management layer	DCIM Management Layer should have an ability to import an AutoCAD 2013/other software .dwg floor drawing and display the floor layout. Rooms can be created based on wall detection on the AutoCAD drawing. This is different from the usual SVG / Raster Imaging used and should not be mixed with that which has been provisioned for Monitoring Layer only.		
<b>DCIM.REQ.078</b>	Converged management layer	User will have the capability to toggle on/off for each Layer of AutoCAD/other software imported inside DCIM.		
<b>DCIM.REQ.079</b>	Converged management layer	DCIM Management Layer should offer back export of the Data Centre design created or modified within DCIM in CAD/other format.		
<b>DCIM.REQ.080</b>	Converged management layer	DCIM Management Layer should have a Combination of thick client and thin client version offering at least the following functionality:		
<b>DCIM.REQ.081</b>	Converged management layer	a. Web view should offer the capability to create User Access control for various views of the system.		
<b>DCIM.REQ.082</b>	Converged management layer	b. Thick client view (the downloadable client) should offer a more advance view of the complete Data Centre starting from birds eye view to reach component level view.		
<b>DCIM.REQ.083</b>	Converged management layer	The web client view of the DCIM should offer at least the following functionalities:		
<b>DCIM.REQ.084</b>	Converged management layer	a. Perform simple rack inventory edits.		
<b>DCIM.REQ.085</b>	Converged management layer	b. Perform quick search and view simultaneous rack front/rear view for the Data Centre.		
<b>DCIM.REQ.086</b>	Converged management layer	c. User Access Control and license management		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DCIM.REQ.087</b>	Converged management layer	d. User Experience customization like Logo and color themes.		
<b>DCIM.REQ.088</b>	Converged management layer	e. Customize the language of operation		
<b>DCIM.REQ.089</b>	Converged management layer	DCIM Management Layer will be able to provide a product catalog that contains up-to-date floor and rack mounted Data Centre equipment having drag & drop functionality to populate devices & design DC floor layout within the system as per physical layout/actuals.		
<b>DCIM.REQ.090</b>	Converged management layer	DCIM Management Layer should offer inventory and mapping of Direct Current Powered devices like Fuses, Rectifiers along with AC powered. This means that user should be able to create a Power path with both types of sources at the same time if required.		
<b>DCIM.REQ.091</b>	Converged management layer	The DCIM tool will have the capability to render the floor layout in both 2D and 3D view.		
<b>DCIM.REQ.092</b>	Converged management layer	DCIM Management Layer should offer extensive Visual network management and representation of cable route from server to switch. It will show free and occupied ports on servers, switches, and patch panels. See a graphical overview of available network capacity.		
<b>DCIM.REQ.093</b>	Converged management layer	DCIM Management Layer should offer capability to create Cages on Data Centre floor and visualize the same in both variants:		
<b>DCIM.REQ.094</b>	Converged management layer	a. Glass cage		
<b>DCIM.REQ.095</b>	Converged management layer	b. Mesh Cage		
<b>DCIM.REQ.096</b>	Converged management layer	c. Solid wall		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DCIM.REQ.097</b>	Converged management layer	DCIM should offer complete information on the layout view for the following parameters:		
<b>DCIM.REQ.098</b>	Converged management layer	a. Empty Racks		
<b>DCIM.REQ.099</b>	Converged management layer	b. Filled Racks: stating the Racks are being used by a Process/Client		
<b>DCIM.REQ.100</b>	Converged management layer	c. Reserved: Racks reserved for a specific Process/Client		
<b>DCIM.REQ.101</b>	Converged management layer	d. Internal Use: Racks reserved for some Internal requirements		
<b>DCIM.REQ.102</b>	Converged management layer	With reference to Space Management in Data Centre, DCIM should offer following information on the layout view for the following parameters:		
<b>DCIM.REQ.103</b>	Converged management layer	a. Room Area		
<b>DCIM.REQ.104</b>	Converged management layer	b. Reserved Area: For specific Process/Client		
<b>DCIM.REQ.105</b>	Converged management layer	c. Closed: Area filled already and is not available		
<b>DCIM.REQ.106</b>	Converged management layer	d. Internal Use: Area used by Internal Racks		
<b>DCIM.REQ.107</b>	Converged management layer	e. Space Efficiency: Ratio between Room Area and sum of Reserved Area, Closed Area and Reserved Area.		
<b>DCIM.REQ.108</b>	Converged management layer	The proposed solution must offer intuitive, color-coded drawings in both plan and rack elevation views which allows users to:		
<b>DCIM.REQ.109</b>	Converged management layer	- View Rack U-space availability		
<b>DCIM.REQ.110</b>	Converged management layer	- View Rack Power availability		
<b>DCIM.REQ.111</b>	Converged management layer	- View Rack weight/Floor Loading		
<b>DCIM.REQ.112</b>	Converged management layer	- View Raised Floor & Rack space utilization		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DCIM.REQ.113</b>	Sandbox Testing	DCIM Management Layer should offer a dedicated Test Environment within the same solution which can import the live Data Centre 3D layouts and all power, cooling, network and u space details into a separate Sandbox Test Model without impacting the live functionality of the Management Layer. This will be used to simulate to simulate different scenarios, for example, whether the design is strong enough to cover your future requirements. If you continue to add equipment at the current pace, would the power supply suffice, or would you need additional power supplies or cooling units; would you continue to have the necessary redundancy, etc. Changes to these lab models should not affect the model of the actual live environment in Core DCIM Management Layer.		
<b>DCIM.REQ.114</b>	Predictive Analysis	Predictive Analysis/What If Analysis & Hypothetical Provisioning/ Modelling to ease decision making (such as: where is the best place to put new server, do my dc have sufficient power, cooling & space to occupy new equipment, etc.)		
<b>DCIM.REQ.115</b>	Power Path Map	Power Path: Ability to model power connections between the equipment supplying and delivering power and the equipment requiring power. This includes power path from switchgear, UPS, main PDU with modular circuit breaker mapping, rack RPDU and to individual servers.		
<b>DCIM.REQ.116</b>	Impact Simulation	Impact simulation: Generates a list of equipment that would be impacted if the selected piece of equipment, e.g., a UPS or cooling unit, about		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		to fail or put in maintenance mode.		
<b>DCIM.REQ.117</b>	Tool	The DCIM tool shall have a dedicated Equipment browser view where device Fields can be customized and sorted as per user need. It should allow for export of these data fields in the same format in a CSV file which can be opened in Excel as set by the user in the Equipment browser and also to save these formats for later use inside the DCIM.		
<b>DCIM.REQ.118</b>	Tool	The DCIM tool shall have an inbuilt Recommendation Engine that keeps on checking the various aspects of Data Centre design like:		
<b>DCIM.REQ.119</b>	Tool	Max Rack Load exceeded		
<b>DCIM.REQ.120</b>	Tool	Equipment weight Exceeds weight limit of floor Room doesn't have enough Airflow		
<b>DCIM.REQ.121</b>	Tool	Amount of Rack PDU Power Outlets has not been Configured		
<b>DCIM.REQ.122</b>	Tool	An Invalid Power Path has been Configured Associated Device Data has been Lost		
<b>DCIM.REQ.123</b>	Tool	Capacity Group Equipment is Placed in Multiple Rooms Connection has not been Configured between PDU and Power Supply		
<b>DCIM.REQ.124</b>	Tool	Connection has not been Configured between Power Panel and Power Supply Connection has not been Configured between Remote Distribution Panel (RDP) and Power Supply		
<b>DCIM.REQ.125</b>	Tool	Equipment Connected to this PDU Draws more Power than is Supported by the Power Supply Breaker		
<b>DCIM.REQ.126</b>	Tool	Equipment Connected to this Power Panel Draws more Power than is Supported by the Power Supply Breaker Equipment Connected to this Remote Distribution Panel (RDP)		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		Draws more Power than is Supported by the Power Supply Breaker		
<b>DCIM.REQ.127</b>	Tool	Equipment in this Rack Receives Power from Multiple Power Supply Devices		
<b>DCIM.REQ.128</b>	Tool	Equipment is Connected to a Rack PDU Outside this Rack Internal Redundancy Setup for UPS and Group Must Match PDU and Connected Rack PDU are Placed in Different Rooms		
<b>DCIM.REQ.129</b>	Tool	Power Connection Configuration is Invalid for Equipment in one or more Racks in the Group		
<b>DCIM.REQ.130</b>	Tool	Power Feed Connection for UPS and Group must Match Power Panel Output Voltage has not been Configured		
<b>DCIM.REQ.131</b>	Change Management	The DCIM tool should enable operators to gain control over the Data Centre environment by implementing organized moves, adds, and change work processes by providing workflow system that can develop and assign work orders, reserve space, track status, and provide a historical audit trail.		
<b>DCIM.REQ.132</b>		Ability to assign deadline and person to each work order.		
<b>DCIM.REQ.133</b>		Ability to create multiple tasks and track task status for each work order.		
<b>DCIM.REQ.134</b>		Ability to create work order templates that can be used for recurring work types like maintenance activities or standard procedure for installation of a certain type of server.		
<b>DCIM.REQ.135</b>		Support workflow management that should allow for easy implementation and tracking of organized moves, additions, and changes.		
<b>DCIM.REQ.136</b>		Support audit trail reporting that would show asset moves, additions,		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		and changes by date/time, owner, and work orders.		
<b>DCIM.REQ.137</b>		DCIM should allow for Integration with Dedicated Change Management Systems like BMC Remedy and Service Now as and when required.		
<b>DCIM.REQ.138</b>		Every network management change should be recorded in audit trail report		
<b>DCIM.REQ.139</b>		It should allow for Auto Scheduled Work Orders which can regenerate certain Service Work orders like Service Schedules for CRAC units which must renew themselves every Quarter or Yearly etc.		
<b>DCIM.REQ.140</b>	Energy Management (PUE & DCiE)	The application should provide real time Power Usage Effectiveness (PUE), DCiE values and able to deliver Weekly, Monthly, Quarterly & Yearly PUE report.		
<b>DCIM.REQ.141</b>	Energy Management (PUE & DCiE)	DCIM should be able to deliver the cost and CO2 emission per subsystem where subsystem data can either be measured (live) or computed (without power meters). It should showcase graphs for IT load, current PUE/DCiE, historical PUE/DCiE, costs and CO2 emission per subsystem.		
<b>DCIM.REQ.142</b>	Dashboard & Reporting	Reporting and Dashboard Proposed platform should offer Dashboard & Reporting on Data Centre key performance indicators, displaying customizable information for a high-level overview of Data Centre operations.		
<b>DCIM.REQ.143</b>	Dashboard & Reporting	We understand that certain DCIM systems may have restrictions to the number of points being Trended so to keep it logical the OEM will have to provision for trending and reporting parameters on site as per their mutual discussion during Pre-Installation Survey. At minimum DCIM		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		should provide Trending and Reporting for the following:		
<b>DCIM.REQ.144</b>	Dashboard & Reporting	PUE		
<b>DCIM.REQ.145</b>	Dashboard & Reporting	Total Facility Load Total It Load		
<b>DCIM.REQ.146</b>	Dashboard & Reporting	Total Cooling Load Row wise IT Load Rack wise IT load		
<b>DCIM.REQ.147</b>	Dashboard & Reporting	Average Temperature and Humidity for Cold Aisle (at Rack Inlet- 3ft)		
<b>DCIM.REQ.148</b>	Dashboard & Reporting	Average Temperature and Humidity for Host Aisle (at Rack Exhale-3ft)		
<b>DCIM.REQ.149</b>	Dashboard & Reporting	Communication Status for Infrastructure devices being monitored		
<b>DCIM.REQ.150</b>	Dashboard & Reporting	Depending on the device for which EM has been installed: Energy Meter: Per Phase Input Current and Voltage Energy Meter: Per Phase Output Current and Voltage Energy Meter: Power Factor per Phase		
<b>DCIM.REQ.151</b>	Dashboard & Reporting	Energy Meter: Frequency		
<b>DCIM.REQ.152</b>	Dashboard & Reporting	Energy Meter: Active Energy (kWh/MWh)		
<b>DCIM.REQ.153</b>	Dashboard & Reporting	Especially for UPS:		
<b>DCIM.REQ.154</b>	Dashboard & Reporting	UPS Per Phase Load percentage UPS Input Power		
<b>DCIM.REQ.155</b>	Dashboard & Reporting	UPS Output Power		
<b>DCIM.REQ.156</b>	Dashboard & Reporting	UPS Time Running on Battery		
<b>DCIM.REQ.157</b>	Dashboard & Reporting	CRAC/Inrow: Supply Air Temperature CRAC/Inrow: Return Air Temperature CRAC/Inrow: Supply Air Temperature Set point CRAC/Inrow: Supply Air Humidity Set point		
<b>DCIM.REQ.158</b>	Dashboard & Reporting	For Diesel Generator:		
<b>DCIM.REQ.159</b>	Dashboard & Reporting	Diesel Generator: Per Phase Voltage Diesel Generator: Mains Frequency Diesel Generator: Genset Frequency Diesel Generator: Engine Speed		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		(rpm) Diesel Generator: Oil Pressure Diesel Generator: Oil Temperature Diesel Generator: Fuel Level Diesel Generator: Running Time		
<b>DCIM.REQ.160</b>	Software	The management system should be centralized server appliance that can be accessed remotely from client workstations/servers via a HTTP/HTTPS connection or Windows client. Energy, Slide Show, Asset, Capacity, Work Order, Analytics, Asset Inspection and Incident Management modules are optionally offered by the management system.		
<b>DCIM.REQ.161</b>		1. On Demand Expendable Architecture of Modules on running DCIM without any downtime.		
<b>DCIM.REQ.162</b>		2. It should support perpetual License.		
<b>DCIM.REQ.163</b>		3. All the Modules Real Time Monitoring, Asset Management and PUE should be in same dashboard.		
<b>DCIM.REQ.164</b>		4. It should support the SNMP, Modbus TCP, Modbus RTU, OPC, Database, RTSP, ONVIF protocols directly.		
<b>DCIM.REQ.165</b>		5. Layout for Camera Monitoring should be on same interface of DCIM and should be configurable for reaction rules like camera popup for any Alarm.		
<b>DCIM.REQ.166</b>		6. Layout should be same for Application and Web UI.		
<b>DCIM.REQ.167</b>		7. Mobile monitoring application for Real time health monitoring and alerts of assets.		

#### 17.34 "Technical Requirements Specifications - Rodent repellent"

Product Name: Rodent repellent

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>RODENTR.REQ.001</b>	General Requirement	Compatible with standard AC power supply, typically around 230V AC, 50Hz. or better		
<b>RODENTR.REQ.002</b>	General Requirement	The device should be able to produce high frequency ultrasonic sound above 20KHZ.		
<b>RODENTR.REQ.003</b>	General Requirement	Area of effectiveness for one device should be more than 230x230 square feet and 8 feet height or better		
<b>RODENTR.REQ.004</b>	General Requirement	The device should have the testing feature		
<b>RODENTR.REQ.005</b>	General Requirement	The device should be compact and easy to install.		
<b>RODENTR.REQ.006</b>	General Requirement	The device should be harmless to humans.		
<b>RODENTR.REQ.007</b>	General Requirement	The device should be capable to keep away rodent from the room in which the device is installed.		

#### 17.35 "Technical Requirements Specifications - Water Leakage Detection"

Product Name: Water Leakage Detection

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>WTRLD.REQ.001</b>	Power	AC220V/50HZ+10% and 24VDC or better		
<b>WTRLD.REQ.002</b>	Voltage Scope	18V or better		
<b>WTRLD.REQ.003</b>	Charging voltage	27 V or better		
<b>WTRLD.REQ.004</b>	Battery	2x12 V/7 Ah or better		
<b>WTRLD.REQ.005</b>	Features	The water alarm control panel should providing the audible and visual information to the user, initiating automatic alarm response sequences and providing the means by which		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		the user interacts with the system		
<b>WTRLD.REQ.006</b>	Features	The water alarm control panel shall be able to be easily configured to meet the exact detection zone and cause/effects output requirement of the building.		
<b>WTRLD.REQ.007</b>	Features	Each zone card shall be capable of providing 300mA or better current and shall maintain a minimum of 24v or better on the zone up to the full extent of the battery standby period		
<b>WTRLD.REQ.008</b>	Features	The water leak alarm control panel shall have provision to drive and monitor a repeater panels		
<b>WTRLD.REQ.009</b>	Features	The water leak alarm control panel shall be capable of monitoring and controlling remotesite devices		
	<b>Water Leak Sensor Cable</b>			
<b>WTRLD.REQ.010</b>	Material	PVC Twisted pair with stainless elements or better		
	<b>Hooter</b>			
<b>WTRLD.REQ.011</b>	Type	Electronic Siren or equivalent		
<b>WTRLD.REQ.012</b>	Operating Voltage	12 Volt DC or better		
<b>WTRLD.REQ.013</b>	Sound level	100 dB or better		
<b>WTRLD.REQ.014</b>	Operating Temperature	0°C to +50° C or better		
<b>WTRLD.REQ.015</b>	IP Rating	IP65 Water Spray Proof / Dust Proof		

### 17.36 "Technical Requirements Specifications - Intelligent Addressable Fire Alarm System"

Product Name: Intelligent Addressable Fire Alarm System

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>INTELAFAS.REQ.001</b>	Basic System	The system shall be a complete, electrically supervised fire detection and evacuation system that includes communication devices such as fire fighter telephones. The system		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		shall be based on a microprocessor-driven control panel or better with the following capabilities and features: (i) Continuous monitoring of all fire alarm components. (ii) Supervision of all devices and circuits to ensure proper functionality. (iii) Efficient management of detection, alarm signaling, and evacuation processes.		
<b>INTELAFAS.REQ.002</b>	Basic System	Communication between network nodes shall be supported, with each node functioning as a self-contained, intelligent control panel. These panels shall provide system-wide displays and be capable of networking with other nodes.		
<b>INTELAFAS.REQ.003</b>	Basic System	The local system shall provide status indicators and control switches for the following functions: (i) Audible and visual notification circuits for zone-specific alarm control. (ii) Monitoring of sprinkler system devices , including water-flow sensors and valve supervisory devices. (iii) Additional status indicators or control functions as specified in the system design, such as emergency generator monitoring, fire pump operation, door unlocking mechanisms, and security bypass capabilities.		
<b>INTELAFAS.REQ.004</b>	Basic System	Each addressable or conventional zone device on the system shall be identified and monitored at the main control panel, allowing for precise location reporting of alarms, supervisory signals, and fault conditions.		
<b>INTELAFAS.REQ.005</b>	Fire Alarm Condition	1. The system shall sound an audible alarm and		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>display a custom screen/message indicating the building in alarm and the specific alarm point on an LCD display.</p> <p>2.The system shall support networking of up to 16 nodes or better</p> <p>3. All activity related to the alarm condition shall be logged into the system's history archives</p> <p>4.The system shall sound an alarm with synchronized audible alerts</p> <p>5.Audible signals shall be silenced from the fire alarm control panel using an alarm silence switch.</p> <p>6.HVAC shutdown shall be controlled by system-operated duct detectors</p>		
<b>INTELAFAS.REQ.006</b>	Fire Alarm Condition	<p>A. The system shall comply with NFPA 72 and meet all specified requirements.</p> <p>B. All interconnections between the fire alarm and monitoring systems shall be designed to enable UL certification.</p> <p>C. The system shall include Style 6 circuits for each floor and operate in alarm mode upon activation of any initiating device.</p>		
<b>INTELAFAS.REQ.007</b>	Fire Alarm Condition	<p>D. The system shall be capable of the following configurations. Both configurations are permitted on the same network.</p> <p>1. The system shall support up to 252 addressable devices, which may be divided in any ratio on one, two, three, or four separate, isolated Class B circuits.</p> <p>2. The system shall support two loops of 252 addressable devices, each of which may be divided in any ratio on one, two, three, or four separate, isolated Class B circuits.</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
INTELAFAS.REQ.008	Fire Alarm Condition	<p>E. The system shall have an optional digital alarm communication transmitter.</p> <p>F. The system shall provide an off-normal warning prior to reset for all active devices.</p> <p>G. The system shall be capable of remote monitoring, a proprietary software system that provides a graphical representation of the fire alarm control panel at a remote PC when connected via Ethernet to the system. The display will show the exact state of the panel, including blinking LEDs, and with menu buttons for control.</p> <p>H. The system shall be capable of being configured via a PC Tool.</p> <p>I. In networked systems, each of 4 control panels shall be configurable to be a global annunciator, capable of viewing all other control panels on the network.</p>		
INTELAFAS.REQ.009	Fire Alarm Condition	<p>J. The system shall provide the following functions and operating features:</p> <ol style="list-style-type: none"> <li>1. The FACP and auxiliary power panels shall provide power, annunciation, supervision and control for the system.</li> <li>2. Provide Class A initiating device circuits.</li> <li>3. Provide Style 7 signaling line circuits for the network.</li> <li>4. Provide two Class A notification appliance circuits. Arrange circuits to allow individual, selective, and visual notification by zone. Notification appliance circuits shall be zoned to correspond with the building fire</li> </ol>		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		barriers and other building features. 5. Strobes shall be synchronized throughout the entire building. 6. Provide electrical supervision of the primary power (AC) supply, presence of the battery, battery voltage, and placement of system modules within the control panel.		
<b>INTELAFAS.REQ.010</b>	Fire Alarm Condition	K. The system shall provide a field test function where one person can test the complete system or a specific area while maintaining full operational function of other areas not being tested. Alarms, supervisory signals, trouble signals shall be logged in system history during the walk-test. L. Alarm functions shall override trouble or supervisory functions. Supervisory functions shall override trouble functions.		
<b>INTELAFAS.REQ.011</b>	Supervisory Condition	1. Display the origin of the supervisory condition report at the fire alarm control panel graphic LCD display. 2. Activate supervisory audible and dedicated visual signal. 3. Audible signals shall be silenced from the control panel by the supervisory acknowledge switch. 4. Record within system history the initiating device and time of occurrence of the event. 5. Print to the system printer (where required) the supervisory condition.		
<b>INTELAFAS.REQ.012</b>	Trouble Condition	1. Activate trouble audible and visual signals at the control panel and as indicated on the drawings.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>2. Audible signals shall be silenced from the fire alarm control panel by a trouble acknowledge switch.</p> <p>3. Trouble conditions that have been restored to normal shall be automatically removed from the trouble display queue and nor require operator intervention. This feature shall be software selectable and shall not preclude the logging of trouble events to the historical file.</p> <p>4. Record within system history, the occurrence of the event, the time of occurrence and the device initiating the event.</p> <p>5. Print to the system printer (where required) the trouble condition.</p>		
<b>INTELAFAS.REQ.013</b>	Security Condition	<p>1. Display at the fire alarm control panel with LCD display, the origin of the security condition report. A dedicated security LED shall flash until the alarm has been acknowledged, then revert to a steady "ON" state.</p> <p>2. The control system shall be capable of bypassing the alarms from an individual security system installed within selected areas. The pass code allowing this function shall be assignable to individual security personnel and each bypass action shall be logged to system history. Intrusion alarms occurring during a bypass period shall be logged to history and displayed but no audible alarm shall occur at the control panel.</p> <p>3. Print to the system</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		printer (where required) the security condition. 4. The Fire Control Panel shall be "UL" 1076 listed for security purposes.		
INTELAFAS.REQ.014	Control panel	<p>The fire alarm control panel shall be microprocessor based using multiple microprocessors throughout the system providing rapid processing of smoke detector and other initiation device information to control system output functions.</p> <p>a. There shall be a watchdog circuit, which shall verify the system processors and the software program. Problems with either the processors or the system program the panel shall activate a trouble signal and reset the panel.</p> <p>b. The system modules shall communicate with an RS 485 network communications protocol. All module wiring shall be to terminal blocks.</p> <p>c. The system shall be capable of the following configurations. Both configurations are permitted on the same network.</p> <p>d. The Cerberus Pro panel shall support two DLC of 252 addressable devices, each of which may be divided in any ratio on one, two, three, or four separate, isolated Class B circuits.</p> <p>e. The control panel shall have a 2"x4-3/4" Size VGA monochrome LCD display and having maximum 320 (8 x 40) Characters in the</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		display. The panel shall have a built-in power supply of 170 Watts and battery charger. Battery charger shall be able to charge the system batteries up to 33 AH. The Panel shall have the capacity of connecting additional 15 panels or Network terminals using network card, with redundancy in the network, TCP/ IP connectivity for Central Monitoring station The system shall be capable of supporting unshielded wiring applications		
<b>INTELAFAS.REQ.015</b>	System Components	i. The System Periphery board shall be capable of 252 intelligent devices distributed between one, two, three, or four Class B SLC circuits. Any trouble on one circuit shall not affect the other circuit. This module controls the signaling from the initiation devices reporting alarms and troubles to the control panel. This module shall also provide the signaling to the field devices for the controlling the output of specific initiation devices. The on-board microprocessor provides the periphery board with the ability to function even if the main microprocessor fails. LED's on the board shall provide annunciation for the following: Power, Gnd. Fault, Alarm, Trouble. This board is integral to the system.		
<b>INTELAFAS.REQ.016</b>		ii. The system periphery board shall be capable of supporting two system drivers of 252 intelligent devices distributed between one, two, three, or four Class B SLC circuits, for a total		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>panel capacity of 504 addressable devices. Any trouble on one circuit shall not affect the other circuit. This module controls the signaling from the initiation devices reporting alarms and troubles to the control panel. This module shall also provide the signaling to the field devices for the controlling the output of specific initiation devices.</p> <p>The on-board microprocessor provides the periphery board with the ability to function even if the main microprocessor fails. LED's on the board shall provide annunciation for the following: Power, Gnd. Fault, Alarm, Trouble. This board is integral to the system.</p>		
	<b>INTELAFAS.REQ.017</b>	<p>iii. The Signal Line Circuits (SLC) shall be tested for opens, shorts and communications with all addressable devices installed before connection to the control panel. Systems without this capability shall have a test panel installed for initial testing to eliminate any possible damage short term or long term to the control panel. After initial testing replace the test panel and proceed with complete testing.</p>		
	<b>INTELAFAS.REQ.018</b>	<p>iv. The standard Operator Interface shall have the ability to view events, acknowledge, silence, and reset the system and any networked Cerberus Pro control panels, when configured as a global PMI.</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
INTELAFAS.REQ.019		v. The LED Operator Interface shall have the ability to view events, acknowledge, silence, and reset the system and any networked control panels, when configured as a global PMI. Additionally, the operator interface provides twelve multicolored configurable LEDs for annunciating system status		
INTELAFAS.REQ.020		vi. The Network Card shall provide internodes (SafeDLink) communication between enclosures. SafeDLink communication shall support Class B Style 4 or Class A Style 7 wiring (in a ring configuration). This card shall plug into the system operator interface.		
INTELAFAS.REQ.021		vii. The System Periphery Board shall contain 2 Class B NAC circuits rated at 3 amps each with power-limited outputs. The zones shall be isolated and independently supervised. There shall be at least 6 unique codes/signals for each circuit based on system logic. These signals shall be Temporal Code 3 (Evacuation), Steady (Such as "Recall"), Temporal Code 3 (for CO alarms), March Time 120ppm, March Time 60ppm, and March Time 30ppm. The card shall have the following LED's to provide trouble shooting and annunciation, Power, Gnd. Fault, Zone Activation or Trouble. This functionality shall be integral to the system.		
INTELAFAS.REQ.022		viii. The control panel shall be equipped with four Form C relays for		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		alarm, trouble, supervisory, and programmable output. The system shall provide the mounting of all system cards, field wiring, and panel's inter-card wiring. All power limited field wiring shall be separated from all non-power limited internal wiring.		
<b>INTELAFAS.REQ.023</b>	Response time	<p>The System response time from alarm to output shall be an average of three (3) seconds.</p> <p>a. All system cards and modules shall have Flash memory for downloading the latest module firmware.</p> <p>b. Passwords:</p> <p>Technician Level Password - There shall be a 4-character password that a user must enter into the control panel in order to perform such maintenance- and control-related functions at the panel as:</p> <p>Arming and disarming devices.</p> <p>1. Activating and deactivating the History Log function and deleting obsolete entries.</p> <p>2. Changing the system time and date.</p> <p>Maintenance Level Password - There shall be a 4 character password that a user must enter into the control panel in order to access the panel's reporting functions and walk test functions.</p> <p>Acknowledge Silence able Reset Access - There shall be a key required to open a locked cabinet that a system user must use in order to acknowledge events, turn silence able</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		audible and visuals on and off, and perform panel resets.		
<b>INTELAFAS.REQ.024</b>	Power Supply	<p>a. The power supply provides power for all system operation, including signaling line circuits, notification appliance circuits, auxiliary power, battery charger, and all optional modules. The power supply shall be rated for 120/240 VAC 50/60 Hz.</p> <p>b. The power supply provides power for all system operation, including signaling line circuits, notification appliance circuits, auxiliary power, battery charger, and all optional modules. The power supply shall be rated for 120/240 VAC 50/60 Hz.</p> <p>c. The battery charger shall be able to charge the system batteries up to 100 AH batteries. Battery charging shall be microprocessor controlled and programmed to select battery sizes.</p> <p>d. Transfer from AC to battery power shall be instantaneous when AC voltage drops to a point where it is not sufficient for normal operation.</p>		
<b>INTELAFAS.REQ.025</b>	Intelligent Initiation Devices	<p>All initiation devices shall be insensitive to initiating loop polarity. Polarity insensitive wiring allows fire detection devices to operate flawlessly even when detector and devices wiring polarity are inverted on the wrong screw terminals. When wiring polarity doesn't need to be observed, wiring troubleshooting is greatly</p>		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		reduced, this will also save time of installation Specifically, the devices shall be insensitive to plus/minus voltage connections on either Style 4 or Style 6 circuits		
<b>INTELAFAS.REQ.026</b>	Intelligent Audible (Sounder) Base	Intelligent Audible (Sounder) Base [with Loop-Power Option shall be UL / ULC Listed — has the option of being powered directly from a signal line circuit (SLC) in a two-wire configuration. In turn, this connection feature gives each audible (sounder) base. The innovative loop-power option shall provide easier two-wire connection for new or expansion applications where additional wiring or power options are limited. Sounder base shall be capable of generating a 3,000 Hz tone that provides a signal up to 85dBA at 10 feet (3.1m) for localized annunciation		
<b>INTELAFAS.REQ.027</b>	Device Programming Unit	the intelligent devices with addresses. The unit shall test the device to respond to its address. Dipswitches and rotary switches shall not be acceptable		
<b>INTELAFAS.REQ.028</b>	Field Programming	he field itself by use of dedicated programming software. In order to avoid unauthorized access programming via panel keyboard is not acceptable. The field programmability will allow changes in various system parameters as per their operation philosophy. All programming will be accomplished through DPU or Laptop. The program (software) used to		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>configure the Fire Alarm Panel will be submitted in a CD along with other submittals during training and handover.</p> <p>All field defined programs will be stored in non-volatile memory to ensure no data is lost during the power loss.</p>		
<b>INTELAFAS.REQ.029</b>	Manual Call Points OR Pull stations	<p>1. Provide addressable manual stations were shown on the drawings, to be flush or surface mounted as required. Manual stations shall contain the intelligence for reporting address, identity, alarm and trouble to the fire alarm control panel. The manual station communications shall allow the station to provide alarm input to the system and alarm output from the system within less than four (4) seconds.</p> <p>2. The manual station shall be equipped with terminal strip and pressure style screw terminals for the connection of field wiring. Surface mounted stations were indicated on the drawings shall be mounted using a manufacturer's prescribed matching red enamel outlet box.</p> <p>3. The single action pull station shall be model number HMS-S.</p> <p>4. Where required, there shall also be available pull stations with break glass, capable of explosion proof installation, capable of weatherproof installation, two stage operation, reset key operation, and metal housings</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
INTELAFAS.REQ.030	Addressable Control Module	<p>1. Addressable control modules shall be provided to supervise and control the operation of one conventional device of compatible, 24 VDC powered polarized audio/visual notification appliances. For fan shutdown and other auxiliary control functions, the control module may be set to operate as a dry contact relay.</p> <p>2. The control module shall mount in a standard 4-inch square (101.6 mm square), 2-1/8 inch (54 mm) deep electrical box, or to a surface mounted back box.</p> <p>3. The control module shall be wired with up to 1 amp of inductive A/V signal, or 2 amps of resistive A/V signal operation, or as a dry contact relay. The relay coil shall be magnetically latched to reduce wiring connection requirements, and to ensure that 100% of all auxiliary relay may be energized at the same time on the same pair of wires.</p> <p>4. Audio/visual power shall be provided by a separate supervised power circuit from the main fire alarm control panel or from a supervised, UL listed remote power supply.</p> <p>5. The control module shall be suitable for pilot duty applications and rated for a minimum of 0.6 amps at 30 VDC.</p>		
INTELAFAS.REQ.031	Interface Module	and is polarity insensitive, achieves the state of an 'intelligent device' through its highly advanced method of address programming and		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		supervision — combined with its sophisticated, bi-directional FACP communication. The relays and contact device inputs are controlled at the same address. For the FACP, the relays and input contacts can be controlled as a separate function. The relay is typically used where control or shunting of external equipment is required. Four (4) independent in/out circuits are permissible. Interface module shall be designed to monitor Normally Open (N.O) or Normally Closed (N.C) dry contact		
	<b>INTELAFAS.REQ.032</b>	potential free-latching-type 'Form A' (dry) relay contacts for fire-control installations. The panel's communication provides supervised, power-limited power supply. The four (4) input / (4) output interface module provides status indication per LED for each input / output, plus one (1) LED for device status.		
	<b>INTELAFAS.REQ.033</b>	Four (4) inputs / four (4) outputs via one (1) address <ul style="list-style-type: none"> <li>• Input lines can be supervised for open, short and ground-fault conditions</li> <li>• Light-emitting diode (LED) display of input / output status</li> <li>• Supports 'Class A' and 'Class B' input-circuit wiring</li> <li>• Polarity insensitive technology</li> <li>• Microprocessor-controlled signal evaluation</li> <li>• Two-wire installation, per addressable loop</li> <li>• Individual addressing</li> <li>• Four (4) AC-rated / DC-</li> </ul>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		<p>rated outputs</p> <ul style="list-style-type: none"> <li>Mounts in one (1) electrical back box</li> <li>§ Optional 12 cm. and 12.7 cm. square back boxes</li> <li>Electronic address programming is easy and dependable</li> <li>Easy front-end access to programming port and wiring terminals</li> <li>Restriction of Hazardous Substances (RoHS compliant)</li> <li>ULC Listed;</li> </ul>		
<b>INTELAFAS.REQ.034</b>	Monitor Module	<p>1. Addressable monitor modules shall be provided to connect one supervised IDC zone of conventional 2-wire smoke detectors or alarm initiating devices (any N.O. dry contact device).</p> <p>2. The two-wire monitor module shall mount in a 4-inch square (101.6 mm square), 2-1/8 inch (54 mm) deep electrical box or with an optional surface back box.</p> <p>3. The IDC zone shall be wired for operation. An LED shall be provided that shall flash under normal conditions, indicating that the monitor module is operational and in regular communication with the control panel.</p>		
<b>INTELAFAS.REQ.035</b>	Addressable Relay Module	<p>Addressable Relay Modules shall be available for HVAC control and other building functions. The relay shall be rated for a minimum of 2.0 Amps resistive or 1.0 Amps inductive. The relay coil shall be magnetically latched to reduce wiring connection requirements, and to ensure that 100% of all auxiliary relay may be energized at</p>		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		the same time on the same pair of wires		
<b>INTELAFAS.REQ.036</b>	Isolator Module	<p>Isolator modules shall be provided to automatically isolate wire-to-wire short circuits on a loop Class A. The isolator module shall limit the number of modules or detectors that may be rendered inoperative by a short circuit fault on the loop segment or branch. At least one isolator module shall be provided for each set of detectors (max 19 numbers).</p> <p>2. If a wire-to-wire short occurs, the isolator module shall automatically open-circuit (disconnect) the loop. When the short circuit condition is corrected, the isolator module shall automatically reconnect the isolated section.</p> <p>3. The isolator module shall not require any address-setting, and its operations shall be totally automatic. It shall not be necessary to replace or reset an isolator module after its normal operation.</p> <p>4. The isolator module shall mount in a standard 4-inch (101.6 mm) deep electrical box or in a surface mounted back box. It shall provide a single LED that shall flash to indicate that the isolator is operational and shall illuminate steadily to indicate that a short circuit condition has been detected and isolated.</p>		
<b>INTELAFAS.REQ.037</b>	Addressable Interface Devices	Addressable Interface Devices shall be provided to monitor contacts for such items as		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		conventional gas/ agent release panels, water-flow, tamper, and PIV switches connected to the fire alarm system.		
<b>INTELAFAS.REQ.038</b>	Notification Appliances	solution shall notify of an alarm (e.g., horns, strobes). Must meet specific requirements, depending on the area covered.		
<b>INTELAFAS.REQ.037</b>	Addressable Interface Devices	Addressable Interface Devices shall be provided to monitor contacts for such items as conventional gas/ agent release panels, water-flow, tamper, and PIV switches connected to the fire alarm system.		
<b>INTELAFAS.REQ.038</b>	Notification Appliances	solution shall notify of an alarm (e.g., horns, strobes). Must meet specific requirements, depending on the area covered.		

### 17.37 "Technical Requirements Specifications - Smoke Detection System"

Product Name: Smoke Detection System

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SMKDS.REQ.001</b>		The ASD panel should be connect with DCIM software to have detail monitoring from centralized level. The alert system can be generated as per user requirements.		
<b>SMKDS.REQ.002</b>	Supply voltage range	EN 54 -10.5–30 VDC/14.0–30 VDC or FM/UL - 12.4–27 VDC/16.4–27 VDC		
<b>SMKDS.REQ.003</b>	Power consumption	210 mA to 115 mA		
<b>SMKDS.REQ.004</b>	Sampling tubes/smoke sensors	1		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>SMKDS.REQ.005</b>	Autolearning, day/night switching	Configurable		
<b>SMKDS.REQ.006</b>	Relays	3 (1alarm, 1fault, 1free)/ 2 (1alarm, 1fault)		
<b>SMKDS.REQ.007</b>	Interfaces	O.C. outputs -See relays, PC tool -USB, Inputs - Reset, day/night/O.C. outputs -See relays, PC tool - Ethernet, Network - RS 485, Ethernet, Inputs - Reset, day/night		
<b>SMKDS.REQ.008</b>	Connection to FACP	1–3, fault, reset		
<b>SMKDS.REQ.009</b>	Number of samplings apertures (with ASD Pipe Flow)	EN 54-20 Class A-8 to 16, EN 54-20 Class B-12 to 50, EN 54-20 Class C 16 to 50		
<b>SMKDS.REQ.010</b>	System limits as per EN 54-20 Class C	Max. quantity sampling apertures-16, Max. length to Max. length to-70m, Max. overall length of all sampling tubes-120m		
<b>SMKDS.REQ.011</b>	System limits without conformity to standards	Max. overall length of all sampling tubes-120mtr		
<b>SMKDS.REQ.012</b>	Calculation of sampling tubes for all four types of aspirating smoke detectors	ASD Pipe Flow- • Calculation according EN-54-20 (Class A, B, C) or NFPA 72		
<b>SMKDS.REQ.013</b>	Fan/sampling system	Suction pressure- > 400 Pa/200pa, Service life (MTTF)- > 65,000 h (at 40°C)/ > 65,000 h (at 40°C), Performance levels- 13, Noise level (1m distance)- 34 dB (A) (fan level 1)/ 25 dB (A) (fan level 1), Soundproof housing- < 20 dB (A)		
<b>SMKDS.REQ.014</b>	Airflow monitoring	1 air flow sensor (therm. Anemometer)		
<b>SMKDS.REQ.015</b>	Housing	EN 60529 port Class-IP 54, Dimensions (W×H×D)- 195×290×140 mm, Cover, grey- RAL 280 70 05, Base, anthracite violet- RAL 300 20 05, Material- ABS blend, UL 94-V0, Weight		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		(approx.)- 1950 g., 1950 g		
<b>SMKDS.REQ.016</b>	Operating temperature/ humidity	-20 – +60°C/95% RH (amb. air max. +40°C)		
<b>SMKDS.REQ.017</b>	Display and operation	Generally, per channel-red «alarm» LED, 1 yellow «fault» LED, , 1 yellow soiling LED, 1		
<b>SMKDS.REQ.018</b>	Event memory/ analogue values	1000 events, up to 1-year on-board option		
<b>SMKDS.REQ.019</b>	Standards/approvals	EN 54-20-VdS G 212163/VdS G 215101, EN 54-27 (ventil. ducts)- yes, UL, FM-yes, Other- Active Fire, CCCF, ISO 7240-20, GOST, Compliance-EMC, CPR, RoHS, EAC		

### 17.38 "Technical Requirements Specifications - Fire Suppression System"

Product Name: Fire Suppression System

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>FRESUPS.REQ.001</b>	Scope	The scope includes the supply, installation, testing & commissioning. The scope also includes fire suppression system piping, installation work with all required accessories and other activities that are not specifically mentioned in the specifications but are required for successful commissioning of the project.		
<b>FRESUPS.REQ.002</b>	General	The bidder shall supply, install, test and put in operation NOVEC 1230 based fire suppression system.		
<b>FRESUPS.REQ.003</b>	General	installation, testing, training & handing over of all materials, equipment, hardware, software appliances and necessary labour to commission the said system, complete with all the required components strictly as per the enclosed tender specifications,		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		design details. The scope also includes the supply, installation & commissioning of any material or equipment including civil works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project.		
<b>FRESUPS.REQ.004</b>	General	The system design should be based on the specifications contained herein, NFPA 2001 and in accordance with the requirements specified in the design manual of the agent. The bidder, shall confirm compliance to the above along with their bid.		
<b>FRESUPS.REQ.005</b>	Refilling and Maintenance	should be possible to refill the cylinders in India itself in the CCOE approved filling station. The contractor should indicate the source of refilling and time that will be taken for refilling and replacement.		
<b>FRESUPS.REQ.006</b>	Discharge Time	quenching of fire as per the relevant standards, the contractor has to ensure that the design meets this requirement. Once the discharge takes place there should be warning signs restricting personal from entering the protected area until the gas has been cleared from the area.		
<b>FRESUPS.REQ.007</b>	Materials and Equipment's	All materials and equipment's shall be from approved manufacturers and shall be suitable for the performance of their respective functions. The cylinders should be complete with all accessories. The contractor shall indicate the dimensions of the		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		cylinders required for each area while quoting.		
<b>FRESUPS.REQ.008</b>	Cylinder	The cylinder shall be high pressure, seamless steel gas cylinder, flat type, concave bottom as per IS 7285 complete with neck ring. Welded and non-CCE approved cylinders will not be accepted.		
<b>FRESUPS.REQ.009</b>	Cylinder	Each cylinder shall be seamless steel type manufactured from billets and tested in accordance with IS 7285.		
<b>FRESUPS.REQ.010</b>	Cylinder	The maximum fill density of Sinorix (NOVEC) 1230 in a cylinder shall not exceed 0.85 Kg/Lit. Of internal volume. Appropriate fill density shall be chosen based on the cylinder location and piping. The hydraulic calculations should prove that the fill density is appropriate and total discharge will take place within 10 seconds		
<b>FRESUPS.REQ.011</b>	Cylinder	The cylinders shall be super-pressurized with dry nitrogen to 42 bars at 20°C. The cylinder shall be capable of withstanding any temperature between -30° C and 70°C. Cylinder shall be mounted according to manufacturer recommendations. The cylinder shall withstand Hydrostatic test pressure up to 250 bars and maximum working pressure at 15°C shall be 150 bars		
<b>FRESUPS.REQ.012</b>	Cylinder	The cylinder/valve assembly shall have suitable metallic protection for the valve enabling transportation of the filled cylinders safely.		
<b>FRESUPS.REQ.013</b>	Cylinder	All cylinders shall be distinctly and permanently marked with the		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		quantity of agent contained, the empty cylinder weight, the pressurization pressure and the zones they are protecting.		
<b>FRESUPS.REQ.014</b>	Cylinder	Each cylinder shall be provided with a valve of suitable size. Each cylinder valve shall have a provision for fixing a supervisory pressure switch and a safety burst disc to protect the cylinder from over pressure. The cylinder valve shall necessarily have a disabling plug (locking pin) to prevent accidental discharge of the valve during transportation and installation. The Valve assembly shall be mounted directly on the cylinder		
<b>FRESUPS.REQ.015</b>	Cylinder	Each valve is to be fitted with a pressure gauge for monitoring loss of pressure.		
<b>FRESUPS.REQ.016</b>	Cylinder	The master cylinder valve is to be released electrically which is performed by means of a solenoid valve arrangement. Pilot cylinder actuation and pyrotechnic devices shall not be used.		
<b>FRESUPS.REQ.017</b>	Cylinder valve Actuators	n a single cylinder system, the cylinder shall have a solenoid operated actuator and a manual actuator incorporating a strike knob mounted on top of the solenoid operated actuator. Multi cylinder systems shall have the same fitted on to the master cylinder and pressure operated actuators fitted on each slave cylinder. All actuators shall be original OEM make and locally		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		manufactured actuators shall not be used.		
<b>FRESUPS.REQ.018</b>	Hoses	Each cylinder valve shall be provided with a plug-in type of flexible rubber discharge hose of minimum 40mm size and shall with stand a test pressure as at least 150 -200% of the cylinder stored pressure. Each hose shall be permanently marked with the test pressure and OEM's part number. Multi cylinder systems shall have an interconnect hose for each cylinder. The interconnect hose shall have a length not less than 700 mm and shall be labeled with the test pressure of 100 Bar and the OEM's part number. All hoses shall be original		
<b>FRESUPS.REQ.019</b>	Manifold with Check valve	The manifold shall be fabricated from ASTM A106 Schedule 40 seamless pipe and shall have integral check valves provided for each cylinder.		
<b>FRESUPS.REQ.020</b>	Other Accessories	Electric Control Head, Pressure operated control head, Master Cylinder Adapter Kit, Flexible discharge hose, discharge Nozzles, and other required accessories shall be approved or listed for use with (NOVEC) 1230 All the gaskets, O-ring, sealant and other components shall be constructed of materials compatible with the clean agent. The system should be engineered using hardware & accessories approved by the Engineering System Distributors of (NOVEC) 1230 as mentioned in the list of approved makes.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		The Vendor shall submit the detailed data sheets & drawings of each accessory with the required part Nos and also the common system data sheet containing these parts with part Nos.		
<b>FRESUPS.REQ.021</b>	Pipes & Fittings	All Pipes shall be of ASTM - A-106, Gr: B, schedule - 40 seamless Mild Steel Pipes and fittings shall be as per ASTM-A-105 standard. Distribution piping and fittings shall be installed in accordance with the manufacturer's requirements, NFPA 2001, and approved piping standards and guidelines. All distribution piping shall be installed by qualified individuals using accepted practices and quality procedures. All piping shall be adequately supported and anchored at all directional changes and nozzle locations.		
<b>FRESUPS.REQ.022</b>	Discharge Nozzle	Engineered discharge nozzles shall be provided within the manufacturer's guidelines to distribute the (NOVEC) 1230 agent throughout the protected spaces Nozzle shall control the flow of (NOVEC) 1230 to ensure high velocity, proper mixing in the surrounding air and uniform distribution of the agent throughout the enclosure.		
<b>FRESUPS.REQ.023</b>	Fire Detection & Gas Release Panel & operation process	fire detection cum gas release panel specifically used for each protected area. The detectors shall be in cross zone and the trigger from the panel shall be for 2 stage action.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>FRESUPS.REQ.024</b>	Fire Detection & Gas Release Panel & operation process	Some of the enhance features of the detection cum gas release panel shall be, <ul style="list-style-type: none"> <li>• Easy on-site configuration</li> <li>• Upload / download of configuration data's</li> <li>• Event logging facilitates identifying origin of events</li> <li>• Display countdown timer before extinguishing release</li> <li>• Extinguishing automatic activation with various alarm combinations</li> <li>• 72h battery backup time</li> <li>• Various system test modes</li> <li>• Automatic calibration facility for actuators control lines (solenoid or pyrotechnical actuators)</li> <li>• Manual Release button for manual activation of extinguishing</li> <li>• Emergency hold button to temporary stop the extinguishing or abort button to cancel the initiated extinguishing release as long as the pre-warning time is running</li> <li>• Remote transmission facility for transmitting alarms and faults</li> </ul>		
<b>FRESUPS.REQ.025</b>	Fire Detection & Gas Release Panel & operation process	If in case the fire detection part is handled by a separate fire control panel, the panel shall have the capability to integrate with larger fire detection system. Also, the panel shall have the facility to connect repeater panel for remote status indication and remote control.		
<b>FRESUPS.REQ.026</b>	Auto mode Operation	The sequence of operation of the gas release system shall be as follows.		
<b>FRESUPS.REQ.027</b>	Auto mode Operation	When the any one of the detectors connected to the building fire alarm panel goes into alarm, immediately the sounder cum		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		strobe shall get activated.		
<b>FRESUPS.REQ.028</b>	Auto mode Operation	The fire detection cum gas release panel shall ensure that the access control shall get deactivated.		
<b>FRESUPS.REQ.029</b>	Auto mode Operation	The first stage activation in the gas release circuit shall happen only when any one of the detectors in the protected area goes into alarm.		
<b>FRESUPS.REQ.030</b>	Auto mode Operation	When the first stage gets activated, the specific zone numbers and the detectors location shall be displayed, and the panel buzzer shall start operating. The stage 1 bells shall be identified by the fact that they pulsate at the rate defined by timer 1.		
<b>FRESUPS.REQ.031</b>	Manual Mode Operation	The manual release shall happen in three ways. Manual Release through the panel, Manual release station & Manual Release directly from the cylinder		
<b>FRESUPS.REQ.032</b>	Manual Mode Operation	The electric manual release (activated through the panel) shall be a dual action switch device which provides a means of manually discharging the suppression system from the panel		
<b>FRESUPS.REQ.033</b>	Manual Mode Operation	The manual release station shall also be a dual action device requiring two distinct operations to initiate a system actuation.		
<b>FRESUPS.REQ.034</b>	Manual Mode Operation	Manual actuation shall be capable of bypass the time delay or shall have the time delay depending upon the client requirements. It shall be possible to program both at site and abort functions and shall cause all release and shutdown devices to operate		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		in the same manner as if the system had operated automatically.		

### 17.39 "Technical Requirements Specifications -Master Control Unit"

Product Name: Master Control Unit

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>MCU.REQ.001</b>	General Specifications	The master control unit shall contain the both public address and voice alarm functions in terms of controlling, monitoring and operation		
<b>MCU.REQ.002</b>	General Specifications	The master control unit shall have 16 programmable keys. 8 of them are configurable for audio selection and the other 8 of them are configuration for loudspeaker line selection. Loudspeaker lines shall be either programmed as one speaker line or a group of speaker lines.		
<b>MCU.REQ.003</b>	General Specifications	The master control unit shall have built-in 500W Class-D amplifiers. The built-in amplifier shall allow two modes of power distribution: to drive totally 8 loudspeaker line output @100V or to drive the first 4 loudspeaker line output. When the built-in amplifier drives the first 4 loudspeaker line output, the master control unit shall allow one more booster amplifier connected to the master control unit to increase another 500W power capacity for audio channel 1.		
<b>MCU.REQ.004</b>	General Specifications	The master control unit shall have the configuration to supervise the status of all of audio inputs, dry contact inputs, dry contact outputs, built-in flash memory, power supply, built-in amplifier and loudspeaker lines through 3 color indicators (normal, fault & emergency) and the fault list in the GUI of screen on the front panel.		
<b>MCU.REQ.005</b>	General Specifications	The master control unit shall be able to connect with 1 x backup amplifier via control port. It shall be		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		able to switch the backup amplifier to replace the faulted amplifier during the system is powered on. Any backup amplifier connected with any control unit including master control unit and zone expander, the master control unit shall automatically proceed the preset backup solution. It shall support 1 x backup amplifier to backup with multiple main amplifiers.		
<b>MCU.REQ.006</b>	General Specifications	The master control unit shall be able to deliver direct paging through PTT microphone on the front panel to all loudspeaker lines during the CPU is defected.		
<b>MCU.REQ.007</b>	General Specifications	The master control unit shall log system faults and operations. Log shall be exported from configuration tools.		
<b>MCU.REQ.008</b>	General Specifications	The master control unit shall have basic settings and the current configurations shall be exportable from the device via configuration tool.		
<b>MCU.REQ.009</b>	General Specifications	The master control unit shall have 4G built-in memory to store music contents in WAV format which shall be able to store 90 minutes of built-in message.		
<b>MCU.REQ.010</b>	General Specifications	There shall be a built-in recorder allowing user to record paging task from PTT and allowing temporarily record task up to 60 minutes. The temporary task shall be auditable before delivery and shall be able to set repeating cycle.		
<b>MCU.REQ.011</b>	General Specifications	Each loudspeaker line outputs shall handle up to 500 Watt.		
<b>MCU.REQ.012</b>	General Specifications	The master control unit shall be able to handle up to 1000 Watt load.		
<b>MCU.REQ.013</b>	General Specifications	The master control unit shall be an CE, CB and CCCF compliant		
<b>MCU.REQ.014</b>	Product Specifications	The master control unit shall be put in a 3 RU, 19"-cabinet.		
<b>MCU.REQ.015</b>	Product Specifications	Main power supply: AC 220V-240V 50/60Hz		
<b>MCU.REQ.016</b>	Product Specifications	Backup power supply: AC 220V-240V 50/60Hz		
<b>MCU.REQ.017</b>	Product Specifications	Fuse: T10AH 250V		
<b>MCU.REQ.018</b>	PTT Microphone	Power consumption : <760W		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
MCU.REQ.019	PTT Microphone	Sensitivity: -59±3dBV		
MCU.REQ.020	PTT Microphone	Frequency response: 100Hz - 14KHz, ±3dB		
MCU.REQ.021	Auxiliary input	SNR: >50dB, A-weighted		
MCU.REQ.022	Auxiliary input	Number: 2		
MCU.REQ.023	Auxiliary input	Input sensitivity: 1V(0dBV)		
MCU.REQ.024	Auxiliary input	Input impedance: 10 KΩ		
MCU.REQ.025	Auxiliary input	Frequency response: 80Hz-18KHz, ±3dB		
MCU.REQ.026	MIC/LINE Input	SNR: >80dB, A-weighted		
MCU.REQ.027	MIC/LINE Input	Input sensitivity: 5mV/1V, set by DIP switch		
MCU.REQ.028	MIC/LINE Input	Input impedance: 20 KΩ		
MCU.REQ.029	MIC/LINE Input	Frequency response: 80Hz-18KHz, ±3dB		
MCU.REQ.030	MIC/LINE Input	SNR: >80dB, A-weighted		
MCU.REQ.031	Audio Output	Phantom power output: 24V DC, set by DIP switch		
MCU.REQ.032	Audio Output	Output channels: CH1, CH2 and record		
MCU.REQ.033	Audio Output	Output signal : 1V (0dBV)		
MCU.REQ.034	Internal Power Amplifier	THD: <0.1%		
MCU.REQ.035	Internal Power Amplifier	Max. power output: 500W		
MCU.REQ.036	Internal Power Amplifier	Output signal: 100V(CH1A)		
MCU.REQ.037	Internal Power Amplifier	Frequency response: 80Hz-18KHz, ±3dB		
MCU.REQ.038	Loudspeaker Interface	Control signal: Self-testing, amplifier fault and power saving control signal		
MCU.REQ.039	Loudspeaker Interface	Zone Number: 8 (each has A and B output)		
MCU.REQ.040	Contact Input / Output	Maximum voltage of the outputs: AC 250V/DC 30V		
MCU.REQ.041	Working Conditions	Memory capacity: 1GB Flash Memory, 4GB SD card		
MCU.REQ.042	Working Conditions	Relative Humidity: < 95%, without condensing		
MCU.REQ.043	Working Conditions	Operating temperature: -10°C~+50°C(14°F to +122°F)		
MCU.REQ.044	Specification	Storage temperature: -40°C~+70°C(-40°F to +158°F)		
MCU.REQ.045	500W Class-D Power Amplifier	The amplifier shall provide 70/100V loudspeaker output voltages that are galvanically separated. The amplifier shall be permanently monitored by the master control unit.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>MCU.REQ.046</b>	500W Class-D Power Amplifier	The amplifier shall have 1 x 100V audio input to support remote audio transmission.		
<b>MCU.REQ.047</b>	500W Class-D Power Amplifier	The amplifier shall have automatic restoring functions when the amplifier is taking over current level from external audio source in standalone mode.		
<b>MCU.REQ.048</b>	500W Class-D Power Amplifier	System control and audio shall be transmitted via RJ45 connectors		
<b>MCU.REQ.049</b>	500W Class-D Power Amplifier	The amplifier shall be used as a system amplifier, but it shall also be possible to use the amplifier standalone. No other type of amplifiers shall be allowed to use with other system components.		
<b>MCU.REQ.050</b>	500W Class-D Power Amplifier	The HAM-2000 amplifier shall be an CE, CB and CCCF compliant		
<b>MCU.REQ.051</b>	Product Features	Supports both balanced and unbalanced audio input.		
<b>MCU.REQ.052</b>	Product Specifications	Main power supply : AC 220V-240V 50/60Hz		
<b>MCU.REQ.053</b>	Product Specifications	Backup power supply: AC 220V-240V 50/60Hz		
<b>MCU.REQ.054</b>	Product Specifications	Power consumption: <720W		
<b>MCU.REQ.055</b>	Product Specifications	Fuse: T10AH 250V		
<b>MCU.REQ.056</b>	Product Specifications	DA output: 70V / 100V		
<b>MCU.REQ.057</b>	Product Specifications	Max. output power: 500W		
<b>MCU.REQ.058</b>	Remote Call Station	Up to 6 call station shall be connected into per system. Each call station shall be extendible with 8 extension key pads (8 keys per keypad). The transmission distance shall be within 600m.		
<b>MCU.REQ.059</b>	Remote Call Station	I The call station shall have 16 keys on the front plate. 8 of them shall be functional keys and audio selection. The other 8 of them shall be configurable for both loudspeaker line, loudspeaker lines group, audio tasks or operations such as volume control.		
<b>MCU.REQ.060</b>	Remote Call Station	I The call station shall have optional gooseneck or PTT microphone. The jack shall be automatic adaptive to gooseneck or PTT microphone.		
<b>MCU.REQ.061</b>	Remote Call Station	The call station shall be fully supervised by master controller in terms of communication and		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		physical connection of microphone inputs and keypads. Any faults shall be shown by both indicators on the front plate and the master control unit.		
<b>MCU.REQ.062</b>	Remote Call Station	The microphone input shall have automatic gain control features and the sensitivity is adjustable to actual requirement.		
<b>MCU.REQ.063</b>	Remote Call Station	The call station shall have one emergency key with plastic closure for emergency mode switch during emergency. It shall be programmable as one button operation to deliver emergency message to defined zones by pushing the key.		
<b>MCU.REQ.064</b>	Remote Call Station	The call station shall have AUX audio inputs to connect with external audio source and the external audio shall be able to route over the entire system communication. Gain of the input shall be adjustable.		
<b>MCU.REQ.065</b>	Remote Call Station	The connection between call stations shall be cascaded. The master control unit shall have dual communication ports to support two direction star type linkage.		
<b>MCU.REQ.066</b>	Remote Call Station	There shall be a built-in recorder allowing user to record paging task from PTT and allowing temporarily record task up to 60 minutes. The temporary task shall be auditable before delivery and shall be able to set repeating cycle.		
<b>MCU.REQ.067</b>	Remote Call Station	The call station shall be powered by 24V adapter or master controller, within 400m, the Master controller shall deliver audio, control, supervision and 24V power to call station.		
<b>MCU.REQ.068</b>	Product Features	The mechanical design of call station shall be adaptive to desktop placement or rackmount.		
<b>MCU.REQ.069</b>	Product Features	Supports gooseneck or PTT microphone for live announcement.		
<b>MCU.REQ.070</b>	Product Features	Built-in loudspeaker to monitor CH1/CH2 audio.		
<b>MCU.REQ.071</b>	Product Features	Temporary recording function.		
<b>MCU.REQ.072</b>	Product Features	Line input interface to connect to external BGM audio source.		
<b>MCU.REQ.073</b>	Product Features	The volume of microphone, line input and loudspeaker can be set		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		via the volume regulators at the rear panel.		
<b>MCU.REQ.074</b>	Product Features	8 programmable buttons, can be configured by software.		
<b>MCU.REQ.075</b>	Product Features	Supports extension key modules as required.		
<b>MCU.REQ.076</b>	Product Features	Automatic supervision of microphone and communication.		
<b>MCU.REQ.077</b>	Product Features	The distance between Master Controller and Call station shall be up to 600 meters via twisted-pair cable.		
<b>MCU.REQ.078</b>	Product Features	Call station can be powered by Master Controller.		
<b>MCU.REQ.079</b>	Product Specifications	Maximum 6 remote call stations can be connected to the system.		
<b>MCU.REQ.080</b>	Product Specifications	Power supply: 24V DC		
<b>MCU.REQ.081</b>	Microphone	Power consumption: 10 W		
<b>MCU.REQ.082</b>	Microphone	Sensitivity: -50dB±3dB		

#### 17.40 "Technical Requirements Specifications - Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp "

Product Name: Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DT.REQ.001</b>	The two winding Distribution Transformer shall be Mineral oil immersed transformers shall conform to IS 1180 (Efficiency Level 1) and Mineral Oil filled transformer and shall have following specifications: This specification covers design, engineering, manufacture; shop testing, inspection, painting, packing, and supply of Distribution Transformers complete with all accessories for efficient and trouble-free operation of the proposed Substation.		
<b>DT.REQ.002</b>	The design, manufacture and performance of equipment shall comply with all currently applicable statutes, regulations and safety codes in the locality where the equipment will be installed. Nothing in this specification shall be construed to relieve the VENDOR of this responsibility. The Quality of Raw material, Manufacturing process & design parameters should meet the requirement so as to ensure quality of transformers		
<b>DT.REQ.003</b>	The equipment shall conform to the latest edition of applicable standards as follows. In case of conflict between applicable standards and this specification, this specification shall govern. . IS:1180, for Tests & tolerance on Guaranteed Particulars . IS:3639 for Fittings and Accessories . IS:2099 for Bushings > 1000 V		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	. IS:7421 for Bushings < 1000 V . IS:1271 for Electrical Insulation classified by Thermal stability		
<b>DT.REQ.004</b>	All material used shall be of best quality and of the class most suitable for working under the conditions specified and shall withstand the variations of temperature and atmospheric conditions, overloads, over excitation, short-circuits as per specified standards, without distortion or deterioration or the setting up of undue stresses in any part, and also without affecting the strength and suitability of the various parts for the work which they have to perform.		
<b>DT.REQ.005</b>	All material used shall be of best quality and of the class most suitable for working under the conditions specified and shall withstand the variations of temperature and atmospheric conditions, overloads, over excitation, short-circuits as per specified standards, without distortion or deterioration or the setting up of undue stresses in any part, and also without affecting the strength and suitability of the various parts for the work which they have to perform.		
<b>DT.REQ.006</b>	The exterior of tank and other steel surfaces exposed to the weather shall be thoroughly cleaned and have a priming coat of zinc chromate applied. The second coat shall be of an oil and weather-resistant nature, preferably of distinct colour from the prime and finish coats. The final coat shall be of a glossy, oil and weather resisting non-fading paint of specified shade. The interior of the tank shall be cleaned by shot blasting and painting with two coats of heat resistant and oil insoluble paint		
<b>DT.REQ.007</b>	Steel bolts and nuts exposed to the atmosphere shall be galvanized.		
<b>DT.REQ.008</b>	Unless otherwise stated, the tank together with radiators, conservator, bushings and other fittings shall be designed to withstand without permanent distortion the following conditions:		
<b>DT.REQ.009</b>	Full vacuum of 760 mm of Hg, for filling with oil by vacuum.		
<b>DT.REQ.010</b>	Internal gas pressure of 0.35 Kg/cm <sup>2</sup> (5 lbs/sq.in) with oil at operating level.		
<b>DT.REQ.011</b>	The tank cover shall be suitably sloped so that it does not retain rain water.		
<b>DT.REQ.012</b>	The material used for gaskets shall be cork neoprene or approved equivalent.		
<b>DT.REQ.013</b>	Transformer shall be double wound ,core type with low loss, non ageing ,high permeability PRIME GRADE , CRGO with M4 Grade or Better, perfectly insulated and clamped to minimize noise and vibrations. Followings should be Mandatory for any Manufacturer :-		
<b>DT.REQ.014</b>	Transformer shall be of BOLTLESS core design		
<b>DT.REQ.015</b>	Core shall be purchased Directly from Manufacturer or from their accredited Marketing organization of		



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	Repute & not through any agent. Bidded has to submit manufacturer's name during bidding having sufficient credential & Core has to be purchased from the approved manufacturer.		
<b>DT.REQ.016</b>	The insulation structure for the core to bolts and core to clamp plates shall be such as to withstand a voltage of 2000V for one minute.		
<b>DT.REQ.017</b>	Winding shall be made with 99.9% pure electrolytic grade copper,insulated with thermally upgraded paper (InsulationClass A / Conductor Interturn insulation Class E). The HV & LV winding should be able withstand thermal and mechanical stress in the event of short circuit.		
<b>DT.REQ.018</b>	Transformer oil shall be as per IS 335.		
<b>DT.REQ.019</b>	One set of winding temperature indicators with necessary current transformer, heating coil and a detector element and one set of oil temperature indicator with maximum reading pointer shall be mounted locally so as to be readable at a standing height from ground level. Each of the above indicators shall be provided with necessary contacts for alarm and trip As per IS 1180		
<b>DT.REQ.020</b>	The Buchholz relay shall be provided with two floats and two pairs of electrically separate contacts for alarm and trip. The relay shall have facility for testing by injection of air by hand pump and with cock for draining and venting of air. The location of the relay shall be such that all rising gas will readily reach it.		
<b>DT.REQ.021</b>	All bushings shall be homogenous, solid porcelain oil commissioning type, uniformly glazed and free from blisters, burns and other defects and shall be furnished complete with suitable terminal connectors of adequate capacity. The bushings shall be located so as to provide necessary electrical clearances between phases and also between phase and ground as specified in relevant standards		
<b>DT.REQ.022</b>	Bushings rated for 400A and above shall have non-ferrous flanges and hardware		
<b>DT.REQ.023</b>	All bushings shall have puncture strength greater than the dry flashover value		
<b>DT.REQ.024</b>	Neutral CTs shall be furnished with its secondary leads wired upto the terminal blocks. The terminals for CT secondary leads shall have provision for shorting. The arrangement shall be such that the CT can be removed from the transformer without removing the tank cover.		
<b>DT.REQ.025</b>	Low voltage terminals of Power transformer shall be brought out to bushing inside Cable Box and Cable shall be provided with Bus Bar Arrangement so that atleast 8 Nos. 400sqmm 3.5 Core Aluminum cables can be easily connected in to it.		
<b>DT.REQ.026</b>	High voltage terminals of Power transformer shall be in arrangement to connection of Cable inside cable box		
<b>DT.REQ.027</b>	The cable box shall be suitable for cable termination kits and shall be self-supporting, weather proof, air		



Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	filled type, complete with all hardware such as gland plate, brass glands, tinned copper lugs, armour clamps etc		
<b>DT.REQ.028</b>	A sheet steel weather proof marshaling box of IP 55 construction, shall be mounted on the tank of transformer and shall accommodate all auxiliary devices except those which must be located directly on the transformer. All terminal blocks for external cable connections shall be located in this box.		
<b>DT.REQ.029</b>	Wiring shall be done with HR PVC 650 V grade wires. The wire size for CT circuits shall be 4 mm <sup>2</sup> copper and for other circuits shall be a minimum of 2.5 mm <sup>2</sup> copper. Not more than two (2) wires shall be connected to a terminal. 10% spare terminals shall be provided.		
<b>DT.REQ.030</b>	All devices and terminal blocks within the marshalling box shall be identified by symbols corresponding to those used in applicable schematic or wiring diagrams.		
<b>DT.REQ.031</b>	Two grounding pads, located on the opposite sides of the tank, shall be provided for connection of Switchyard ground mat for each transformer. Grounding pads shall have clean buffed surface with tapped holes. M10 G.I. bolts, nuts and spring washer shall be provided.		
<b>DT.REQ.032</b>	2 Nos. Ground terminals each shall also be provided on marshalling box, cable box & OLTC panel to ensure effective earthing.		
<b>DT.REQ.033</b>	The Neutrals of the windings shall be brought out through neutral bushings at suitable location. The neutrals shall be suitable for connecting 75x10 mm Copper flat.		
<b>DT.REQ.034</b>	For conductivity of earth connection, all gasketed joints shall be provided with minimum two nos. of copper strip of adequate size.		
<b>DT.REQ.035</b>	The OLTC gear shall be designed to complete successfully tap changes for the maximum current to which transformer can be loaded i.e. 150% of the rated current. Devices shall be incorporated to prevent tap change when the through current is in excess of the safe current that the tap changer can handle. The OLTC gear shall withstand through fault currents without injury.		
<b>DT.REQ.036</b>	When a tap change has been commenced it shall be completely independently of the operation of the control relays and switches. Necessary safeguard shall be provided to allow for failure of auxiliary power supply or any other contingency which may result in the tap changer movement not being completed once it is commenced.		
<b>DT.REQ.037</b>	Oil in compartments which contain the making and breaking contacts of the OLTC shall not mix with oil in other compartments of the OLTC or with transformer oil. Gases released from these compartments shall be conveyed by a pipe to a separate oil conservator or to a segregated compartment within the main transformer		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	conservator. An Oil surge relay shall be installed in the above pipe. The conservator shall be provided with a prismatic oil level gauge		
<b>DT.REQ.038</b>	Oil, in compartments of OLTC which do not contain the make and break contacts, shall be maintained under conservator head by valve pipe connections. Any gas leaving these compartments shall pass through the Buchholz relay before entering the conservator.		
<b>DT.REQ.039</b>	Oil filled compartments shall be provided with filling plug, drain valve with plug, air release vent, oil sampling device, inspection opening with gasketed and bolted cover with lifting handles.		
<b>DT.REQ.040</b>	OLTC driving mechanism and its associated control equipment (local) shall be mounted in an outdoor, weatherproof cabinet with IP 55 protection which shall Include: -		
<b>DT.REQ.041</b>	Driving motor (415V, 3-phase, 50 Hz. AC squirrel cage).		
<b>DT.REQ.042</b>	Motor starting contactor with Motor Protection Circuit Breaker, isolating switch and HRC fuses.		
<b>DT.REQ.043</b>	Mechanical tap position indicator showing rated tap voltage against each position and resettable maximum and minimum indicators.		
<b>DT.REQ.044</b>	Limit switches to prevent motor over-travel in either direction and final mechanical stops.		
<b>DT.REQ.045</b>	Brake or clutch to permit only one tap change at a time on manual operation		
<b>DT.REQ.046</b>	Emergency manual operating device (hand crank or hand wheel).		
<b>DT.REQ.047</b>	A five-digit operation counter.		
<b>DT.REQ.048</b>	Electrically interlocked reversing contactors (preferably also mechanically interlocked).		
<b>DT.REQ.049</b>	240V, 50 Hz. AC space heater with switch and HRC fuses.		
<b>DT.REQ.050</b>	Interior lighting fixture with lamp door switch and HRC fuses.		
<b>DT.REQ.051</b>	Gasketed and hinged door with locking arrangement		
<b>DT.REQ.052</b>	Terminal blocks, internal wiring, earthing terminals and cable glands for power and control cables.		
<b>DT.REQ.053</b>	Necessary relays, contactors, current transformers etc		
<b>DT.REQ.054</b>	Control requirements for OLTC: The following electrical control features shall be provided:		
<b>DT.REQ.055</b>	Positive completion of load current transfer, once a tap change has been initiated, without stopping on any intermediate position, even in case of failure of external power supply.		
<b>DT.REQ.056</b>	Only one tap change from each tap change impulse even if the control switches or push button is maintained in the operated position.		
<b>DT.REQ.057</b>	Cut-off of electrical control when manual control is resorted to. Cut-off of a counter impulse for a reverse tap change until the mechanism comes to rest and resets the circuits for a fresh operation		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DT.REQ.058</b>	Cut-off of electrical control when it tends to operate the tap beyond its extreme position.		
<b>DT.REQ.059</b>	Automatic Control of OLTC: Automatic OLTC control shall include the following items		
<b>DT.REQ.060</b>	Voltage setting device.		
<b>DT.REQ.061</b>	Voltage sensing and voltage regulating devices.		
<b>DT.REQ.062</b>	Line drop compensator with adjustable R and X elements.		
<b>DT.REQ.063</b>	Timer 5-25 seconds for delaying the operation of the tap changer in the first step for every tap change operation.		
<b>DT.REQ.064</b>	Adjustable dead band for voltage variation.		
<b>DT.REQ.065</b>	RTCC Panel:		
<b>DT.REQ.066</b>	The OLTC remote control equipment shall be suitable for 30V DC supply and shall be housed in an indoor sheet cubicle to be located in a remote control room. The OLTC control panel shall comprise of rigid welded structural frames made of structural steel section or of pressed and formed cold rolled steel and frame enclosures, doors and partitions shall be of cold rolled steel of thickness 2 mm.		
<b>DT.REQ.067</b>			
<b>DT.REQ.068</b>	Stiffeners shall be provided wherever necessary. All doors, removable covers and plate shall be gasketed all around with neoprene gaskets. Panel shall be dust, weather and vermin proof providing degree of protection of IP54, colour of finish shade for interior and RAL7032 respectively. Earthing bus shall be of 25 x 6 mm copper. exterior shall be Powder Coated		
<b>DT.REQ.069</b>	Lamp indications for:		
<b>DT.REQ.070</b>	1 Tap change in progress		
<b>DT.REQ.071</b>	2 Lower limit reached		
<b>DT.REQ.072</b>	3 Upper Limit reached		
<b>DT.REQ.073</b>	4) Cable glands for power and control cables		
<b>DT.REQ.074</b>	5) 240 V rated panel space heater with ON-OFF switch		
<b>DT.REQ.075</b>	6) Fluorescent type interior lighting fixture with lamp and door switch		
<b>DT.REQ.076</b>	7) HRC fuses		
<b>DT.REQ.077</b>	8) Terminal blocks		
<b>DT.REQ.078</b>	9) Internal wiring		
<b>DT.REQ.079</b>	10) Earthing terminal		
<b>DT.REQ.080</b>	11) Supply ON Indication Lamp		
<b>DT.REQ.081</b>	12) Labels for Accessories.		
<b>DT.REQ.082</b>	13) Automatic Voltage Regulating Relay.		
<b>DT.REQ.083</b>	14) Heater Switch (Rotary Type)		
<b>DT.REQ.084</b>	15) Control Supply Switch (Rotary Type)		
<b>DT.REQ.085</b>	16) Hooter for Facia annunciator (230V AC)		
<b>DT.REQ.086</b>	17) Time Delay Relay for 'Tap Change Delayed' (110V AC)		
<b>DT.REQ.087</b>	18) H.V. Voltmeter (Digital Type)		
<b>DT.REQ.088</b>	19) H.V. Voltmeter Selector Switch (Rotary Type)		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DT.REQ.089</b>	20) L.V. Voltmeter (Digital Type)		
<b>DT.REQ.090</b>	21) L.V. Voltmeter Selector Switch (Rotary Type)		
<b>DT.REQ.091</b>	22) PT for AVR.		
<b>DT.REQ.092</b>	23) Tap changer Counter for registering		
<b>DT.REQ.093</b>	Every valve shall be provided with open/close position indicators. The valves shall be suitable for pad locking in open/close positions. All screwed valves shall be furnished with pipe plugs for protection.		
<b>DT.REQ.094</b>	All valves shall be provided with flanges having machined faces drilled to suit the applicable requirements.		
<b>DT.REQ.095</b>	Oil tight blank flanges shall be provided for the following.		
<b>DT.REQ.096</b>	valves opening to atmosphere for each connection for use when any radiator is detached.		
<b>DT.REQ.097</b>	Any special radiator valves tools required shall be supplied by the MSI.		
<b>DT.REQ.098</b>	The Transformer shall provide with Nitrogen Fire Protection system so as to envisage complete safety from Fire Hazards		
<b>DT.REQ.099</b>	ROUTINE TESTS – The manufacturer should have NABL accredited test lab.		
<b>DT.REQ.100</b>	a. Measurement of winding resistance		
<b>DT.REQ.101</b>	b. Measurement of voltage ratio and check of voltage vector relationship		
<b>DT.REQ.102</b>	c. Measurement of impedance of voltage (principal tapping), short circuit impedance and load loss.		
<b>DT.REQ.103</b>	d. Measurement of no load loss and current		
<b>DT.REQ.104</b>	e. Separate source voltage withstand test		
<b>DT.REQ.105</b>	f. Induced overvoltage withstand test (2 times the rated voltage)		
<b>DT.REQ.106</b>	g. 2kV withstand test for all wiring		
<b>DT.REQ.107</b>	h.Magnetic Balance Test.		
<b>DT.REQ.108</b>	i. Separate source voltage withstand test f.Induced overvoltage withstand test (2 times the rated voltage)		
<b>DT.REQ.109</b>	j .2kV withstand test for all wiring h.Magnetic Balance Test.		
<b>DT.REQ.110</b>	k . Pressure & Vacuum test needs to carried out on 1unit of each rating		
<b>DT.REQ.111</b>	l . Noise level test needs to carried out on 1 unit of each rating.		
<b>DT.REQ.112</b>	Losses shall be as follows :-		
<b>DT.REQ.113</b>	Respective Current density &Flux Density shall be so as to suit the above required No load & loss levels		
<b>DT.REQ.114</b>	All the measurement of losses shall be carried out by digital meters of class 0.5or better accuracy and should be certified by the manufacturer. If the losses measured are found to be out of tolerance band as stated in Standard and guaranteed losses declared by manufacturer , the same shall be attributed to the manufacturer as per capitalization formula till the end of warranty period . In extreme conditions the		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	customer has got holds absolute rights to reject the lot and terminate the contract of vendor		
<b>DT.REQ.115</b>	One transformer of each rating , selected randomly from the lot shall to send for measurement of losses , declared by vendor ( on data sheet) at third party / any NABL accredited lab.. In case loss figures deviates more than tolerances specified in IS 1180, purchaser reserves rights of terminating the contract of vendor		
<b>DT.REQ.116</b>	ACCEPTANCE TESTS( Manufacturer should have NABL accredited test laboratory)		
<b>DT.REQ.117</b>	One transformer of each rating, selected randomly from the lot shall to sent For measurement of losses , declared by vendor ( on data sheet) at third party / any NABL accredited lab.. In case loss figures deviates more than tolerances specified in IS 1180 , purchaser reserves rights of terminating the contract of vendor		
<b>DT.REQ.118</b>	Oil Leakage test for acceptance shall be conducted at pressure of 0.35kg/sq.cm for one hour		
<b>DT.REQ.119</b>	Checking of weights, Dimensions, fitting and accessories, tank sheet thickness, oil quantity, material, finish and workmanship, Physical verification of core coil assembly and measurement of flux density on one unit of each rating of the offered lot with reference to the GTP and contract drawings		
<b>DT.REQ.120</b>	Temperature rise test on one transformer selected randomly to be sent at NABL accredited		
<b>DT.REQ.121</b>	lab at Manufacturer's cost . IF transformers fails the test or found to be under rated the contract		
<b>DT.REQ.122</b>	shall ne terminated and the manufacturer will be black listed		
<b>DT.REQ.123</b>	PURCHASER may reject any transformer if during tests or service any of the following conditions arise:		
<b>DT.REQ.124</b>	No load loss exceeds the guaranteed value greater than tolerance limit mentioned in IS1180		
<b>DT.REQ.125</b>	Load loss exceeds the guaranteed value greater than tolerance limit mentioned in IS1180		
<b>DT.REQ.126</b>	Impedance value differs the guaranteed value by + 10% or more		
<b>DT.REQ.127</b>	Winding temperature rise exceeds the specified value by 5°C		
<b>DT.REQ.128</b>	Transformer fails on impulse test		
<b>DT.REQ.129</b>	Transformer fails on power frequency voltage withstand test		
<b>DT.REQ.130</b>	Transformer is proved to have been manufactured not in accordance with the agreed specification		
<b>DT.REQ.131</b>	The PURCHASER reserves the right to retain the rejected transformer and take it into service until the SELLER replaces, at no extra cost to PURCHASE, the defective transformer by a new acceptable transformer.		
<b>DT.REQ.132</b>	The Bidder shall carried out following Pre Commissioning Checks at site after Installation but before commissioning of Transformer all These Tests		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	shall be carried out free of cost by the bidder and no extra cost shall be paid		
<b>DT.REQ.133</b>	Visual Check of Transformer		
<b>DT.REQ.134</b>	Transformer Level in Conservator Tank		
<b>DT.REQ.135</b>	IR Values test		
<b>DT.REQ.136</b>	Ratio Check		
<b>DT.REQ.137</b>	Winding Resistance Test		
<b>DT.REQ.138</b>	Magnetic Current Check (HV & LV Both)		
<b>DT.REQ.139</b>	Vector Group Check		
<b>DT.REQ.140</b>	OTI/WTI/Buchholz Tip & Alarm Check		
<b>DT.REQ.141</b>	PRV Trip Check		
<b>DT.REQ.142</b>	Low Level Alarm Check		
<b>DT.REQ.143</b>	Operation of OLTC & RTCC		

#### 17.41 "Technical Requirements Specifications - Advance Building Management System (BMS)"

Product Name: Advance Building Management System (BMS)

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>BMS.REQ.001</b>	<b>OBJECTIVE</b>	The objective is to install a Building Management System to control HVAC installed at data center. and Monitoring the unit like LT Panels, HT Panels, UPS, Energy Meters, BTU Meters, Water Meters, Fire Fighting Pumps, PAC units and any other third party units. solution should control, Monitor, Data logging, History viewing, Alarm Generation and viewing with Graphics view. The purpose of the system to control and monitor all building related units under one place.		
<b>BMS.REQ.002</b>	<b>OBJECTIVE</b>	Building Automation System (BAS/BMS) comprises the control and monitoring functionality of mechanical (heating, ventilation and air conditioning) and electrical systems in a building. The core functionality of Building Automation (BAS/BMS) should keep the building climate within a specified range, provides schedule, monitors system performance and device		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		failures, and provides notifications to building facility staff.		
<b>BMS.REQ.003</b>	<b>OBJECTIVE</b>	The typical scope of BAS/BMS contains control and monitoring of mechanical and electrical systems, including cooling/heating system, ventilation system, pumps, tanks, lifts and often also consumption metering.		
<b>BMS.REQ.004</b>	<b><u>REFERENCE STANDARDS</u></b>	<ul style="list-style-type: none"> <li>•ASHRAE 35-2001, BACnet or equivalent</li> <li>•Standard 135-2004 – BACnet or equivalent</li> <li>•BTL or equivalent</li> </ul>		
<b>BMS.REQ.005</b>	<b>General Requirement</b>	The Integrated Software Platform (ISWP) shall coordinate and integrate with all Extra Low Voltage Building Systems to ensure that data exchange between the various ELV building systems meet the project requirements. The ISWP shall have the common GUI, database and data storage, application program and operating systems. This ISWP shall be a gateway between systems enabling the transfer of relevant information between the systems in the appropriate protocols.		
<b>BMS.REQ.006</b>		The ISWP shall provide both client and server functions; the ISWP shall request information from the various ELV buildings communicating on the Common LAN. The ISWP shall determine the routing of all data between systems, the ISWP shall determine which system shall be the recipients of the data based on the nature of the data, and all data transferred from one system to another shall be routed via the ISWP.		
<b>BMS.REQ.007</b>		The ELV building systems have its own monitoring and control mechanism. The required information like alarm, control point, set temperature, etc. will be		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		transferred to the ISWP. The ISWP shall have responsibility for providing an interoperable system that enables the sharing of information between the ELV building systems.		
<b>BMS.REQ.008</b>		The ISWP shall at minimum support the following protocols over the TCP/IP backbone: 1. BACnet (Server/ Client) 2. LonTalk 3. MODBUS (Master/Slave) 4. SNMP 5. MQTT 6. SOAP (Server Client) 7. OPC (Server Client) 8. KNX 9. M-Bus/IP 10. Other Industrial standard protocols		
<b>BMS.REQ.009</b>		The software shall be capable to accept at least BACNET/IP, MODBUS/IP, LONWORKS/IP, M-Bus/IP and SNMP without any additional software driver or any additional hardware. Manufacturers who do not have this inbuilt capability need to provide a separate converter for each of the above protocols for ease of openness in the future else their system shall be unacceptable.		
<b>BMS.REQ.010</b>		The ISWP shall be based on a Java-based framework. The framework shall provide an open automation infrastructure that integrates diverse systems and devices (regardless of manufacturer, communication standard or software) into a unified platform that can be easily managed in real time over Intranets or Internet using a standard Web browser. Systems not developed on Java based framework platform are unacceptable.		
<b>BMS.REQ.011</b>		The ISWP should provide a common design language for a unified experience between desktop, tablet and mobile. It		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		shall serve real-time graphical information to standard Web-browser clients and provide server-level functions. These functions include centralized data logging/trending, archiving to external databases, alarming, customizable dashboards, system navigation, master scheduling, database management, and integration with other enterprise software applications through an XML interface. Also, it shall provide a comprehensive graphical engineering toolset for application development.		
	<b>BMS.REQ.012</b>	The ISWP shall be a comprehensive component model with a structure that serves as a foundation for building applications and integrating diverse connected systems. Through graphical programming and open APIs, the component model shall provide a method of modelling the data and attributes of diverse connected systems, while at the same time provide a method of modelling and creating the end applications delivered to the end user.		
	<b>BMS.REQ.013</b>	The manufacturer should provide a unified engineering tool for Control strategy, Network management, visualization graphics, Integration configuration and Data analytics set-up. This unified engineering tool should be handed over to the end client during the handing over process to ensure independence from the system integrator and manufacturer.		
	<b>BMS.REQ.014</b>	The following key application areas must be supported by the ISWP at a minimum: Scalable and distributed architecture, Unified Software Environment,		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		Extensibility, Integrated Control Engine and Web services.		
<b>BMS.REQ.015</b>		The mechanical and electrical systems shall be controlled and monitored by smart, Direct IP based BMS controllers. The BMS controllers shall provide for capability of control and monitoring of all mechanical and electrical systems, including cooling/heating system, ventilation system, pumps, tanks, lifts, energy meters and other electrical equipment at the minimum but not limited to above mentioned systems.		
<b>BMS.REQ.016</b>		BMS controllers shall be freely programmable and shall include the full intelligence for system functionality and to be capable of operating independently without interference from management applications. BMS controllers shall be easily expandable with I/O expansion units.		
<b>BMS.REQ.017</b>		BMS controllers shall support distributed intelligence and centralized system designs alike. It shall be possible to distribute BMS controllers at electrical switchboards or cabinets close to the controlled system to minimize cabling.		
<b>BMS.REQ.018</b>		Each BMS controller shall support standard field bus connectivity over BACnet/IP. Controllers shall contain at least the following communication interfaces: BACnet/IP, BACnet MS/TP, Modbus RTU. The BACnet MS/TP and Modbus RTU should be pre enabled for integration with any 3rd party devices using the mentioned protocols. This is to ensure reduction in cabling costs and ease of commissioning. Manufacturers who do not have an inbuilt enabled port		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		need to provide a separate BACnet MS/TP to BACnet/IP or Modbus RTU to BACnet/IP Converter else their system shall be unacceptable. Any failure problem in communication bus should not affect the operation of the controller.		
	<b>BMS.REQ.019</b>	BMS controllers shall be capable of using both 24VAC and 24VDC as operating voltage. BMS controllers shall support user friendly operation and maintenance by having clearly visible LED:s in the front panel to indicate status of the controller, communication, etc and status of digital output points..		
	<b>BMS.REQ.020</b>	The controllers must communicate on open protocols such as BACNET/IP, MODBUS/IP only. Any propriety protocols like C-Bus, J-Bus, ARCNET, Linknet shall not be permitted. Else their system shall be unacceptable.		
	<b>BMS.REQ.021</b>	The controller must be BTL Listed under the BACnet Advanced Application Controller (B-AAC) and BACnet Router (B-RTR) category.		
	<b>BMS.REQ.022</b>	Each BMS controller involved in process controls shall contain flexible I/O points (each controller including a set of universal inputs and outputs) with freely configurable software functions. Each controller shall be capable of handling I/O point belonging to different systems to enable flexible distribution of I/O points throughout the whole system.		
	<b>BMS.REQ.023</b>	The I/O points shall support the following features. <ul style="list-style-type: none"> <li>• DI: Digital input, potential free contact</li> <li>• AI: Analog input</li> </ul> Voltage: 0 - 10V, 0 - 5V Current: 4 - 20mA ,0 - 20mA		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		Resistance: 0 - 30K , 0 - 10K, 0 - 1.5K Thermistor Sensor: NTC: 10K TYPE 2/3, 3K, 20K ( $\pm 0.1$ °C) RTD: 1K Balco, 1K Platinum ( $\pm 0.2$ °C) • DO: Digital output, Relay output • AO: Analog output Voltage: 0 - 10V Current: 0 - 20mA, 4 - 20mA (Max load resistance 800 ohms)		
<b>BMS.REQ.024</b>		The BMS controllers shall include freely programmable and configurable software functions to implement complex engineering system process controls. These functions shall include PID controllers and thermostat (ON/OFF controller) functions for implementing the control loops used in process controls, as well as sequencing functionality for sets of devices controlled in sequence (e.g. pumps, fans). Logical functions (for example AND and OR logical gates) shall be integral part of the configurable software in the BMS controllers. The controllers shall have soft PID loops that can be defined from the software.		
<b>BMS.REQ.025</b>		The BMS controllers shall have numbered connection strips for easy installation. The BMS controllers shall support mounting in DIN rail and directly on the panel.		
<b>BMS.REQ.026</b>		Configuration of BMS controllers shall be done through a graphical system configuration tool.		
<b>BMS.REQ.027</b>	<b>Cables &amp; Containment</b>	Cabling shall be with copper multi stranded conductor Cables with conductor cross section 1 sq.mm suitable to the length of loop/type of sensor used as per manufacturer's specs.		
<b>BMS.REQ.028</b>	<b>Cables &amp; Containment</b>	Cable shall be laid on surface / true ceiling slab with GI saddle & spacers		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		with required MS powder coated / galvanized junction boxes, single compression Glands and necessary ferrules & tags.		
<b>BMS.REQ.029</b>	<b>Cables &amp; Containment</b>	Any vertical movement of unexposed Cables shall be through GI perforated cable trays. Multiple cable drops for exposed cables terminating in all Panels shall be through MS Powder coated Trunks.		

#### 17.42 "Technical Requirements Specifications - Dome Camera"

Product Name: Dome Camera

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DOMCAM.REQ.001</b>	<b>OBJECTIVE</b>	1/2.8" progressive scan CMOS or better		
<b>DOMCAM.REQ.002</b>	<b>OBJECTIVE</b>	2560x1920@30fps or better		
<b>DOMCAM.REQ.003</b>	<b>OBJECTIVE</b>	128kbps~16Mbps or better		
<b>DOMCAM.REQ.004</b>	<b><u>REFERENCE STANDARDS</u></b>	Data rate should be independently configurable for each video stream		
<b>DOMCAM.REQ.005</b>	<b>General Requirement</b>	3 video streams or better		
<b>DOMCAM.REQ.006</b>	Sensitivity	Color mode: 0.005 lux (IR OFF) or better		
<b>DOMCAM.REQ.007</b>	a) Colour Mode	B/W mode: 0.0005 lux (IR OFF) or better		
<b>DOMCAM.REQ.008</b>	b) Monochrome mode	0 lux (IR ON)		
<b>DOMCAM.REQ.009</b>	Exposure Control	Auto/Manual/Shutter		
<b>DOMCAM.REQ.010</b>	Shutter	1/1s~1/30000s or better		
<b>DOMCAM.REQ.011</b>	"Wide Dynamic	up to 128 dB or better		
<b>DOMCAM.REQ.012</b>	Range (WDR) "	The camera shall be Day/Night		
<b>DOMCAM.REQ.013</b>	Day/Night Camera	Motorized zoom lens, F1.6, f=2.8~12mm		
<b>DOMCAM.REQ.014</b>	Lens	50m or better		
<b>DOMCAM.REQ.015</b>	"Infra-Red Night	850 nm or better		
<b>DOMCAM.REQ.016</b>	Vision Distance "	Auto/Manual/Shutter		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DOMCAM.REQ. 017</b>	IR wavelength	up to 4 definable area or better		
<b>DOMCAM.REQ. 018</b>	Focus and Iris Control	IP 67 or better		
<b>DOMCAM.REQ. 019</b>	Privacy Masking	Motion detection, camera tampering, FOV Change, defocus detection, high brightness detection, low brightness detection		
<b>DOMCAM.REQ. 020</b>	Edge Analytics	Support density detection and crowd detection Support queue length monitoring and dwelling detection		
<b>DOMCAM.REQ. 021</b>	Edge Analytics	Wire crossing detection, intrusion detection, left object detection, object Removed detection, loitering detection		
<b>DOMCAM.REQ. 022</b>	Signal to Noise ratio	>65dB		
<b>DOMCAM.REQ. 023</b>	Edge Storage	Supports a Micro SD/SDHC/SDXC card. Camera Shall be supplied with 128 GB card		
<b>DOMCAM.REQ. 024</b>	Network Interface	One RJ45 10/100M self-adaptive Ethernet port		
<b>DOMCAM.REQ. 025</b>	"Camera discovery in local Network	required		
<b>DOMCAM.REQ. 026</b>	Supported protocols	IPv4/IPv6, TCP, UDP, IGMP, ICMP, IGMPv2/3, DHCP, SNMP (V1, V2, V3), FTP, SMTP, NTP, RTP, RTSP, RTCP, HTTP, HTTPS, SSL, 802.1x, QoS, PPPoE, DNS, DDNS, ARP, UPnP, IP Filter, TLS, Multicast, SIP		
<b>DOMCAM.REQ. 027</b>	IP Address Filter	Blacklist and whitelist filtering for up to 1024 IP segments or better		
<b>DOMCAM.REQ. 028</b>	Web Server	Embedded web server		
<b>DOMCAM.REQ. 029</b>	"Maximum Number of Users "	64		
<b>DOMCAM.REQ. 030</b>	Auto, Manual, Outdoor	Minimum 3 types of user's privileges required: administrator, normal user, and operator		
<b>DOMCAM.REQ. 031</b>	Auto Gain Control	Auto, Manual		
<b>DOMCAM.REQ. 032</b>	Back Light Compensation	Required		
<b>DOMCAM.REQ. 033</b>	White Balance	Auto, Manual, Outdoor		
<b>DOMCAM.REQ. 034</b>	Alarm Inputs/Output	2 Alarm Inputs, 1 Output		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
DOMCAM.REQ. 035	Power options	PoE (IEEE 802.3af)/12VDC ( $\pm 20\%$ )/24VAC ( $\pm 25\%$ )		
DOMCAM.REQ. 036	Power Consumption	<6W (IR off),		
DOMCAM.REQ. 037		<13W (IR on)		
DOMCAM.REQ. 038	Operating Temperature	-10C ~ 100C		
DOMCAM.REQ. 039	Storage Temp	-10C ~ 100C		
DOMCAM.REQ. 040	Humidity	0%~95% RH (non-condensing)		
DOMCAM.REQ. 041	Flicker control	required		
DOMCAM.REQ. 042	Defog	required		
DOMCAM.REQ. 043	Highlight Suppression	required		
DOMCAM.REQ. 044	Electronic Image Stabilization (EIS)	Required		
DOMCAM.REQ. 045	Anti-Static	Air discharge up to 8KV or better,		
DOMCAM.REQ. 046		contact protection for ports 6KV		
DOMCAM.REQ. 047	Surge Protection	Difference mode $\pm 2KV$ , common mode $\pm 4KV$ (for network port and power port)		
DOMCAM.REQ. 048	Camera Mount	Mounting bracket shall be part of the camera		
DOMCAM.REQ. 049	ONVIF (Open Network Video	ONVIF Profile S/G/Q		
DOMCAM.REQ. 050	Interface forum) Compliance			
DOMCAM.REQ. 051	Audio	Two-way audio		
DOMCAM.REQ. 052	Audio Compression	G.711 A, G.711 U, G.726, AAC		
DOMCAM.REQ. 053	Audio Sample Rate	8KHz (for G.711-A/G.711-U/G.726),		
DOMCAM.REQ. 054		16KHz, 32KHz, 44.1KHz and 48KHz (for AAC)		
DOMCAM.REQ. 055	Audio Interface	1 Linear input, 1 linear Output		
DOMCAM.REQ. 056	Firmware upgrade	The camera shall support remote firmware upgrade		
DOMCAM.REQ. 057	Regulatory Approvals/ Certifications	CE, FCC, BIS, IP66, IK10		
DOMCAM.REQ. 041	Flicker control	required		
DOMCAM.REQ. 042	Defog	required		
DOMCAM.REQ. 043	Highlight Suppression	required		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>DOMCAM.REQ.044</b>	Electronic Image Stabilization (EIS)	Required		
<b>DOMCAM.REQ.045</b>	Anti-Static	Air discharge up to 8KV or better,		
<b>DOMCAM.REQ.046</b>		contact protection for ports 6KV		
<b>DOMCAM.REQ.047</b>	Surge Protection	Difference mode $\pm 2KV$ , common mode $\pm 4KV$ (for network port and power port)		
<b>DOMCAM.REQ.048</b>	Camera Mount	Mounting bracket shall be part of the camera		
<b>DOMCAM.REQ.049</b>	ONVIF (Open Network Video	ONVIF Profile S/G/Q		

#### 17.43 "Technical Requirements Specifications - Bullet Camera"

Product Name: Bullet Camera

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>BULLCAM.REQ.001</b>	Image Sensor	1/2.8" progressive scan CMOS		
<b>BULLCAM.REQ.002</b>	Resolution	2560x1920@30fps		
<b>BULLCAM.REQ.003</b>	Compression	H.265, H.264, MJPEG		
<b>BULLCAM.REQ.004</b>	Data Rate	128kbps~16Mbps		
<b>BULLCAM.REQ.005</b>		Data rate should be independently configurable for each video stream		
<b>BULLCAM.REQ.006</b>	Video Streaming	3 video streams		
<b>BULLCAM.REQ.007</b>	Sensitivity	Color mode: 0.005 lux (IR OFF);		
<b>BULLCAM.REQ.008</b>	a) Colour Mode	B/W mode: 0.0005 lux (IR OFF);		
<b>BULLCAM.REQ.009</b>	Monochrome Mode	0 lux (IR ON)		
<b>BULLCAM.REQ.010</b>	Exposure Control	Auto/Manual/Shutter		
<b>BULLCAM.REQ.011</b>	Shutter	1/1s~1/30000s		
<b>BULLCAM.REQ.012</b>	"Wide Dynamic Range (WDR)"	up to 128 dB or better		
<b>BULLCAM.REQ.013</b>	Day/Night Camera	The camera shall be Day/Night		



Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>BULLCAM.REQ.014</b>	Lens	Motorized zoom lens, F1.6, f=2.8~12mm		
<b>BULLCAM.REQ.015</b>	"Infra-Red Night Vision Distance "	50m		
<b>BULLCAM.REQ.016</b>	IR wavelength	850 nm		
<b>BULLCAM.REQ.017</b>	Focus & Iris control	Auto		
<b>BULLCAM.REQ.018</b>	Privacy masking	up to 4 definable area		
<b>BULLCAM.REQ.019</b>	Housing	IP67		
<b>BULLCAM.REQ.020</b>	Edge Analytics	Motion detection, camera tampering, FOV Change, defocus detection, high brightness detection, low brightness detection		
<b>BULLCAM.REQ.021</b>	Edge Analytics	Support density detection and crowd detection Support queue length monitoring and dwelling detection		
<b>BULLCAM.REQ.022</b>	Edge Analytics	Wire crossing detection, intrusion detection, left object detection, object Removed detection, loitering detection		
<b>BULLCAM.REQ.023</b>	Signal to Noise ratio	>65dB		
<b>BULLCAM.REQ.024</b>	Edge Storage	Supports a Micro SD/SDHC/SDXC card. Camera Shall be supplied with 128 GB card		
<b>BULLCAM.REQ.025</b>	Network Interface	One RJ45 10/100M self-adaptive Ethernet port		
<b>BULLCAM.REQ.026</b>	"Camera discovery in local Network "	Required		
<b>BULLCAM.REQ.027</b>	"Supported Protocols "	IPv4/IPv6, TCP, UDP, IGMP, ICMP, IGMPv2/3, DHCP, SNMP (V1, V2, V3), FTP, SMTP, NTP, RTP, RTSP, RTCP, HTTP, HTTPS, SSL, 802.1x, QoS, PPPoE, DNS, DDNS, ARP, UPnP, IP Filter, TLS, Multicast, SIP		
<b>BULLCAM.REQ.028</b>	IP Address Filter	Blacklist and whitelist filtering for up to 1024 IP segments or better		
<b>BULLCAM.REQ.029</b>	Web Server	Embedded web server or equivalent		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>BULLCAM.REQ.030</b>	"Maximum Number of Users "	50 or better		
<b>BULLCAM.REQ.031</b>	User Privileges	Minimum 3 types of user's privileges required: administrator, normal user, and operator		
<b>BULLCAM.REQ.032</b>	Auto Gain Control	Auto, Manual		
<b>BULLCAM.REQ.033</b>	"Back Light Compensation "	Required		
<b>BULLCAM.REQ.034</b>	White Balance	Auto,Manual		
<b>BULLCAM.REQ.035</b>	Alarm Inputs/Outputs	2 Inputs, 1 output		
<b>BULLCAM.REQ.036</b>	Power	PoE (IEEE 802.3af)/12VDC ( $\pm 20\%$ )/24VAC ( $\pm 25\%$ )		
<b>BULLCAM.REQ.037</b>	Operating Temperature	-.10 degree celsius to 80 Degree Celsius		
<b>BULLCAM.REQ.038</b>	Storage Temp	-.10 degree celsius to 80 Degree Celsius		
<b>BULLCAM.REQ.039</b>	Humidity	0%~95% RH (non-condensing)		
<b>BULLCAM.REQ.040</b>	Flicker control	required		
<b>BULLCAM.REQ.041</b>	Defog	required		
<b>BULLCAM.REQ.042</b>	"Highlight Suppression "	required		
<b>BULLCAM.REQ.043</b>	Electronic Image Stabilization (EIS)	Required		
<b>BULLCAM.REQ.044</b>	Surge Protection	Difference mode $\pm 2KV$ , common mode $\pm 4KV$ (for		
<b>BULLCAM.REQ.045</b>	Surge Protection	network port and power port)		
<b>BULLCAM.REQ.046</b>	Camera Mount	Mounting bracket shall be provided with camera		
<b>BULLCAM.REQ.047</b>	"ONVIF (Open Network Video			
<b>BULLCAM.REQ.048</b>	Firmware upgrade	The camera shall support remote firmware upgrade		

## 17.44 "Technical Requirements Specifications - PTZ Camera"

Product Name: PTZ Camera

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
PTZCAM.REQ.001	Image Sensor	1/2.8", CMOS		
PTZCAM.REQ.002	Pixel Resolution	1920(H) x 1080(V)		
PTZCAM.REQ.003	Data Rate	Constant Bit Rate		
PTZCAM.REQ.004		Variable Bit Rate varying from 128kbps~10000kbps		
PTZCAM.REQ.005		Each stream should be independently configurable bit rate		
PTZCAM.REQ.006	Compression method	H.265/H.264/M-JPEG/SVC or equivalent		
PTZCAM.REQ.007	Video Streaming	4 independent configurable video streams		
PTZCAM.REQ.008	Sensitivity	Color mode: 0.005 lux (IR OFF);		
PTZCAM.REQ.009	a) Colour Mode	B/W mode: 0.0005 lux (IR OFF);		
PTZCAM.REQ.010	b) Monochrome mode	0 lux (IR ON)		
PTZCAM.REQ.011	Exposure Control	Auto/Manual/Shutter		
PTZCAM.REQ.012	Wide Dynamic Range (WDR) "	up to 128 dB or better		
PTZCAM.REQ.013	Noise Reduction	3D noise reduction		
PTZCAM.REQ.014	Day/Night Camera	ICR		
PTZCAM.REQ.015	Lens	30x		
PTZCAM.REQ.016	Infra Red Night Vision Distance "	150 m or better		
PTZCAM.REQ.017	IR wavelength	850 nm		
PTZCAM.REQ.018	Focus and Iris Control	Auto/Manual/Shutter		
PTZCAM.REQ.019	Privacy Masking	up to 4 definable area		
PTZCAM.REQ.020	Housing	IP 67		
PTZCAM.REQ.021	Edge Analytics	Motion detection, camera tampering, FOV Change, defocus detection, high brightness detection, low brightness detection		
PTZCAM.REQ.022		Support density detection and crowd detection Support queue		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
		length monitoring and dwelling detection		
PTZCAM.REQ .023		Wire crossing detection, intrusion detection, left object detection, object Removed detection, loitering detection		
PTZCAM.REQ .024	Signal to Noise ratio	>60dB		
PTZCAM.REQ .025	Edge Storage	shall support a Micro SD/SDHC/SDXC card. Camera Shall be supplied with Minimum 128 GB card		
PTZCAM.REQ .026	Network Interface	Minimum one RJ45 10/100M self-adaptive Ethernet port		
PTZCAM.REQ .027	"Camera discovery			
in local Network "	required			
PTZCAM.REQ .028	Supported protocols	IPv4/IPv6, TCP, UDP, IGMP, ICMP, IGMPv2/3, DHCP, SNMP (V1, V2, V3), FTP, SMTP, NTP, RTP, Etc. or equivalent		
PTZCAM.REQ .029	IP Address Filter	IP address filtering support		
PTZCAM.REQ .030	Web Server	Embedded web server		
PTZCAM.REQ .031	"Maximum Number of users	10		
PTZCAM.REQ .032	Auto, Manual, Outdoor	Minimum 3 types of user's privileges required: administrator, normal user, and operator		
PTZCAM.REQ .033	Auto Gain Control	Auto, Manual		
PTZCAM.REQ .034	Back Light Compensation	Required		
PTZCAM.REQ .035	White Balance	Auto, Manual, Outdoor		
PTZCAM.REQ .036	Alarm Inputs/Output	2 Alarm Inputs, 1 Output		
PTZCAM.REQ .037	Camera Presets	782 or more		
PTZCAM.REQ .038	Camera Pattern	10 or more		
PTZCAM.REQ .039	Auto pan	10 or more		
PTZCAM.REQ .040	Tour	14		
PTZCAM.REQ .041	Home return of PTZ	Required		
PTZCAM.REQ .042	Auto Scan	Required		
PTZCAM.REQ .043	Area Zoom	Required		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
PTZCAM.REQ .044	Timing tour	Required		
PTZCAM.REQ .045	Manual Pan Speed	0.10~8500/s		
PTZCAM.REQ .046	Manual Tilt Speed	0.10~ 2850/s		
PTZCAM.REQ .047	Preset Speed	Up to 3600/s or better		
PTZCAM.REQ .048	Rotation Angle	Pan: 3600/s or better		
PTZCAM.REQ .049	Rotation Angle	Tilt: -40~ 900(auto-flip)		
PTZCAM.REQ .050	Preset Accuracy	<±0.10		
PTZCAM.REQ .051	Power options	PoE (IEEE 802.3af)/12VDC (±20%)/24VAC (±25%		
PTZCAM.REQ .052	Power Consumption	<6W (IR off),		
PTZCAM.REQ .053	Power Consumption	<13W (IR on)		
PTZCAM.REQ .054	Operating Temperature	-10C ~ 100C		
PTZCAM.REQ .055	Storage Temp	-10C ~ 100C		
PTZCAM.REQ .056	Humidity	0%~95% RH (non-condensing)		
PTZCAM.REQ .057	Flicker control	required		
PTZCAM.REQ .058	Defog	required		
PTZCAM.REQ .059	Highlight Suppression	required		
PTZCAM.REQ .060	Electronic Image Stabilization (EIS)	Required		
PTZCAM.REQ .061	Anti-Static	Air discharge up to 8KV or better,		
PTZCAM.REQ .062	Anti-Static	contact protection for ports 6KV		
PTZCAM.REQ .063	Surge Protection	Difference mode ±2KV, common mode±4KV (for network port and power port)		
PTZCAM.REQ .064	Camera Mount	Mounting bracket shall be part of the camera		
PTZCAM.REQ .065	ONVIF (Open Network Video	ONVIF Profile S/G/Q		
PTZCAM.REQ .066	Interface forum) Compliance			
PTZCAM.REQ .067	Audio	Two-way audio		
PTZCAM.REQ .068	Audio Compression	G.711 A, G.711 U, G.726, AAC		
PTZCAM.REQ .069	Audio Sample Rate	8KHz (for G.711-A/G.711-U/G.726),		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>PTZCAM.REQ.070</b>	Audio Sample Rate	16KHz, 32KHz, 44.1KHz and 48KHz (for AAC)		
<b>PTZCAM.REQ.071</b>	Audio Interface	1 Linear input, 1 linear Output		
<b>PTZCAM.REQ.072</b>	Firmware upgrade	The camera shall support remote firmware upgrade		
<b>PTZCAM.REQ.073</b>	Regulatory Approvals/ Certifications	CE, FCC, BIS, IP66, IK10		

#### 17.45 "Technical Requirements Specifications - Passive cabling"

Product Name: Passive cabling

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>PASSCAB.REQ.001</b>	All Copper/fiber cable and components should be from the same OEM. The OEM should have ISO certificate for the manufacturing facilities related to all products to be used in this solution. Proposed ethernet and optical fiber cable and components should be compatible with the proposed solution		
<b>PASSCAB.REQ.002</b>	All Passive Components should be RoHS (Restriction of Certain Hazardous Substances) compliant. Declaration to be provided for RoHS Compliance		
<b>PASSCAB.REQ.003</b>	There should be 25-year extended performance warranty/Application Assurance for end -to-end channel and should not be any performance degradation/issue during entire contract duration.		
<b>PASSCAB.REQ.004</b>	All the components should comply with their respective specifications stated below.		
<b>PASSCAB.REQ.005</b>	ETL/3P certificates should be present on respective Lab website for all Copper Components		
	<b>Passive Specs for Cat 6A cables and components</b>		
<b>PASSCAB.REQ.006</b>	Cable Should be Cat 6A , 4 Pair Shielded S/FTP Cable		
<b>PASSCAB.REQ.007</b>	Conductor Size : 23 AWG or better		
<b>PASSCAB.REQ.008</b>	Each pair enclosed in Aluminum foil or better		
<b>PASSCAB.REQ.009</b>	Sheath Type: Flame retardant and Low Smoke Zero Halogen (LSZH). ETL/3P certificate to be submitted along with bid		
<b>PASSCAB.REQ.010</b>	Cable shall be UL listed		
<b>PASSCAB.REQ.011</b>	The Cat6A UTP/STP SCS must be tested by Intertek test facility under 4 connector channel to the following standards:		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	ANSI/TIA 568.2-D: Category 6A Channel – 4 connector IEEE 802.3bt PoE upto 60 deg C EN50173 standard		
	<b>Shielded CAT 6A INFORMATION OUTLET with Face Plate</b>		
PASSCAB.REQ.012	Should support frequency of 500 MHZ or better		
PASSCAB.REQ.013	material Should be nickel plated zinc die cast or better		
PASSCAB.REQ.014	Should provide 10Gbast T performance upto 100 meter or better		
PASSCAB.REQ.015	Should have standard mating cycles of 900 or equivalent		
PASSCAB.REQ.016	Information Outlet should be Toolless, and should be provided with face plate and other required accessories		
PASSCAB.REQ.017	IO should be UL listed		
	<b>24 PORT CAT6A JACK PANEL LOADED</b>		
PASSCAB.REQ.018	Should be made from Sheet Steel		
PASSCAB.REQ.019	Have port identification numbers on the front of the panel.		
PASSCAB.REQ.020	Should have self-adhesive, clear label holders and designation labels with the panel, with optional color labels / icons.		
PASSCAB.REQ.021	Jack panel should be UL listed		
PASSCAB.REQ.022	Each port / jack on the panel should be removable on field from the panel.		
PASSCAB.REQ.023	Should have integrated rear cable management shelf.		
PASSCAB.REQ.024	Ports should be in zig zag manner or should have sideways orientation		
	<b>MOUNTING CORDS – S/FTP Cat 6A</b>		
PASSCAB.REQ.025	Should be 4 pair 26 AWG stranded copper wire Cat 6A or better		
PASSCAB.REQ.026	Each pair enclosed in aluminium foil or better		
PASSCAB.REQ.027	Should be terminated with Insulation Displacement Technology or equivalent technology to avoid heating in POE+ devices		
PASSCAB.REQ.028	Patch Cord should support 802.3 bt		
PASSCAB.REQ.029	patch cord should be UL listed		
PASSCAB.REQ.030	Sheath Should be LSFRZH		
PASSCAB.REQ.031	Should support minimum 900 mating cycles		
PASSCAB.REQ.032	Should be verified by ETL/3P in channel for Cat6A (Certificate to be available online on intertek or 3Ptest website)		
	<b>Passive Specs for Fiber Products</b>		
	<b>FIBER CABLE INDOOR/OUTDOOR 12 CORE or higher OM4 MULTIMODE as per requirement</b>		
PASSCAB.REQ.033	Should be as per IEC 60794-1-2 E1; IEC 60794-1-2 E11; IEC 60794-1-2 E3; IEC 60794-1-2 F1; IEC 60794-1-2 E4; IEC 60794-		

Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	1-2 E7; IEC 60794-1-2 E10 or equivalent		
PASSCAB.REQ.034	Should be unarmored		
PASSCAB.REQ.035	Type: Multimode OM4 or better		
PASSCAB.REQ.036	Cable Jacket material: Low Smoke Zero Halogen or better		
PASSCAB.REQ.037	Minimum Cores 12 or better		
	<b>LIU - LOADED WITH DUPLEX LC PORTS WITH SPLICE TRAY</b>		
PASSCAB.REQ.038	Have sufficient slots to accommodate 24 Duplex LC Ports		
PASSCAB.REQ.039	Should have fiber management provision inside		
PASSCAB.REQ.040	Should have Splice holder for minimum 24 Fiber cores or better		
PASSCAB.REQ.041	Should be made of Steel CRCA or better		
PASSCAB.REQ.042	Material Should steel: 1.5 mm, powder-coated or better		
	<b>OPTICAL FIBER PIGTAILS OM4 MULTIMODE MODE LC</b>		
PASSCAB.REQ.043	Connector type LC		
PASSCAB.REQ.044	Fiber Type MM OM4		
PASSCAB.REQ.045	Compact design (SFF). 1.25 mm ferrule technology or equivalent		
PASSCAB.REQ.046	Length 1meter/1.5 meter or better as per the solution requirement		
	<b>OPTICAL FIBER EQUIPMENT CORDS (MINIMUM 2 METER)</b>		
PASSCAB.REQ.047	All optical fiber patch leads shall comprise of Multimode OM4 or better		
PASSCAB.REQ.048	Jacket should be LSZH sheath or equivalent		
PASSCAB.REQ.049	Connector: Zirconia ceramic ferrule or equivalent		
PASSCAB.REQ.050	Connector type Duplex LC-LC		
PASSCAB.REQ.051	Mating cycles: delta IL < 0.2 dB after 500 mating cycles or better		
PASSCAB.REQ.052	Pull-out force patch cord: ≥ 100 N (per connector) or better		
PASSCAB.REQ.053	Should have option for Visual coding, mechanical coding and lock protection.		
PASSCAB.REQ.054	Length 2 meter /3 meter /5 meter/7 mtr/10 mtr/15 Mtr (as per the overall solution requirement)		



## 17.46 "Technical Requirements Specifications - HVAC System/PAC"

Product Name:HVAC System/ PAC

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>PAC.REQ.001</b>	General Requirement	solution should be capable of providing sensible cooling capacities at design ambient temperature & humidity with adequate airflow. Proposed system should be capable to be integrated with the Building management System for effective monitoring.		
<b>PAC.REQ.002</b>	General Requirement	The PAC should be step less variable capacity cooling, horizontal Throw unit complete with Compressor, green Refrigerant, outdoor unit, heater, humidifier, rated for actual cooling capacity @ 32 Deg C return air temp. suitable to give 21+/- 2 Deg. C in Cold aisle at 37 deg C ambient condition.		
<b>PAC.REQ.003</b>	General Requirement	Constant Bit Rate		
<b>PAC.REQ.004</b>	Redundancy	This PACs should be as per N+1 or N+N redundancy requirement		
<b>PAC.REQ.005</b>	Temperature Requirements	The environment inside the room and Portable Server Firm Enclosure at DC shall need to be continuously maintained at $22 \pm 2$ Centigrade. It is advised that the temperature and humidity be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24x7 basis and logged for providing reports.		
<b>PAC.REQ.006</b>	Temperature Requirements	The precision air-conditioners should be capable of maintaining a temperature range of 22 degree with a maximum of 2 degree variation on higher and lower side and relative humidity of 50% with a maximum variation of 5% on higher and lower side		
<b>PAC.REQ.007</b>	Relative Humidity (RH) requirements	Ambient RH levels shall need to be maintained at $50\% \pm 5$ non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>PAC.REQ.008</b>	Air quality levels	The PAC shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, blocking the function of moving parts, causing components to overheat etc. Air filters shall be 95% efficiency & provide up-to 5 Micron particulate shall be deployed		
<b>PAC.REQ.009</b>	Air quality levels	B/W mode: 0.0005 lux (IR OFF);		
<b>PAC.REQ.010</b>	Miscellaneous	The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.		
<b>PAC.REQ.011</b>	Miscellaneous	The refrigerant used shall be environment friendly R-410-A in view of long term usage of the data centre equipment, availability of spares and refrigerant.		
<b>PAC.REQ.012</b>	Display Unit	· Room temperature and humidity.		
<b>PAC.REQ.013</b>	Display Unit	· Humidifier working status		
<b>PAC.REQ.014</b>	Display Unit	· Manual / Auto unit status		
<b>PAC.REQ.015</b>	Display Unit	· Temperature set point		
<b>PAC.REQ.016</b>	Display Unit	· Humidity set point		
<b>PAC.REQ.017</b>	Display Unit	· Working hours of main component i.e. compressors, fans, heater,		
<b>PAC.REQ.018</b>	Display Unit	· humidifier		
<b>PAC.REQ.019</b>	Display Unit	· Unit working hours		
<b>PAC.REQ.020</b>	Display Unit	· Current date and time		
<b>PAC.REQ.021</b>	Display Unit	· Type of alarm (with automatic reset or block)		
<b>PAC.REQ.022</b>	Display Unit	· The last 10 intervened alarms		
<b>PAC.REQ.023</b>	Display Unit	· The microprocessor should be able to perform following functions		
<b>PAC.REQ.024</b>	The control system shall include the following settable features	· Unit identification number		
<b>PAC.REQ.025</b>	The control system shall include the following	· Startup Delay, Cold start Delay and Fan Run on timers		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	settable features			
<b>PAC.REQ.026</b>	The control system shall include the following settable features	· Sensor Calibration		
<b>PAC.REQ.027</b>	The control system shall include the following settable features	· Remote shutdown & general Alarm management		
<b>PAC.REQ.028</b>	The control system shall include the following settable features	· Compressor Sequencing		
<b>PAC.REQ.029</b>	The control system shall include the following settable features	· Return temperature control		
<b>PAC.REQ.030</b>	The control system shall include the following settable features	· Choice of Modulating output types		
<b>PAC.REQ.031</b>	The microprocessor should be able to perform following functions	· Testing of the working of display system		
<b>PAC.REQ.032</b>	The microprocessor should be able to perform following functions	· Password for unit calibration values modification		
<b>PAC.REQ.033</b>	The microprocessor should be able to perform following functions	· Automatic re-start of program		
<b>PAC.REQ.034</b>	The microprocessor should be able to perform following functions	· Compressor starting timer		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
<b>PAC.REQ.035</b>	The microprocessor should be able to perform following functions	Humidifier capacity limitation		
<b>PAC.REQ.036</b>	The microprocessor should be able to perform following functions	Date and time of last 10 intervened alarm		
<b>PAC.REQ.037</b>	The microprocessor should be able to perform following functions	Start / Stop status storage		
<b>PAC.REQ.038</b>	The microprocessor should be able to perform following functions	Random starting of the unit.		
<b>PAC.REQ.039</b>	The microprocessor should be able to perform following functions	Outlet for the connection to remote system		
<b>PAC.REQ.040</b>	The microprocessor should be able to perform following functions	Temperature and humidity set point calibration		
<b>PAC.REQ.041</b>	The microprocessor should be able to perform following functions	Delay of General Alarm activation		
<b>PAC.REQ.042</b>	The microprocessor should be able to perform following functions	·Alarm calibration		
<b>PAC.REQ.043</b>	Alarms shall be displayed on screen of microprocessor unit	·Air flow loss		
<b>PAC.REQ.044</b>	Alarms shall be displayed on screen of	Clogged Filters		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	microprocessor unit			
<b>PAC.REQ.045</b>	Alarms shall be displayed on screen of microprocessor unit	Compressor low pressure		
<b>PAC.REQ.046</b>	Alarms shall be displayed on screen of microprocessor unit	Compressor high pressure		
<b>PAC.REQ.047</b>	Alarms shall be displayed on screen of microprocessor unit	Smoke – fire		
<b>PAC.REQ.048</b>	Alarms shall be displayed on screen of microprocessor unit	Humidifier Low water level		
<b>PAC.REQ.049</b>	Alarms shall be displayed on screen of microprocessor unit	· High / Low room temperature		
<b>PAC.REQ.050</b>	Alarms shall be displayed on screen of microprocessor unit	· High/Low room humidity		
<b>PAC.REQ.051</b>	Alarms shall be displayed on screen of microprocessor unit	· Spare External Alarms		
<b>PAC.REQ.052</b>	Alarms shall be displayed on screen of microprocessor unit	· Water Under floor		
<b>PAC.REQ.053</b>	The unit shall incorporate the following protections	· Single phasing preventers		
<b>PAC.REQ.054</b>	The unit shall incorporate the following protections	· Reverse phasing		
<b>PAC.REQ.055</b>	The unit shall incorporate the following protections	Phase misbalancing		
<b>PAC.REQ.056</b>	The unit shall incorporate the	· Phase failure		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Reference (Document /Page no)
	following protections			
<b>PAC.REQ.057</b>	The unit shall incorporate the following protections	Overload tripping (MPCB) of all components		

#### 17.47 "Technical Requirements Specifications – 42U Rack

Sr .No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Reference (Document /Page no)
<b>RACK.REQ.001</b>	<b>Racks</b>	Proposed Racks will be used to mount and house all server and network devices.		
<b>RACK.REQ.002</b>		The rack has to be designed to meet the safety requirements.		
<b>RACK.REQ.003</b>		Both the front and rear door should have got a comfort handle with different locking options. Cable entry should be entered via the roof plate inside the rack.		
<b>RACK.REQ.004</b>	<b>Frame</b>	Symmetrical frame construction of sheet steel, removable top & Bottom cover with Cable entry provision. The enclosures should be bay-able on all faces. 42U 19" L type angle Front & Rear on vertical cable trough on 6 x punched section with Nickel Chrome or better plated. should be Mounted on Installation bracket for stability and strength, with U marking.		
<b>RACK.REQ.005</b>	<b>Doors</b>	Sheet steel front and rear door, large perforated area, front and rear door with locking system to provide more strengthen to doors.		
<b>RACK.REQ.006</b>		Front perforated single door and rear perforated double door.		
<b>RACK.REQ.007</b>	<b>Roof &amp;Base</b>	Top cover with 4 x cut-out of Dia. Bottom cover with 4 x cut-out of Dia.		
<b>RACK.REQ.008</b>	<b>Side Panels</b>	Screw-fastened or plug-type version, sheet steel side panel with .		
<b>RACK.REQ.009</b>	<b>Cooling Fan</b>	230V,AC 90CFM fan pack of 4 Nos.or more		

Sr .No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Reference (Document /Page no)
<b>RACK.REQ.010</b>	<b>Interior Installation</b>	19 inch attachment level front and rear, L-shaped mounting angles with square holes to EIA 310-D, infinitely depth adjustable, attached to 4 punched sections with mounting flanges (2 per side). Static load capacity (19 inch) with mounting angles: 1000 kg or better		
<b>RACK.REQ.011</b>	<b>Surface Finish</b>	Nano Coated, electro-dip coat primed to 20 microns and powder coated to 80 to 120 microns or better		
<b>RACK.REQ.012</b>	<b>Dimensions</b>	600 x 2000 x 1200 mm (W x H x D), 42UH for Server Rack, 800 x 2000 x 1200 mm (W x H x D), 42UH for network RACK		
<b>RACK.REQ.013</b>	<b>Shelf</b>	720 mm deep component shelves 2 Nos.		
<b>RACK.REQ.014</b>	<b>Castor wheel</b>	Rack should have 2 Nos. castor wheel with brake and 2 Nos. castor wheel without brake or better		
<b>RACK.REQ.015</b>	<b>Cable Management</b>	80 mm wide x 1800 mm height cable route at rear side with 10 nos. metal shunting rings. 5 Nos. 19" mount PVC finger type horizontal cable manager.		
<b>RACK.REQ.016</b>	<b>PDU</b>	2 Nos. vertical mount PDU with 10 Nos. C-13 and 5 Nos. 5/15 amp sockets with 2.5 mtr cable with industrial plug 32A.		
<b>RACK.REQ.017</b>	<b>Load Capacity</b>	Rack frame load bearing capacity of 1200 Kgs or better .		
<b>RACK.REQ.018</b>	<b>Approvals</b>	Rack should approved with EIA-310, DIN-41494 and IEC-297 certificates. ISO 9001, 14001, 45001, ROHS, UL 2416 or equivalent		

#### Annexure-18: Unpriced Bill of Material

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity	Make	Model
<b>A</b>	<b>IT Components</b>				
1	Rack Server	Nos	12		
2	Hyper Converged Infrastructure	Nos	12		
3	Virtualisation Software and Management Solution for Rack server Cluster	Nos	1		
4	Windows Operating System Data Center Edition - 16 Core License Model	Nos	36		
5	Redhat Linux Operating System Enterprise Edition - Socket Based	Nos	12		
6	MS SQL Database Enterprise Edition - Core Based	Nos	32		
7	Postgres SQL Enterprise Edition - Core Based	Nos	64		
8	Backup Hardware & Software (500 TB front end capacity or 500 VM)	Nos	1		
9	Server Load Balancer	Nos	2		
10	SDN Controller	Nos	2		
11	SPINE Switch	Nos	2		
12	Leaf switch – OFC	Nos	8		
13	Core Router – Internet	Nos	2		
14	Core Router – Intranet	Nos	2		
15	Management Switch	Nos	2		
16	Link Load balancer - Internet	Nos	2		
17	Link Load balancer - Intranet	Nos	2		
18	L2 Managed Switch for NOC	Nos	2		
19	SAN Switch	Nos	2		
20	Enterprise Storage (500 TB Usable Storage)	Nos	1		
21	Next Generation Firewall - Internet	Nos	2		
22	Next Generation Firewall - Intranet	Nos	2		
23	Web Application Firewall	Nos	2		
24	EDR - Endpoint Detection Response	Nos	500		
25	Identity Access Manager	Nos	500		
26	Enterprise Monitoring System (NMS, ITSM, ISMS)	Nos	500		
27	Network Access Controller	Nos	2		
28	HSM - Hardware Security Module	Nos	2		
29	HIPS - Host Intrusion Prevention System	Nos	500		
30	NDR - Network Detection and Response	Nos	2		
31	DDoS	Nos	1		
<b>B</b>	<b>Non IT Components</b>				



Sr. No.	Item Description	Unit of Measurem ent	Indicative Quantity	Make	Model
1	UPS - 300 KVA with battery bank upgradable to 400 KVA	Nos	2		
2	Battery Bank for 300 KVA - Min 4 Hrs backup	Lot	1		
3	UPS - 20 KVA with Battery Bank	Nos	2		
4	Battery Bank for 20 KVA - Min 4 Hrs backup	Lot	1		
5	Split AC - 1.5 Ton	Nos	3		
6	Split AC - 2 Ton	Nos	2		
7	HVAC System - Precision Air Conditioner	Nos	4		
8	Biometric Door Access System	Nos	1		
9	Smart TV - 55 inch	Nos	4		
10	Smart TV - 75 inch	Nos	4		
11	Data Center Infrastructure Management (DCIM)	Nos	1		
12	Ultrasonic Rodent Repellent System	Nos	1		
13	Water Leak Detection System	Nos	1		
14	Intelligent Addressable Fire Alarm System	Nos	1		
15	Smoke Detection System	Nos	1		
16	Fire Suppression System	Nos	1		
17	Master Control Unit	Nos	1		
18	Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp including substation protection and metering devices	Nos	1		
19	42U Rack (Network + Server)	Nos	8		
20	DG Set 380 KVA (D Check & Fuel Refilling)	Nos	1		
21	Advanced Building Management System (BMS)	Nos	1		
22	Structured Cabling	Lot	1		
23	Loaded Fiber Enclosure for Type I MPO Cassettes	Lot	1		
24	Passive Cabling	Lot	1		
25	Fiber Optic solutions for DC Connectivity	Lot	1		
26	Fiber Panel	Lot	1		
27	CAT6A U/UTP Cable	Lot	1		
28	24 Port Patch Panel loaded	Lot	1		
29	CAT6 I/O for loaded Patch Panel	Lot	1		
30	CAT6A Patch Cord	Lot	1		
31	MFZ Verifocal Dome	Nos	24		
32	Bullet Camera	Nos	2		
33	PTZ Camera	Nos	2		
34	Power Cables	Lot	1		

Sr. No.	Item Description	Unit of Measurement	Indicative Quantity	Make	Model
<b>C</b>	<b>Civil &amp; Interior</b>				
1	One time Site Preparation (Civil & Electrical) Cost for DC including complete site preparation of Data Center, inclusive but not limited to false flooring, lighting fixture, electrical works, Mason Works, Dismantling existing Wall, Doors, Window or any structure of any material etc(Refer Scope of Work for further details)	Lot	1		
2	EARTHING: Preparation of All Earth Pits, Necessary Repair, Testing earth resistivity and electrode resistance	Lot	1		
3	Electrical works - for NOC, DC, DG Set UPS and LT Panel	Lot	1		
4	Setting up of State of the art NOC room with required Furniture and other components including false flooring, lighting fixture, electrical works, beautifications of NOC area, wall panels, Mason Works, etc. (Refer Scope of Work for further details)	Lot	1		

## Annexure-19: Existing Asset Details of Current Infrastructure at CGSDC

S. No	Device Type	Make	Model	Serial Number	Date of Installation	Warranty upto
1	Core switch	HP	HP A 7510 JD238B-Core Switch	CN22D56015	24-Nov-12	09-Feb-23
2	Core switch	HP	HP A 7510 JD238B-Core Switch	CN22D5600Y	24-Nov-12	09-Feb-23
3	Router	HP	HP ROUTER A MSR 50-40	CN18BPD002	24-Nov-12	09-Feb-23
4	Router	HP	HP ROUTER A MSR 50-40	CN1BBDJ00T	24-Nov-12	09-Feb-23
5	NIPS	MCAFE E	NIPS - MCAFEE Intru-shield M-6050	W021234231	14-Sep-12	Not Available
6	NIPS	MCAFE E	NIPS - MCAFEE Intru-shield M-6050	W021234236	14-Sep-12	Not Available
7	Access Switch	HP	HP A 5120 Access SWITCH - 24 Port	CN25BYR00T	24-Nov-12	09-Feb-23
8	Access Switch	HP	HP A 5120 Access SWITCH - 24 Port	CN25BYR013	24-Nov-12	09-Feb-23
9	Access Switch	HP	HP A 5120 Access SWITCH- 48 Port	CN27BYS0LJ	24-Nov-12	09-Feb-23
10	Access Switch	HP	HP A 5120 Access SWITCH- 48 Port	CN27BYS08K	24-Nov-12	09-Feb-23
11	Access Switch	HP	HP A 5120 Access SWITCH- 48 Port	CN27BYS0L0	24-Nov-12	09-Feb-23
12	Access Switch	HP	HP A 5120 Access SWITCH- 48 Port	CN19BYS0LT	10-Jun-17	09-Feb-23
13	Access Switch	HP	HP A 5120 Access SWITCH- 48 Port	CN23BYS02C	24-Nov-12	09-Feb-23
14	Access Switch	HP	HP A 5120 Access SWITCH- 48 Port	CN27BYS0BP	24-Nov-12	09-Feb-23
15	Firewall	Fortinet	FORTIGATE 620 B	FG600B3912600 115	21-Sep-12	30-Jan-23
16	Firewall	Fortinet	FORTIGATE 620 B	FG600B3912600 108	21-Sep-12	30-Jan-23
17	Firewall	Fortinet	SP-FG620B-RPS	RPS6003G12000 012	24-Nov-12	30-Jan-23
18	HIPS	HIPS	Windows server 2008	06FNXD3	24-Nov-12	09-Feb-23
19	KVM Switch	Aten	Aten	A1C9B100AKH00 03	24-Nov-12	09-Feb-23
20	KVM Switch	Aten	Aten	A1C9E100AKL00 05	24-Nov-12	09-Feb-23
21	KVM Switch	Aten	Aten	A1C95100AKB00 08	24-Nov-12	09-Feb-23
22	KVM Switch	Aten	Aten	A1C9B100AKH00 07	24-Nov-12	09-Feb-23
23	KVM Switch	Aten	Aten	A1C9Z100AK500 02	24-Nov-12	09-Feb-23
24	KVM MONITOR	Aten	Aten	Z8C40061C0100 60	24-Nov-12	09-Feb-23
25	KVM MONITOR	Aten	Aten	Z8C4D083C2S00 46	24-Nov-12	09-Feb-23
26	KVM MONITOR	Aten	Aten	Z8C4K061C0500 22	24-Nov-12	09-Feb-23
27	KVM MONITOR	Aten	Aten	Z8C4T061C0400 50	24-Nov-12	09-Feb-23
28	KVM MONITOR	Aten	Aten	Z8C4L083C2F00 60	24-Nov-12	09-Feb-23
29	SAN Switch	Cisco	MDS9148	JAF1626BGGM	24-Nov-12	09-Feb-23
30	SAN Switch	Cisco	MDS9148	JAF1638AHRB	24-Nov-12	09-Feb-23
31	SAN Switch	Cisco	MDS9148	AMS18060234	23-Feb-15	09-Feb-23
32	SAN Switch	Cisco	MDS9148	AMS18060564	23-Feb-15	09-Feb-23

#	Type	Description	Make	Model	Serial Number	Raw Capacity	Total HDD/Tape	Date of Installation	Warranty Upto
1	IT	NetApp Storage	NetApp	V3240	'850000196709		47	24-Nov-12	09-Feb-23
2	IT	NetApp Storage	NetApp	V3240	'500000146911		23	24-Nov-12	09-Feb-23
3	IT	NetApp Storage	NetApp	DS4243	LBS957320025A64			24-Nov-12	09-Feb-23
4	IT	NetApp Storage	NetApp	DS4244	LBS9573200262E4	67.2 TB		24-Nov-12	09-Feb-23
5	IT	NetApp Storage	NetApp	DS4245	LBS95732001C09D			24-Nov-12	09-Feb-23
6	IT	NetApp Storage	NetApp	DS4246	LBS9573200272EA			24-Nov-12	09-Feb-23
7	IT	IBM	IBM	TS3310	1322280		60	24-Nov-12	09-Feb-23
8	IT	Dell Backup	Dell	Net Vault Backup Server Enterprise Edition	NA	NA	NA	30-Sep-12	09-Feb-23
9	IT	Dell-EMC Storage	Dell-EMC	Dell EMC MD3800F	Power Vault MD3800F	100TB		03-Jun-18	09-Feb-23
10	IT	HDS storage & Heterogenous replicator	HDS	VSP-A0001.S	91791	93.75		13-Jan-15	09-Feb-23
11	IT	IBM V3700	IBM	V5030F	781W998	34.2TB		Jun-17	09-Feb-23

#	Product Description	Make	Product	Version	Total Licenses	Used Licenses
<b>Operating System</b>						
1	Microsoft windows server CAL 2012 snl open 1 Lic. level c user CAL user CAL	Microsoft	Microsoft	2012	30	0
2	Microsoft windows server Data Centre 2012 snl open 1 Lic level C 2 PROC	Microsoft	Microsoft	2012	22	11
3	Microsoft windows server external connector 2012 snl open 1 Lic level C	Microsoft	Microsoft	2012	2	0
4	Microsoft windows server Enterprise Edition	Microsoft	Microsoft	2008	18	8
5	RedHat Enterprise Linux Server, Standard 1-2 sockets	RedHat	RedHat	RHEL Server, Standard (1-2 sockets) (Up to 1 guest)	7	7
<b>Database Licenses</b>						
6	Oracle Database Enterprise Edition - Processor Perpetual - 08 Processors (Oracle Database)	Oracle	Oracle	11GR2-Enterprise Edition	8	8
7	MS SQL Enterprise latest Edition, SQLSvrEnt 2008R2 SNGL OLP C 1Proc	Microsoft	Microsoft	2008	2	2
8	Microsoft SQL Svr Enterprise core 2012 Sngl Open 2 Lic level c core Lic	Microsoft	Microsoft	2012	16	16
<b>Antivirus</b>						
9	Trend Micro Antivirus	Trend Micro	Trend Micro	11.x	250	36
10	HIPS	IBM	IBM	2.9	18	12
<b>Backup Software</b>						
11	NETVAULT BACKUP SERVER ENTERPRISE EDITION FOR WINDOWS PER MACHINE ID LICENSE/MAINT PACK	Quest Software(Dell)	Quest Software(Dell)	Version 9.00	1	1
<b>Qradar</b>						
12	Base Software Appliance 31XX and License	IBM	Qradar	QRS- 31XX-SW	1	1
<b>IBM TIVOLI</b>						
13	EMS Complete solution(Linux 5.x Operating System for EMS Blade)	IBM	TIVOLI Suite		7	7

#	Product Description	Make	Product	Version	Total Licenses	Used License
Firewall and IPS						
14	External Firewall	Fortinet	Fortigate 620 B	V5.2.0	2	2
15	IPS	McAfee	Intrushield M6050	8.1.3.6	2	2

## 1. Non-IT

Sr No.	Name	Make	Model	Capacity	Quantity	Date of Installation	Warranty Upto	Brief Details
1	UPS For Computer + Emergency Lights	Emerson Power	Liebert Hipulse 7400 M	20 KVA	2	Nov'12	31-Jan-23	NA
2	APFC Panel	Risha Control	NA	160 KVA	2	Nov'12		NA
3	UPS PDU	Risha Control & SJ Electricals	NA	630A & 100A	6	Nov'12	31-Jan-23	NA
4	UPS O/P PDU	Risha Control	NA	630 A	2	Nov'12	31-Jan-23	NA
5	Utility Ups PDU	Risha Control	NA	100A	1	Nov'12	31-Jan-23	NA
6	ATS Panel for PAC	Risha Control	NA	63A	5	Nov'12	31-Jul-22	NA
7	Isolator of PAC	NA	NA	63A	5	Nov'12	31-Jul-22	
8	DB-01 For Workstation from 20 KVA UPS	Schneider Electric	NA	NA	1	Nov'12	31-Jul-22	NA
9	Precision Air Conditioner	Uniflare	TDAV2222AN002	20 TR	5	Oct'12	31-Jul-22	NA
10	Biometric Reader	HID	Bioclass	NA	1	Nov'12	18-Feb'23	NA
11	Proximity Card Reader	HID	R10	NA	13	Nov'12	18-Feb'23	NA
12	Push Button Exit Switch	Ecrabtree	NA	Na	3	Nov'12	18-Feb'23	NA
13	Emergency Door Release Switch	NA	NA	NA	6	Nov'12	18-Feb'23	NA
14	Manual Call Point Switch	NA	NA	NA	4	Nov'12	18-Feb'23	NA
15	CCTV Camera	Honeywell	HDC890NV	NA	19	Nov'12	18-Feb'23	NA
16	CCTV Monitor	LG	Flatron E2242	Na	1	Nov'12	18-Feb'23	NA
17	CCTV Monitor	Dell		Na	1	Nov'12	18-Feb'23	NA
18	Public address System	BOSCH	PLENA-LBB1950/10	NA	1	Nov'12	18-Feb'23	NA
19	PAS Speaker	BOSCH	LBD8352/10	NA	25	Nov'12	18-Feb'23	NA
20	Access control Panel	Honeywell		NA	1	Nov'12	18-Feb'23	NA
21	BMS Control Panel	Honeywell		NA	1	Nov'12	18-Feb'23	NA
22	Fire Alarm panel	Honeywell	Morley IAS9	NA	1	Nov'12	18-Feb'23	NA
23	WLD Control Panel	Star Electronic	Gain Control	NA	1	Nov'12	18-Feb'23	NA
24	Vesda Panel	Xtrails VESDA	VLC-505	NA	1	Nov'12	18-Feb'23	NA
25	Gas Release Panel	Ravel	RE1206R	NA	1	Nov'12	18-Feb'23	NA
26	Gas Release Switch	NA	NA	NA	1	Nov'12	18-Feb'23	NA
27	Gas Abort Switch	NA	NA	NA	1	Nov'12	18-Feb'23	NA
28	Solenoid Volve	Grestone	Na	NA	1	Nov'12	18-Feb'23	NA
29	RH Sensor	Grestone	Na	NA	1	Nov'12	18-Feb'23	NA
30	Smoke Detector	Morley IAS Fire System	MI-PSE-S2-IV	NA	60	Nov'12	18-Feb'23	NA

Sr No.	Name	Make	Model	Capacity	Quantity	Date of Installation	Warranty Upto	Brief Details
31	Fire Response Indicator	Agni Devices	NA	NA	36	Nov'12	18-Feb'23	NA
32	Vesda Detectors	VESDA	NA	NA	8	Nov'12	18-Feb'23	NA
33	Hooter For Fire Alarm System	Mini Strobe Siren	AD-ES-F1	NA	7	Nov'12	18-Feb'23	NA
34	Hooter For WLD System		NA	NA	1	Nov'12	18-Feb'23	NA
35	Electromagnetic Lock For Single Door	BEL	600 LED	NA	3	Nov'12	18-Feb'23	NA
36	Electromagnetic Lock For Double Door	BEL	600-D-LED	NA	6	Nov'12	18-Feb'23	NA
37	BMS Server System Monitor	HP	HP LV1911	NA		Nov'12	18-Feb'23	NA
	Battery Circuit Breaker for 300 KVA							
38	UPS Battery Circuit	NA	T5D630	NA	2	Nov'12		NA
39	Breaker for 20 KVA UPS	NA	T1B160	NA	2	Nov'12		NA
40	Fire Alarm Control Module	Morley IAS Fire System	MI-DCMO	NA	7	Nov'12	Mar'18	NA
41	Fire Alarm Line isolator	Morley IAS Fire System	MI-DISO	NA	4	Nov'12	Mar'18	NA
42	Volume Control Unit	Audio track	NA	NA	1	Nov'12	Mar'18	NA
43	RTU For access Control system	Honeywell	RTU_A08	NA	9	Nov'12	Feb'23	NA

## 2. Non-IT with Extended AMC required

Sr No.	Name	Make	Model	Capacity	Quantity	Date of Installation	Warranty Upto	Brief Details
1	UPS For Server Farm Area	Emerson Power	Liebert Hi-pulse	300 KVA	2	Nov'12	31-Jan-23	
2	Ductable AC	LG	LG-LTN80851QC	8.5 TR	3	Oct'21	21-Oct-22	Replacement done, under warranty. Only AMC required from GoLive.
3	Cassette AC	LG	LG-LTNC246PLFO	2 TR	2	Nov'12	21-Oct-22	
4	Split AC	LG	LG-LSA5NR2A	1.5 TR	1	Nov'12	21-Oct-22	
5	Split AC	LG	LG-LSA3UR2A	1 TR	2	Nov'12	21-Oct-22	
6	Rodent Console	Maser Electronics	MASER VHFO	NA	5	Nov'12	18-Feb'23	
7	Rodent Transducer	MASER	VHFO MISTE		60	Nov'12	18-Feb'23	
8	Co2 Fire Extinguisher Cylinder	Fireshield	6.5 KG	NA	1	Nov'12		
9	Co2 Fire Extinguisher Cylinder	Fireshield	4.5 KG	NA	5	Nov'12		
10	Co2 Fire Extinguisher Cylinder	Fireshield	2 KG	NA	3	Nov'12		
11	Battery Bank for 300 KVA Ups	HBL	TRIUMPH-HPF850PP	850 AH	2 Set(204 Nos of Cells in 1 Set.)	Nov'21	Not Available	
12	Battery Bank for 20 KVA Ups	HBL	TRIUMPH-HPF80PP	80 AH	2 Set(204 Nos of Cells in 1 Set.)	Nov'21	Not Available	

## 3. CoLo Infra

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
1	IT	Server	IBM	IBM-X3750 M4	06DR110	HDD 300*2 gb RAM 128 gb	24-Nov-12	02-May-18	WINDOW S Server 2012
2	IT	Blade Server	IBM	IBM-HS22	06ZWD56	HDD 600 gb RAM 32 gb Pro 16 Core*2 3.60Ghz	24-Nov-12	10-Nov-15	LINUX
3	IT	Blade Server	IBM	IBM-HS23	06DTPTL	HDD 600 gb RAM 32 gb Pro 16 Core*2 E5	24-Nov-12	15-Feb-18	
4	IT	Server	Dell	Dell-PWREdgeR720	J3NM542	HDD 300*2 gb RAM 128 gb Pro Int Xeon E5 2.5 Ghz	24-Nov-12	14-Mar-18	WINDOW S Server 2012
5	IT	Server	Dell	Dell-PWREdgeR720	24NM542	HDD 300*2 gb RAM 128 gb Pro Int Xeon E5 2.5 Ghz	24-Nov-12	21-Mar-18	RHEL 6.5
6	IT	Server	Dell	Dell-PWREdgeR720	14NM542	HDD 300*2 gb RAM 128 gb Pro Int Xeon E5 2.5 Ghz	24-Nov-12	14-Mar-18	RHEL 6.5
7	IT	Server	Dell	Dell-PWREdgeR720	84NM542	HDD 300*2 gb RAM 128 gb Pro Int Xeon E5 2.5 Ghz	24-Nov-12	21-Mar-18	WINDOW S Server 2012

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
8	IT	Server	IBM	IBM-X3750 M4	06DF815	HDD 300*2 gb RAM 128 gb Pro Int Xeon E5 2.5 Ghz	24-Nov-12	15-Feb-18	UBUNTU LINUX
9	IT	Server	IBM	IBM-X3750 M4	06DF814	HDD 300*2 gb RAM 128 gb Pro 16 Core*2 Xeon E5	24-Nov-12	15-Feb-18	WIN SVR 2012 DataCenter
10	IT	Blade Server	IBM	IBM-HS23	06VLKM7	HDD 598 gb RAM 32 gb Pro 16 Core *2 2.40 Ghz	24-Nov-12	20-Oct-16	CentOS release 6.3
11	IT	Blade Server	IBM	IBM-HS23	06VLKM5	HDD 598 gb RAM 32 gb Pro 16 Core *2 2.40 Ghz	24-Nov-12	20-Oct-16	CentOS release 6.3
12	IT	Blade Server	IBM	IBM-HS23	06VLKM4	HDD 598 gb RAM 32 gb Pro 16 Core *2 2.40 Ghz	24-Nov-12	20-Oct-16	WINDOW S
13	IT	Blade Server	IBM	IBM-HS23	06DTPM	HDD 598 gb RAM 32 gb Pro 16 Core *2 2.40 Ghz	24-Nov-12	15-Feb-18	WINDOW S
14	IT	Blade Server	IBM	IBM-HS23	06VLKM6	HDD 598 gb RAM 32 gb Pro 16 Core *2 2.40 Ghz	24-Nov-12	20-Oct-16	WINDOW S
15	IT		IBM	IBM-HS23	06VLKM3	HDD 598 gb RAM 32 gb Pro 16 Core *2 2.40 Ghz	24-Nov-12	20-Oct-16	WINDOW S
16	IT		IBM	IBM-HS23	06ENGHE	HDD 300 gb RAM 32 gb Xeon pro E5 26094C	24-Nov-12	20-Oct-16	WINDOW S SVR 2012 R2 Standard
17	IT		IBM	IBM-HS23	06BXFYN	HDD 300 gb RAM 32 gb Xeon pro E5 2600*2	24-Nov-12	15-Feb-18	
18	IT	Blade Server	IBM	IBM-HS23	06FPNAW	HDD 300 gb RAM 32 gb Xeon pro E5 2600*2	24-Nov-12	20-Oct-16	RHEL 6.5
19	IT	Blade Server	IBM	IBM-HS23	06FPNAT	HDD 300 gb RAM 32 gb Xeon pro E5 2600*2	24-Nov-12	20-Oct-16	
20	IT	Blade Server	IBM	IBM-HS23	06VLKH8	HDD 300*2 gb RAM 16 gb Xeon pro 2600*2	24-Nov-12	31-Oct-16	WIN SVR 2012 R2
21	IT	Blade Server	IBM	IBM-HS23	06FPNAV	HDD 300*2 gb RAM 16 gb Xeon pro 2600*2	24-Nov-12	31-Jul-18	Vmware ESXi 5.5.0
22	IT	Blade Server	IBM	IBM-HS23	06DTPTK	HDD 300*2 gb RAM 32 gb Xeon pro 2609 2.40 Ghz*2	24-Nov-12	15-Feb-18	WIN SVR 2012 R2
23	IT	Blade Server	IBM	IBM-HS23	06VLKM8	HDD 300*2 gb RAM 32 gb Xeon pro 2609 2.40 Ghz*2	24-Nov-12	20-Oct-16	Vmware ESXi 5.5.0
24	IT	Blade Server	IBM	IBM-HS23	06XRLF9	HDD 300*2 gb RAM 16 gb Xeon pro 2609 2.40 Ghz*2	24-Nov-12	19-Jan-17	WIN SVR 2008 R2
25	IT	Blade Server	IBM	IBM-HS23	06XRLG0	HDD 300*2 gb RAM 32 gb	24-Nov-12	19-Jan-17	WIN SVR 2008 R2



Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						Xeon pro 2609 2.40 Ghz*2			
26	IT	Blade Server	IBM	IBM-HS23	06FPNAX	HDD 300*2 gb RAM 64 gb Xeon pro 2600*2	24-Nov-12	31-Jul-18	Vmware ESXi 5.5.0
27	IT	Blade Server	IBM	IBM-HS23	06ZYPD9	HDD 300*2 gb RAM 32 gb Pro Xeon e5 2665 2.4 Ghz	24-Nov-12	09-May-17	RHEL 6.5
28	IT	Blade Server	IBM	IBM-HS23	06VLKH6	HDD 300*2 gb RAM 64 gb Pro Xeon e5 2665 2.4 Ghz	24-Nov-12	31-Oct-16	Vmware ESXi 5.5.0
29	IT	Blade Server	IBM	IBM-HS23	06VLKH9	HDD 300*2 gb RAM 64 gb Pro Xeon e5 2665 2.4 Ghz	24-Nov-12	31-Oct-16	Vmware ESXi 5.5.0
30	IT	Blade Server	IBM	IBM-HS23	06ZYPD8	HDD 300*2 gb RAM 64 gb Pro Xeon e5 2665 2.4 Ghz	24-Nov-12	09-May-17	Vmware ESXi 5.5.0
31	IT	Blade Server	IBM	IBM-HS23	06ZYPE0	HDD 300*2 gb RAM 60 gb Pro Xeon e5 2665 2.4 Ghz	24-Nov-12	09-May-17	Vmware ESXi 5.5.0
32	IT	Blade Server	IBM	IBM-HS23	06ZYPE1	HDD 300*2 gb RAM 32 gb Pro Xeon e5 2665 2.4 Ghz	24-Nov-12	10-May-17	Vmware ESXi 5.5.0
33	IT	Rack Server	Dell	Dell-PWREdgeR720	44NM542	HDD (300GB X 4), DDR3 SDRAM (16GB X 8), Intel Xeon (8 Cores X 2) Processor 2.60 GHz	24-Nov-12	14-Mar-18	WINDOW S Server 2012
29	IT	SAN Switch	Cisco	JAF1626BGGM	MDS9148	48Port	24-Nov-12	19-Nov-14	M9010-S3EK9MZ. 5.0.1A.bin
30	IT	SAN Switch	Cisco	JAF1638AHRB	MDS9148	48 Port	24-Nov-12	19-Nov-14	M9010-S3EK9MZ. 5.0.1A.bin
31	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023B	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
32	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023D	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
33	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023O	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
34	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023H	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
35	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023L	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
36	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN75440237	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
37	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023N	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
38	IT	HP Blade	HP	HP Proliant BL660C Gen8	CN7544023J	HDD (600 GB X 2), DDRIII SDRAM (32 GB X 16 ), Intel Xeon ( 32 Core X 1) Processor 2.30 Ghz	20-Jul-16	Apr-17	Windows Server 2012
39	IT	WIPRO	HP	WIPRO		HDD (140 GB X 4), DDRIII SDRAM (8 GB X 8 ), Intel Xeon E7520( 4 Core X 2) Processor 1.86 Ghz,	Nov-12	Nov-13	Windows Server 2003
40	IT	HCL	HP	HCL	B083A116800A	HDD(160GB X 8), DDRIII SDRAM (2GB X 16) RAM, Intel Xeon (4Core X 2) E7-7310 @ 1.6 GHz	Nov-12	Nov-13	Windows Server 2008
41	IT	HCL	HP	HCL	2103A1307790	HDD(160GB X 8), DDRIII SDRAM (2GB X 16) RAM, Intel Xeon (4Core X 2) E7-7310 @ 1.6 GHz	Nov-12	Nov-13	Windows Server 2008
42	IT	HCL	HP	HCL	B083A1168003	HDD(160GB X 8), DDRIII SDRAM (2GB X 16) RAM, Intel Xeon (4Core X 2) E7-7310 @ 1.6 GHz	Nov-12	Nov-13	Windows Server 2008
43	IT	HP	HP	HP		HDD (300 GB X 1), DDRIII SDRAM (16 GB X 3 ), Intel Xeon E5-2440 (12Core X 2) Processor 2.40Ghz	Nov-12	Nov-13	Windows Server 2008
44	IT	WIPRO	HP	WIPRO	12FFYU04200002	HDD (300 GB X 3), DDRIII SDRAM (8 GB X 8 ), Intel Xeon E7520( 8 Core X 2) Processor 1.87 G	Nov-12	Nov-13	Windows Server 2008

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
45	IT	WIPRO	HP	WIPRO	12FFYU04200003	HDD (300 GB X 3), DDRIII SDRAM (8 GB X 8 ), Intel Xeon E7520( 8 Core X 2) Processor 1.87 G	Nov-12	Nov-13	Windows Server 2008
46	IT	HP Blade	HP	HP Proliant BL460C Gen8	SGH409CS7A	HDD (300GB X 2), 16GB RAM, Intel Xenon e5 2.0GHz Window Server 2012 R2	01-Jul-16	May-17	Window Server 2012 R2
47	IT	HP Blade	HP	HP Proliant BL460C Gen8	SGH409CS7C	HDD (300GB X 2), 16GB RAM, Intel Xenon e5 2.0GHz Window Server 2012 R2	01-Jul-16	May-17	Window Server 2012 R2
48	IT	HP Blade	HP	HP Proliant BL460C Gen8	SGH409CS79	HDD (300GB X 2), 16GB RAM, Intel Xenon e5 2.0GHz Window Server 2012 R2	01-Jul-16	May-17	Window Server 2012 R2
49	IT	HP Blade	HP	HP Proliant BL460C Gen8	SGH409CS7B	HDD (300GB X 2), 16GB RAM, Intel Xenon e5 2.0GHz Window Server 2012 R2	01-Jul-16	May-17	Window Server 2012 R2
50	IT	Lenovo	Lenovo	Lenovo-X3850X6	J31DKHD	HDD (300GB X 2), DDRIII SDRAM (8GB X 16), Intel Xeon (8 Core X 1) Processor 2.06 Ghz	Jul-16	Jun-18	
51	IT	Lenovo	Lenovo	Lenovo-X3850X6	J31DKHC	HDD (300GB X 2), DDRIII SDRAM (8GB X 16), Intel Xeon (8 Core X 1) Processor 2.06 Ghz	Jul-16	Jun-18	
52	IT	Lenovo	Lenovo	Lenovo-X3850X6	J31DKHE	HDD (300GB X 2), DDRIII SDRAM (8GB X 16), Intel Xeon (8 Core X 1) Processor 2.06 Ghz	Jul-16	Jun-18	
53	IT	Rack Server	Dell	Dell-PWREdgeR620	D7NZQG2	HDD (600GB X 3), DDR4 (16GB x 12), Intel Xeon E5-2620v4 (8 Cores X 2) 2.10 GHz	Jul-16	Jun-18	Window server 2016
54	IT	Rack Server	Dell	Dell-PWREdgeR620	D7NWQG2	HDD (600GB X 3), DDR4 (16GB x 12), Intel Xeon E5-2620v4 (8 Cores X 2) 2.10 GHz	Jul-16	Jun-18	Window server 2016
55	IT	Rack Server	Dell	Dell-PWREdgeR620	D7P1RG2	HDD (600GB X 3), DDR4 (16GB x 12), Intel Xeon E5-2620v4 (8	Jul-16	Jun-18	Window server 2016

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						Cores X 2) 2.10 Ghz			
56	IT	Rack Server	Dell	Dell-PWREdgeR620	D7P3RG2	HDD (1.2TB X 6), DDR4 (16GB x 12), Intel Xeon E5-2620v4 (8 Cores X 2) 2.10 Ghz	Jul-16	Jun-18	Window server 2016
57	IT	Rack Server	Dell	Dell-PWREdgeR630	462NXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Mar-17	Feb-18	
58	IT	Rack Server	Dell	Dell-PWREdgeR630	461KXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Mar-17	Feb-18	
59	IT	Rack Server	Dell	Dell-PWREdgeR630	462GH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Mar-17	Feb-18	
60	IT	Rack Server	Dell	Dell-PWREdgeR630	46PGXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Apr-17	Mar-18	
61	IT	Rack Server	Dell	Dell-PWREdgeR630	46QNXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Apr-17	Mar-18	
62	IT	Rack Server	Dell	Dell-PWREdgeR630	463MXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Apr-17	Mar-18	
63	IT	Rack Server	Dell	Dell-PWREdgeR630	46TMXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Apr-17	Mar-18	
64	IT	Rack Server	Dell	Dell-PWREdgeR630	46RPXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	Apr-17	Mar-18	
65	IT	Rack Server	Dell	Dell-PWREdgeR630	46SPXH2	HDD 600*4 gb, RAM: 16*16gb, Processor: intel 8core e5 2.1 Ghz	15-03-2017	14-03-2018	
66	IT	Blade Server	Dell	Dell-PWREdgeM830	32670J2	HDD 1.2TB*2, RAM: 16*16GB, Processor: intel 10core e5-4627 2.6 Ghz	Aug-17	Jul-18	
67	IT	Blade Server	Dell	Dell-PWREdgeM830	45K70J2	HDD 1.2TB*2, RAM: 16*32GB, Processor: intel 10core e5-4627 2.6 Ghz	Aug-17	Jul-18	
68	IT	Blade Server	Dell	Dell-PWREdgeM630	32740J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Aug-17	Jul-18	
69	IT	Blade Server	Dell	Dell-PWREdgeM630	32730J2	HDD 1.2TB*2, RAM: 2*32GB,	Aug-17	Jul-18	

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						Processor: intel 4core e5-2637-2.6 Ghz			
70	IT	Blade Server	Dell	Dell-PWREdgeM630	32690J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Aug-17	Jul-18	
71	IT	Blade Server	Dell	Dell-PWREdgeM630	45K60J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Aug-17	Jul-18	
72	IT	Blade Server	Dell	Dell-PWREdgeM630	32680J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Aug-17	Jul-18	
73	IT	Blade Server	Dell	Dell M1000	32760J2	2 switchbox installed with 4 SPF transerver each	Jul-17	Jun-18	
74	IT	Blade Server	Dell	Dell-PWREdgeM830	45K50J2	HDD 1.2TB*2, RAM: 16*16GB, Processor: intel 10core e5-4627 2.6 Ghz	Jul-17	Jun-18	
75	IT	Blade Server	Dell	Dell-PWREdgeM630	326B0J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Jul-17	Jun-18	
76	IT	Blade Server	Dell	Dell-PWREdgeM630	32750J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Jul-17	Jun-18	
77	IT	Blade Server	Dell	Dell-PWREdgeM630	45K80J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Jul-17	Jun-18	
78	IT	Blade Server	Dell	Dell-PWREdgeM630	45KB0J2	HDD 1.2TB*2, RAM: 2*32GB, Processor: intel 4core e5-2637-2.6 Ghz	Jul-17	Jun-18	
79	IT	Blade Server	Dell	Dell M1000	45K90J2	2 switchbox installed with 4 SPF transerver each	Jul-17	Jun-18	
80	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNXB	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2) Processor 2.10 Ghz			CentOS Linux release 7.3
81	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNXA	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2) Processor 2.10 Ghz			
82	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNX7	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2)			

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						Processor 2.10 Ghz			
83	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNX5	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2) Processor 2.10 Ghz			Windows Server 2012 Standard
84	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNX8	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2) Processor 2.10 Ghz			
85	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNX6	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2) Processor 2.10 Ghz			
86	IT	Blade Server	Lenovo	Lenovo-9532AC1	J32GNX9	HDD (300GB X 2), DDRIII SDRAM (16GB X 2), Intel Xeon (8 Core X 2) Processor 2.10 Ghz			ubuntu 4.4.0-31generic
87	IT	Blade Server	Hp	M620	C9NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
88	IT	Blade Server	Hp	M620	49NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
89	IT	Blade Server	Hp	M620	69NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
90	IT	Blade Server	Hp	M620	99NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
91	IT	Blade Server	Hp	M620	59NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
92	IT	Blade Server	Hp	M620	B9NFD2S	HDD (146GB X 2), DDRIII			

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
93	IT	Blade Server	Hp	M620	89NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz			
94	IT	Blade Server	Hp	M620	79NFD2S	HDD (146GB X 2), DDRIII SDRAM (2GB X 16), Intel Xeon E5-2650 (8 Core X 2) Processor 2.00 Ghz	Nov-12	Nov-13	
95	IT	Rack sServer	Dell	Power Edge R715	3BVDD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
96	IT	Rack sServer	Dell	Power Edge R716	JLHDD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
97	IT	Rack sServer	Dell	Power Edge R717	HLHDD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
98	IT	Rack sServer	Dell	Power Edge R718	CHNFD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
99	IT	Rack sServer	Dell	Power Edge R719	9HNFD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
100	IT	Rack sServer	Dell	Power Edge R720	4BVDD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
101	IT	Rack sServer	Dell	Power Edge R721	DHNFD2S	HDD (300GB X 2), DDRIII	Nov-12	Nov-13	

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz			
102	IT	Rack s Server	Dell	Power Edge R722	8NNFD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
103	IT	Rack sServer	Dell	Power Edge R723	2TFGD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
104	IT	Rack sServer	Dell	Power Edge R724	BHNFD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
105	IT	Rack sServer	Dell	Power Edge R725	7NNFD2S	HDD (300GB X 2), DDRIII SDRAM (2GB X 16), AMD Opteron 6204 (4 Core X 2) Processor 3.3 Ghz	Nov-12	Nov-13	
106	IT	Blade Server	Hp	HP BL460C	SGHG24VA9R	HDD( 600GBX2 ) DDRIII (16GB X 8 ), Intel Xeon 2.6 GHz (8 Core X 2)	Sep-16	Sep-17	
107	IT	Blade Server	Hp	HP BL460C	SGHG24VA9J	HDD( 600GBX2 ) DDRIII (16GB X 8 ), Intel Xeon 2.6 GHz (8 Core X 2)	Sep-16	Sep-17	
108	IT	Blade Server	Hp	HP BL460C	SGHG24VA9N	HDD( 600GBX2 ) DDRIII (16GB X 8 ), Intel Xeon 2.6 GHz (8 Core X 2)	Sep-16	Sep-17	
109	IT	Blade Server	Hp	HP BL460C	SGHG24VA9L	HDD( 600GBX2 ) DDRIII (16GB X 8 ), Intel Xeon 2.6 GHz (8 Core X 2)	Sep-16	Sep-17	
110	IT	Blade Server	Hp	HP Proliant BL685c G7	SGH308N8SE	HDD (300 GB X 2), DDRIII SDRAM (8 GB X 8), AMD Opteron™ 16 (Core x2) Processor 6212			Oracle Linux 6.4,
111	IT	Blade Server	Hp	HP Proliant BL685c G7	SGH308N8SC	HDD (300 GB X 2), DDRIII SDRAM (8 GB X 8), AMD Opteron™ 16 (Core x2) Processor 6212			Oracle Linux 6.4,



Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
112	IT	Blade Server	Hp	HP ProLiant BL460c G8	SGH325XN40	HDD (300 GB X 2), DDRIII SDRAM (8 GB X 8), Intel(R) Xeon(R) CPU E5-2643 (8 Core x2) @ 3.30 GHz			Oracle Linux 6.4,
113	IT	Blade Server	Hp	HP ProLiant BL460c G8	SGH308N916	HDD (300 GB X 2), DDRIII SDRAM (8 GB X 8), Intel(R) Xeon(R) CPU E5-2643 (8 Core x2) @ 3.30 GHz			Oracle Linux 6.4,
114	IT	Blade Server	Hp	HP ProLiant BL685c G7	SGH308N8SN	HDD (300 GB X 2), DDRIII SDRAM (8 GB X 8), AMD Opteron™ 16 (Core x2) Processor 6212			Oracle Linux 6.4,
115	IT	Blade Server	Hp	HP ProLiant BL685c G7	SGH308N8SL	HDD (300 GB X 2), DDRIII SDRAM (8 GB X 8), AMD Opteron™ 16 (Core x2) Processor 6212			
116	IT	Blade Server	Hp	HP ProLiant BL460c G7	SGH246FHS8	HDD (300GBX2) DDR III SDRAM (8GBX2), Intel Xeon (4 Core X 2) Processor 3.20 Ghz			
117	IT	Blade Server	Hp	HP ProLiant BL460c G7	SGH246FHSE	HDD (300GBX2) DDR III SDRAM (8GBX2), Intel Xeon (4 Core X 2) Processor 3.20 Ghz			
118	IT	Blade Server	Hp	HP ProLiant BL460c G7	SGH246FHSA	HDD (300GBX2) DDR III SDRAM (8GBX2), Intel Xeon (4 Core X 2) Processor 3.20 Ghz			
119	IT	Blade Server	Hp	HP ProLiant BL460c G9	SGH610VR9V	HDD (900GBX2) DDR III SDRAM (16GBX2), Intel Xeon (6 Core ) Processor 2.4 Ghz			Microsoft Windows Server 2012 - R2 Standard Edition
120	IT	Blade Server	Hp	HP ProLiant BL460c G9	SGH610VR9S	HDD (900GBX2) DDR III SDRAM (16GBX2), Intel Xeon (6 Core ) Processor 2.4 Ghz			Microsoft Windows Server 2012 - R2 Standard Edition
121	IT	Blade Server	Hp	HP ProLiant BL460c G9	SGH610VR9T	HDD (900GBX2) DDR III SDRAM (16GBX2), Intel Xeon (6 Core ) Processor 2.4 Ghz			Microsoft Windows Server 2012 - R2 Standard Edition

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
122	IT	Blade Server	Hp	HP ProLiant BL460c G9	SGH610VR9R	HDD (900GBX2) DDR III SDRAM (16GBX2), Intel Xeon (6 Core ) Processor 2.4 Ghz			Microsoft Windows Server 2012 - R2 Standard Edition
123	IT	Blade Server	Hp	HP ProLiant BL460c G7	SGH246FHSB	HDD (300GBX2) DDR III SDRAM (8GBX2), Intel Xeon (4 Core X 2) Processor 3.20 Ghz			
124	IT	Blade Server	Hp	HP ProLiant BL460c G7	SGH246FHSC	HDD (300GBX2) DDR III SDRAM (8GBX2), Intel Xeon (4 Core X 2) Processor 3.20 Ghz			
125	IT	Blade Server	IBM	IBM -HS23	06ENGHE	HDD (300GB X 2) DDRIII SDRAM (4GB X 8 ), Intel Xeon (4 Core X 2) Processor 2.40 Ghz			
126	IT	Rack Server	IBM	IBM-SystemS824L	68ED90W	HDD (600 GB X 4 & 1200 GB X 4), DDR IV (16GB X 2, 32GB X 2, 64GB X 10) RAM, Power8 (12 Core X 2) 3.52 Ghz Processor	Augst-2017	24-05-2018	Windows 2012 Stand
127	IT	Rack Server	IBM	IBM-SystemS824L	68ED8FW	HDD (600 GB X 4 & 1200 GB X 4), DDR IV (16GB X 2, 32GB X 2, 64GB X 10) RAM, Power8 (12 Core X 2) 3.52 Ghz Processor	Augst-2017	24-05-2018	Windows 2012 Stand
128	IT	Rack Server	IBM	IBM-SystemS824L	686332AA	HDD (600 GB X 4 & 1200 GB X 4), DDR IV (16GB X 2, 32GB X 2, 64GB X 10) RAM, Power8 (12 Core X 2) 3.52 Ghz Processor	Augst-2017	24-05-2018	Windows 2012 Stand
129	IT	Rack Server	IBM	IBM-SystemS824L	686329A	HDD (600 GB X 4 & 1200 GB X 4), DDR IV (16GB X 2, 32GB X 2, 64GB X 10) RAM, Power8 (12 Core X 2) 3.52 Ghz Processor	Augst-2017	24-05-2018	Windows 2012 Stand
130	IT	Rack Server	IBM	IBM-SystemS824L	686327A	HDD (600 GB X 4 & 1200 GB X 4), DDR IV (16GB X 2,	Augst-2017	24-05-2018	Windows 2012 Stand

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
						32GB X 2, 64GB X 10) RAM, Power8 (12 Core X 2) 3.52 Ghz Processor			
131	IT	Rack Server	IBM	IBM-SystemS824L	686328A	HDD (600 GB X 4 & 1200 GB X 4), DDR IV (16GB X 2, 32GB X 2, 64GB X 10) RAM, Power8 (12 Core X 2) 3.52 Ghz Processor	Augst-2017	24-05-2018	Windows 2012 Stand
132	IT	Rack Server	Dell	Dell-PowerededgeR430	6FSSXJ2	HDD (600 GB X 6), RAM 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X 2) Processor 2.39 Ghz	Augst-2017	24-05-2018	Windows 2012 Stand
133	IT	Rack Server	Dell	Dell-PowerededgeR430	6FRRXJ2	HDD (600 GB X 6), RAM 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X 2) Processor 2.39 Ghz	Augst-2017	24-05-2018	Windows 2012 Stand
134	IT	Rack Server	Dell	Dell-PowerededgeR430	6G4NXJ2	HDD (600 GB X 6), RAM 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X 2) Processor 2.39 Ghz	Augst-2017	24-05-2018	Windows 2012 Stand
135	IT	Rack Server	Dell	Dell-PowerededgeR430	6FDTXJ2	HDD (600 GB X 6), RAM 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X 2) Processor 2.39 Ghz	Augst-2017	24-05-2018	Windows 2012 Stand
136	IT	Rack Server	Dell	Dell-PowerededgeR430	6G4PXJ2	HDD (600 GB X 6), RAM 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X 2) Processor 2.39 Ghz	Augst-2017	24-05-2018	Windows 2012 Stand
137	IT	Rack Server	IBM	Dell-PowerededgeR430	781W998	HDD (600 GB X 6), RAM 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X 2) Processor 2.39 Ghz 128 GB, Intel Xeon E5- 2609 v4 1.7 GHz (8 Core X	Augst-2017	24-05-2018	Windows 2012 Stand
138	IT	SWITCH	CISCO	Cisco-2960	FDO2117BDR1	Switch	Augst-2017	24-05-2018	Catalyst OS
139	IT	SWITCH	CISCO	Cisco-2960	FDO2117BOQU	Switch	Augst-2017	24-05-2018	Catalyst OS
140	IT	SWITCH	CISCO	Cisco-2960	FDO2117BOPV	Switch	Augst-2017	24-05-2018	Catalyst OS

Sr No	IT / NON IT	Device Type	Make	Model	Serial Number	Capacity	Date of Installation	Warranty upto	OS / IOS
141	IT	Router	CISCO	Cisco-4331	FDO2120A0D5	Router	Augst-2017	24-05-2018	CISCO IOS
142	IT	Router	CISCO	Cisco-4332	FDO2120A0D2	Router	Augst-2017	24-05-2018	CISCO IOS
143	IT	Router	CISCO	Cisco-4333	FDO2120A0D4	Router	Augst-2017	24-05-2018	CISCO IOS
144	IT	Server	Dell	Dell power edge R730	9NL9NK2	HDD (800 GB X 2), DDR IV (16GB X 8), Intel Xeon E5-2667 ( 8 Core X 1) Processor 3.20 Ghz	08-08-2017	08-07-2018	vm ware
145	IT	Server	HP	HP DL 380	CM765201U4	HDD (146 GB X 2), DDR IV (8GB X 8), Intel Xeon E5- 2667 ( 8 Core X 1) Processor 1.18 Ghz	27-08-2017	26-08-2018	CentOS release 7.0
146	IT	Server	HP	SGH534X2WT	HP Proliant DL360 Gen9	HDD (1.2TB X 2), DIMM (16GB X 13), Intel(R) Xeon®(10 Core X 2) CPU E5-2650 v3 @ 2.30GHz	01-10-2015	01-10-2016	VMWare ESXi Server, OS ESXi 5.5
147	IT	Server	HP	SGH534X2WR	HP Proliant DL360 Gen9	HDD (1.2TB X 2), DIMM (16GB X 13), Intel(R) Xeon®(10 Core X 2) CPU E5-2650 v3 @ 2.30GHz	01-10-2015	01-10-2016	VMWare ESXi Server, OS ESXi 5.5
148	IT	Server	HP	SGH534X2WL	HP Proliant DL360 Gen9	HDD (1.2TB X 2), DIMM (16GB X 13), Intel(R) Xeon®(10 Core X 2) CPU E5-2650 v3 @ 2.30GHz	01-10-2015	01-10-2016	VMWare ESXi Server, OS ESXi 5.5
149	IT	Server	HP	SGH534X2Y1	HP Proliant DL360 Gen9	HDD (1.2TB X 2), DIMM (16GB X 13), Intel(R) Xeon®(10 Core X 2) CPU E5-2650 v3 @ 2.30GHz	01-10-2015	01-10-2016	VMWare ESXi Server, OS ESXi 5.5
150	IT	Server	HP	SGH534X2WN	HP Proliant DL360 Gen9	HDD (1.2TB X 2), DIMM (16GB X 13), Intel(R) Xeon®(10 Core X 2) CPU E5-2650 v3 @ 2.30GHz	01-10-2015	01-10-2016	VMWare ESXi Server, OS ESXi 5.5

#### 4. Running Websites/Applications

S.No	Project Name	Website/ Application Name
1	Chips	<a href="https://itistock.cgstate.gov.in">https://itistock.cgstate.gov.in</a>
2	DPR	<a href="https://www.uad.cgstate.gov.in">https://www.uad.cgstate.gov.in</a>
3	FOREST	<a href="http://www.cgforest.com">http://www.cgforest.com</a>
4	FOREST	<a href="http://www.fmisonline.org">http://www.fmisonline.org</a>

S.No	Project Name	Website/ Application Name
5	FOREST	<a href="https://rvvn.cgstate.gov.in">https://rvvn.cgstate.gov.in</a>
6	KOHA	<a href="http://raipurcentrallibrary.cgstate.gov.in">http://raipurcentrallibrary.cgstate.gov.in</a>
7	KOHA	<a href="http://cglib.cgstate.gov.in">http://cglib.cgstate.gov.in</a>
8	KOHA	<a href="http://cglibadmin.cgstate.gov.in">http://cglibadmin.cgstate.gov.in</a>
9	KOHA	<a href="http://centrallibrarycitizen.cgstate.gov.in">http://centrallibrarycitizen.cgstate.gov.in</a>
10	CGMSC	<a href="https://cgmsc.gov.in">https://cgmsc.gov.in</a>
11	SLCM-PWC	<a href="https://cgvyapam.cgstate.gov.in/slcm-web-2020/vyapam/admin">https://cgvyapam.cgstate.gov.in/slcm-web-2020/vyapam/admin</a>
12	FOOD	<a href="https://khadya.cg.nic.in">https://khadya.cg.nic.in</a>
13	SLCM	<a href="https://dbt.cgstate.gov.in">https://dbt.cgstate.gov.in</a>
14	SLCM	<a href="https://vyapam.cgstate.gov.in">https://vyapam.cgstate.gov.in</a>
15	CG ROFRA	<a href="https://cgvanadhikar.cgstate.gov.in">https://cgvanadhikar.cgstate.gov.in</a>
16	Digital Secretariat	<a href="http://cgdigital.cgstate.gov.in">http://cgdigital.cgstate.gov.in</a>
17	Digital Secretariat	<a href="https://cgds.cgstate.gov.in">https://cgds.cgstate.gov.in</a>
18	Digital Secretariat	<a href="http://cgdigital.gov.in">http://cgdigital.gov.in</a>
19	CHIPS GIS	<a href="https://csidcgis.cgstate.gov.in">https://csidcgis.cgstate.gov.in</a>
20	E-district	<a href="https://edistrict.cgstate.gov.in">https://edistrict.cgstate.gov.in</a>
21	E-district	<a href="https://dashboard.cgstate.gov.in">https://dashboard.cgstate.gov.in</a>
22	E-district	<a href="http://tested.cgstate.gov.in">http://tested.cgstate.gov.in</a>
23	E-district	<a href="http://choice.gov.in">http://choice.gov.in</a>
24	NRDA	<a href="https://nrda1.cgstate.gov.in">https://nrda1.cgstate.gov.in</a>
25	CM Dashboard	<a href="https://cmdashboard.cgstate.gov.in">https://cmdashboard.cgstate.gov.in</a>
26	CGSAU	<a href="http://sau.cgstate.gov.in">http://sau.cgstate.gov.in</a>
27	E-procurement	<a href="https://eproc.cgstate.gov.in">https://eproc.cgstate.gov.in</a>
28	Sankalp	<a href="https://sankalp.cgstate.gov.in">https://sankalp.cgstate.gov.in</a>
29	AUA	<a href="https://pehchan.cgstate.gov.in">https://pehchan.cgstate.gov.in</a>
30	AUA	<a href="http://testpehchan.cgstate.gov.in">http://testpehchan.cgstate.gov.in</a>
31	CSC	<a href="https://aua.cgstate.gov.in">https://aua.cgstate.gov.in</a>
32	Mining	<a href="https://khanijonline.cgstate.gov.in">https://khanijonline.cgstate.gov.in</a>
33	Mining	<a href="http://103.51.8.74/KhanijTest">http://103.51.8.74/KhanijTest</a>
34	CDFI	<a href="https://sankalpbeta.cgstate.gov.in">https://sankalpbeta.cgstate.gov.in</a>
35	CPMU	<a href="https://cpms.cgstate.gov.in/3dspace">https://cpms.cgstate.gov.in/3dspace</a>
36	SWC	<a href="http://cgswc.cgstate.gov.in">http://cgswc.cgstate.gov.in</a>
37	Election Comission	<a href="http://cgseconno.cgstate.gov.in">http://cgseconno.cgstate.gov.in</a>
38	SEC-ER	<a href="http://cgsecerms.cgstate.gov.in">http://cgsecerms.cgstate.gov.in</a>
39	PMAYG	<a href="https://pmayg.cgstate.gov.in">https://pmayg.cgstate.gov.in</a>
40	NRDA	<a href="https://nrda.cgstate.gov.in">https://nrda.cgstate.gov.in</a>
41	E-procurement	<a href="https://sourcing.cgstate.gov.in">https://sourcing.cgstate.gov.in</a>
42	E-procurement	<a href="https://sourcingdemo.cgstate.gov.in">https://sourcingdemo.cgstate.gov.in</a>
43	CSC(common service centre)	<a href="https://csc.cgstate.gov.in/">https://csc.cgstate.gov.in/</a>
44	Rajiv Gandhi	<a href="http://cgedu.ssachhattisgarh.gov.in">http://cgedu.ssachhattisgarh.gov.in</a>
45	GGRC	<a href="http://champs.cgstate.gov.in">http://champs.cgstate.gov.in</a>
46	PSSOU(SUNDARLALSHARMA)	<a href="http://103.51.8.54/pssou">http://103.51.8.54/pssou</a>
47	Virtual education	<a href="https://stagingavidya.cgstate.gov.in">https://stagingavidya.cgstate.gov.in</a>

S.No	Project Name	Website/ Application Name
48	CPMU	<a href="https://cpmsqa.cgstate.gov.in/3dspace">https://cpmsqa.cgstate.gov.in/3dspace</a>
49	Cosmos	<a href="https://shaalakoshstate.cgstate.gov.in">https://shaalakoshstate.cgstate.gov.in</a>
50	CCTNS	<a href="http://dashboard.cgpolice.gov.in/userlogin/login.jsp">http://dashboard.cgpolice.gov.in/userlogin/login.jsp</a>
51	CCTNS	<a href="http://modules.cgpolice.gov.in/userlogin">http://modules.cgpolice.gov.in/userlogin</a>
52	CDFI	<a href="https://sankalpchips.cgstate.gov.in">https://sankalpchips.cgstate.gov.in</a>
53	CSC	<a href="https://disabilitysurvey.cgstate.gov.in">https://disabilitysurvey.cgstate.gov.in</a>
54	CHIPS GIS	<a href="https://chipsgis.cgstate.gov.in/">https://chipsgis.cgstate.gov.in/</a>
55	RDA	<a href="https://rda.cgstate.gov.in">https://rda.cgstate.gov.in</a>
56	IPEG-Sankalp	<a href="https://sankalpcg.cgstate.gov.in">https://sankalpcg.cgstate.gov.in</a>
57	Higher Education	<a href="http://highereducation.cg.gov.in/highereducation">http://highereducation.cg.gov.in/highereducation</a>
58	SETU	<a href="https://slcm.cgstate.gov.in/Setu/UserLogin.aspx">https://slcm.cgstate.gov.in/Setu/UserLogin.aspx</a>
59	CM Flagship Portal	<a href="https://cmchhattisgarh.cgstate.gov.in/">https://cmchhattisgarh.cgstate.gov.in/</a>
60	CM Flagship	<a href="https://cmflagaudit.cgstate.gov.in/">https://cmflagaudit.cgstate.gov.in/</a>
61	CG - voluntary service for COVID -19	<a href="https://coronahelp.cgstate.gov.in/">https://coronahelp.cgstate.gov.in/</a>
62	Godhan Nyay Yojna	<a href="https://godhannyay.cgstate.gov.in/">https://godhannyay.cgstate.gov.in/</a>
63	Academy	<a href="http://cgaoa.gov.in/">http://cgaoa.gov.in/</a>
64	Handicraft	<a href="https://cg handicraft.cgstate.gov.in/">https://cg handicraft.cgstate.gov.in/</a>
65	CG Parliament	<a href="https://cgparliamentary.cgstate.gov.in/">https://cgparliamentary.cgstate.gov.in/</a>
66	CG Rajbhavan	<a href="https://rajbhavancg.gov.in/">https://rajbhavancg.gov.in/</a>
67	CG DTE	<a href="https://cgdterapur.cgstate.gov.in/">https://cgdterapur.cgstate.gov.in/</a>
68	CG Map	<a href="http://cgjs.cgstate.gov.in/">http://cgjs.cgstate.gov.in/</a>
69	CG Police	<a href="https://cgpolice.gov.in/">https://cgpolice.gov.in/</a>
70	CG sericulture	<a href="https://sericulture.cgstate.gov.in/">https://sericulture.cgstate.gov.in/</a>
71	VC SWAN	<a href="https://vc.cgstate.gov.in/">https://vc.cgstate.gov.in/</a>
72	CHIIPS	<a href="https://www.chips.gov.in/">https://www.chips.gov.in/</a>
73	CG railway pvt.ltd.	<a href="https://crcl.cgstate.gov.in/">https://crcl.cgstate.gov.in/</a>
74	CG ITI	<a href="https://cgiti.cgstate.gov.in/">https://cgiti.cgstate.gov.in/</a>
75	Energy Department	<a href="http://energy.cgstate.gov.in">http://energy.cgstate.gov.in</a>
76	Future Partners	<a href="https://futurepartners.cgstate.gov.in/">https://futurepartners.cgstate.gov.in/</a>
77	GRP Rail police	<a href="https://grpraipur.cgstate.gov.in/">https://grpraipur.cgstate.gov.in/</a>
78	Haj committee	<a href="https://hajcommittee.cgstate.gov.in">https://hajcommittee.cgstate.gov.in</a>
79	Tilda college	<a href="http://gdckohka.ac.in">http://gdckohka.ac.in</a>
80	CG Labour	<a href="http://cglabour.gov.in">http://cglabour.gov.in</a>
81	Mata karma collage	<a href="http://mkgcgmhmd.ac.in/">http://mkgcgmhmd.ac.in/</a>
82	Noni suraksha	<a href="https://nonisuraksha.cgstate.gov.in/">https://nonisuraksha.cgstate.gov.in/</a>
83	Prashasan Vibhag	<a href="https://prashasanvibhag.cgstate.gov.in">https://prashasanvibhag.cgstate.gov.in</a>
84	CG Prosecution	<a href="http://cgprosecution.gov.in">http://cgprosecution.gov.in</a>
85	Panchayat and social welfare	<a href="http://cgpsw.gov.in/">http://cgpsw.gov.in/</a>
86	Panchayat	<a href="http://103.51.8.122/login.php">http://103.51.8.122/login.php</a>
87	Resident commissioner	<a href="http://rcchhattisgarh.gov.in">http://rcchhattisgarh.gov.in</a>
88	IGR	<a href="https://igrs.cgstate.gov.in">https://igrs.cgstate.gov.in</a>
89	IGR	<a href="https://epanjeeyan.cg.gov.in/IGRPortalWeb/Home">https://epanjeeyan.cg.gov.in/IGRPortalWeb/Home</a>

S.No	Project Name	Website/ Application Name
90	Sanskritmandalam	<a href="http://cgsvm.cgstate.gov.in">http://cgsvm.cgstate.gov.in</a>
91	Smartcity Raipur	<a href="https://smartcityraipur.cgstate.gov.in">https://smartcityraipur.cgstate.gov.in</a>
92	Sudhar ayog shakha	<a href="https://sarc.cgstate.gov.in">https://sarc.cgstate.gov.in</a>
93	Poshan abhiyan	<a href="https://shuposhitchhattisgarh.cgstate.gov.in">https://shuposhitchhattisgarh.cgstate.gov.in</a>
94	CG WCD	<a href="http://cgwcd.gov.in">http://cgwcd.gov.in</a>
95	Jansampark Vibhag	<a href="http://dprcg.gov.in">http://dprcg.gov.in</a>
96	CECB	<a href="https://cei.cgstate.gov.in">https://cei.cgstate.gov.in</a>
97	CREDA	<a href="https://creda.cgstate.gov.in">https://creda.cgstate.gov.in</a>
98	Raipur Police	<a href="https://raipurpolice.cgstate.gov.in">https://raipurpolice.cgstate.gov.in</a>
99	Law Department	<a href="https://law.cgstate.gov.in">https://law.cgstate.gov.in</a>
100	Rent Control Department	<a href="https://rct.cgstate.gov.in">https://rct.cgstate.gov.in</a>
101	CSIDC	<a href="https://csidc.cgstate.gov.in">https://csidc.cgstate.gov.in</a>
102	CSIDC	<a href="https://csidconline.cgstate.gov.in">https://csidconline.cgstate.gov.in</a>
103	CSIDC	<a href="https://csidc.in">https://csidc.in</a>
104	RERA	<a href="https://rera.cgstate.gov.in">https://rera.cgstate.gov.in</a>
105	State Portal	<a href="https://cgstate.gov.in">https://cgstate.gov.in</a>
106	EDU APP	<a href="http://eduapp.cgstate.gov.in">http://eduapp.cgstate.gov.in</a>
107	Food	<a href="https://legalmetrology.cg.nic.in">https://legalmetrology.cg.nic.in</a>
108	Food	<a href="https://markfed.cg.nic.in">https://markfed.cg.nic.in</a>
109	CG School	<a href="https://cgschool.in">https://cgschool.in</a>
110	SUDA	<a href="https://morebus.net/cbits/index.php">https://morebus.net/cbits/index.php</a>
111	SUDA BUILDING PERMISSION	<a href="https://bpms.sudacg.in">https://bpms.sudacg.in</a>
112	CG School	<a href="http://shiksha.cg.nic.in">http://shiksha.cg.nic.in</a>
113	Patel Commission	<a href="https://cgqdc.in">https://cgqdc.in</a>
114	Regional Science Centre	<a href="http://rsc.cgstate.gov.in">http://rsc.cgstate.gov.in</a>
115	E-Samiksha	<a href="https://cgcamp.cgstate.gov.in">https://cgcamp.cgstate.gov.in</a>
116	Janshikayat	<a href="https://cmjanshikayat.cgstate.gov.in">https://cmjanshikayat.cgstate.gov.in</a>
117	ROW	<a href="https://row.cgstate.gov.in">https://row.cgstate.gov.in</a>
118	Gouthan	<a href="https://gauthanmap.cgstate.gov.in">https://gauthanmap.cgstate.gov.in</a>
119	DPCG	<a href="http://dpcg.cgstate.gov.in">http://dpcg.cgstate.gov.in</a>
120	Panchayat	<a href="http://cgpanchayat.cgstate.gov.in">cgpanchayat.cgstate.gov.in</a>

Capital Expenditure for CGSDC (Table 1)		
Sr. No.	Item Description	Unit of Measurement
<b>A</b>	<b>IT Components</b>	
1	Rack Server	Nos
2	Hyper Converged Infrastructure	Nos
3	Virtualisation Software and Management Solution for Rack server Cluster	Nos
4	Windows Operating System Data Center Edition - 16 Core License Model	Nos
5	Redhat Linux Operating System Enterprise Edition - Socket Based	Nos
6	MS SQL Database Enterprise Edition - Core Based	Nos
7	Postgres SQL Enterprise Edition - Core Based	Nos
8	Backup Hardware & Software (500 TB front end capacity or 500 VM)	Nos
9	Server Load Balancer	Nos
10	SDN Controller	Nos
11	SPINE Switch	Nos
12	Leaf switch – OFC	Nos
13	Core Router – Internet	Nos
14	Core Router – Intranet	Nos
15	Management Switch	Nos
16	Link Load balancer – Internet	Nos
17	Link Load balancer – Intranet	Nos
18	L2 Managed Switch for NOC	Nos
19	SAN Switch	Nos
20	Enterprise Storage (500 TB Usable Storage)	Nos
21	Next Generation Firewall – Internet	Nos
22	Next Generation Firewall – Intranet	Nos
23	Web Application Firewall	Nos
24	EDR - Endpoint Detection Response	Nos
25	Identity Access Manager	Nos
26	Enterprise Monitoring System (NMS, ITSM, ISMS)	Nos
27	Network Access Controller	Nos
28	HSM - Hardware Security Module	Nos
29	HIPS - Host Intrusion Prevention System	Nos
30	NDR - Network Detection and Response	Nos
31	DDoS	Nos
<b>B</b>	<b>Non IT Components</b>	
1	UPS - 300 KVA with battery bank upgradable to 400 KVA	Nos
2	Battery Bank for 300 KVA - Min 4 Hrs backup	Lot
3	UPS - 20 KVA with Battery Bank	Nos
4	Battery Bank for 20 KVA - Min 4 Hrs backup	Lot
5	Split AC - 1.5 Ton	Nos
6	Split AC - 2 Ton	Nos
7	HVAC System - Precision Air Conditioner	Nos
8	Biometric Door Access System	Nos
9	Smart TV - 55 inch	Nos
10	Smart TV - 75 inch	Nos
11	Data Center Infrastructure Management (DCIM)	Nos
12	Ultrasonic Rodent Repellent System	Nos
13	Water Leak Detection System	Nos
14	Intelligent Addressable Fire Alarm System	Nos
15	Smoke Detection System	Nos
16	Fire Suppression System	Nos
17	Master Control Unit	Nos



18	Distribution Transformer, 750 kVA 11kV Oil filled, On Load Tapp including substation protection and metering devices	Nos
19	42U Rack (Network + Server)	Nos
20	DG Set 380 KVA (D Check & Fuel Refilling)	Nos
21	Advanced Building Management System (BMS)	Nos
22	Structured Cabling	Lot
23	Loaded Fiber Enclosure for Type I MPO Cassettes	Lot
24	Passive Cabling	Lot
25	Fiber Optic solutions for DC Connectivity	Lot
26	Fiber Panel	Lot
27	CAT6A U/UTP Cable	Lot
28	24 Port Patch Panel loaded	Lot
29	CAT6 I/O for loaded Patch Panel	Lot
30	CAT6A Patch Cord	Lot
31	MFZ Verifocal Dome	Nos
32	Bullet Camera	Nos
33	PTZ Camera	Nos
34	Power Cables	Lot
C	Civil & Interior	
1	One time Site Preparation (Civil & Electrical) Cost for DC including complete site preparation of Data Center, inclusive but not limited to false flooring, lighting fixture, electrical works, Mason Works, Dismantling existing Wall, Doors, Window or any structure of any material etc(Refer Scope of Work for further details)	Lot
2	EARTHING: Preparation of All Earth Pits, Necessary Repair, Testing earth resistivity and electrode resistance	Lot
3	Electrical works - for NOC, DC, DG Set UPS and LT Panel	Lot
4	Setting up of state of the art NOC room with required Furniture and other components including false flooring, lighting fixture, electrical works, beautifications of NOC area, wall panels, Mason Works, etc. (Refer Scope of Work for further details)	Lot
D	One time cost for Connectivity	
1	Provisioning 1 GBPS MPLS Connectivity	Lumpsum
E	Data Centre Certification	
1	ISO 27001, ISO 20000, ISO 22301 and Surveillance Audit including Recertification	Lumpsum
<b>Total CAPEX (A)</b>		

[illegible]

1		-
8		-
1		-
1		-
1		-
1		-
1		-
1		-
1		-
1		-
1		-
1		-
1		-
1		-
24		-
2		-
2		-
1		-
1		-
1		-
1		-
1		-
1		-