Annexure-1

1. Scope of Work

RailTel Customer intends to engage for setting up RailTel Customer Data Centre Business Continuity and Disaster recovery site on cloud. CSP (cloud service provider) shall be responsible for Design, Development, Delivery, Configuration, Implementation, Testing, Data Migration, Commissioning and Operations & Maintenance of RailTel Customer Data Centre Business Continuity and Disaster recovery site. The objective of this RFP is to provide and manage -

1- Disaster Recovery Center as Manage Service

2- DR Site as Backup & Archive as Manage Service

The scope of work of the RFP is to provide DR on Cloud Services, Migration (RailTel Customer Data Centre to Cloud Site) of the existing few major applications of RailTel Customer which are to be provided cloud service support, professionals services from CSP though not limited to the given scope.

1- Setup the cloud account of the proposed Cloud service provider, The Bidder would be responsible for providing cloud for setting up, installation, configuration, management, up gradation, database servers/storage, security etc. and also maintain and manage and configure the VMs, Storage, Network, Database etc.

2- The Bidder will support RailTel Customer application service provider for implementation, management and monitoring of DDOS, IPS, IDS Services, anti-malware, vulnerability scanning and penetration testing etc. to be configured for our application and ensure 99.98 % uptime of services as per agreement.

3- The Bidder is expected to understand the complete architecture of existing applications. The Bidder shall be responsible for deployment of Security patches on cloud platform in coordination with the RailTel Customer Data Centre.

4- The bidder shall be responsible to monitor and manage the cloud services.

5- Bidder will provide the support to application service provider for Deployment of New Applications on cloud, security administration, planning and implementation of cloud management and monitoring portals for complete infrastructure and services procured and reporting services.

6- Bidder shall provide minimum 2 Cloud engineers/cloud professionals throughout the contract period to support the client/ RailTel Customer Data Centre /application service provider as per the BoM.

7- Service provider shall be responsible for security of resources, Network infrastructure along with implementation security compliances.

8- Service provider shall be responsible for any Risk Management and planning, or issues related to migration of data from DC to DR as per the requirements (If any).

9- Service provider shall provide necessary technical documentations, design documentations, standard Operating Procedures (SOPs) required for operations and management of services.

10- The bidder shall assist RailTel Customer Data Centre in planning for capacity building to meet growth and peak load assessment from time to time, to ensure future requirements of RailTel Customer Data Centre are addressed.

11- The bidder shall provide necessary details including sizing, current loads, utilization, expected growth/demand and other details for scale up/scale down at the end of first year in close coordination with RailTel Customer Data Centre Team.

12- The bidder shall provide the relevant reports, including real time as well as past data/reports on dashboard as per the requirement of the project.

13- Service provider shall be responsible for conduct of Business Continuity and follow Standard Operating Procedures (SOP) and inform RailTel Customer Data Centre in advance for such drills conducted twice a year normally, with 15 days' prior notice.

14- The Service Provider will train and transfer the knowledge to the replacement agency or RailTel Customer to ensure continuity and performance of services post expiry of Contract if required.

15- Optimize the resources/manage services for optimum billing with satisfactory service.

16- Provide report on utilization and optimization of the resources.

17- Provide portal logins for billing, provisioning, usage etc. as per the requirement of the projects also the bidder will provide the access of root account of CSP to RailTel Customer.

18- Provide support at any time (24 hours a day, 7 days a week) via all possible modes including phone, chat, and email support to RailTel Customer and its DCO for provisioning and configuring cloud resources

19- The bidder will provide the dashboard for monitoring and financial aspects as per the bid document requirement

20- If any new guidelines are published by MeitY which CSPs are required to adhere to, RailTel will not bearany responsibility or cost associated with adherence to these guidelines by the CSPs.

21- The bidder will submit the quarterly invoice based on actual consumption.

22- No consortium will be allowed.

23- The bidder should ensure that there should not be any data loss during migration (if any).

24- After the end of the contract period, as part of the exit process, cloud service provider will delete/remove VMs, contents and data with approval of DIC and ensure data cannot be forensically recovered and intimation of compliance thereafter.

25- The bidder should ensure fault-tolerance and provide business continuity plan. In case of failure, automated processes should shift application traffic to the redundant hosts.

26- It is assumed that backup of applications is provisioned by the bidder in proposed cloud service, meeting all the service requirements. In case of failure, automated processes should move customer data traffic away from the affected area to the failover site. Applications should be deployed in such a way that in the event of a Data Centre failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites, for which adequate bandwidth be available. Seamless movement of traffic must happen in case of a failure at the Active Site

27- The CSP & Bidder should ensure the Data at Rest or in Motion should at all times remain in India.

28- The proposed CSP should provide adequate bandwidth between their Data Centre Facilities to provide business continuity. In the event of a Primary site failover or switchover, failover site should take over the active role, and all requests should be routed through that site.

29- RailTel reserves the rights to cancel the bid at any stage without giving any reason

30- The bidder, during exit/ termination/ expiry of contract, must have to provide support to RailTel Customer / its partner regarding knowledge transfer, covering data, code, architecture design etc. as per therequirements.

2. **Phase wise details are as-**

A. Phase I- (Migration from RailTel Customer Data Centre to CSP Site)

This phase shall comprise the following:

a. Complete understanding of the architecture of applications/projects

b. Identification of all the components of the technology stack, their dependencies & integrations – both internal and external, configurations, keys and certificates, domain settings, security settings etc.

c. Establishing connectivity between RailTel Customer Data Centre and DR Site for data migration, testing and live within 21 days after signing contract.

d. Deploy manpower onsite within 07 days of contract signing

e. Deployment of all the components of the stack on the Bidder's proposed CSP's infrastructure in their respective environments (dev, staging, production etc.).

f. Data transfer: The Bidder shall provide all necessary support and tools for data transfer to the proposed CSP such as VPN tunnel for data transfer, data transfer tools etc. There shall be no additional cost implication for this and shall be covered under the Migration service.

g. During the migration period to The Bidder shall bring manpower with necessary technical experts to carry out the migration work. The resources should comprise of and not limited to - Delivery/Migration Manager, Cloud Solution Architect, Cloud Engineer, Cloud System Administrator, Cloud Database SME, Cloud Security Expert. Technical evaluation of the Bidder shall include quality of these resources based on their expertise and understanding of the projects. The Bidder shall ensure that SME resources are deployed in the migration process

h. Bidder shall be responsible for security of resources, network infrastructure along with implementation of security compliances.

B. Phase 2 - Go-Live

For the purpose of RFP, "Go-Live" is defined as the date on which all the projects/applications are completely operational in the production environment in a state (functionalities, performance, security etc.) same as the currently deployed ones and accepted by RailTel

C. Phase 3 -Stabilization

The Bidder shall be responsible for stabilization of the redeployed projects/applications. The Stabilization period is defined as the period during which the bidder has to do a parallel run of both the systems at the RailTel Customer Data Centre

as well as the selected CSP. The stabilization period will be for a period of 21 days (3 weeks) after Go-Live to ensure success of the migration to the CSP.

Phase 4 -Operation and Maintenance – The bidder shall be responsible for providing O&M service for the DR Setup till duration of the contract.

Note – RailTel Customer may asked bidder to provide DR Service for more applications. For these application bidder shallfollow the same process as defined above and rate shall be consider from rate card.

3. Overview of Scope for Cloud Services

Bidder shall be responsible for below mentioned activities but not limited to:

1. The bidder shall be responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of RailTel Customer Data Centre and meet the RPO and RTO requirements.
2. RPO/RTO requirement of application shall be as per below table:

RPO (Minute)	RTO (Minute)
15	30

3. Bidder shall meet the above mentioned RPO/RTO for entire contract duration. However, during the change from Primary DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the bidder shall be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.
4. DC/DR would operate in an active passive state with 100% allocated storage replicated from primary to DR site.
5. *Apart from maintaining RTO/RPO CSP Service Inclusions:*
   - *i. Tools disaster recovery management and replication*
   - *ii. During the change from DC-Cloud to DR-Cloud or vice-versa (regular planned changes), there should not be any data loss.*
   - *iii. There shall be asynchronous replication of data between DC Cloud and DR-Cloud.*
   - *iv. During normal operations, the DC-Cloud will serve the requests. The DR-Cloud site will not be performing any work but will remain on standby.*
   - *v. DC-Cloud Storage shall be replicated (Active-Passive) on an ongoing basis at DR-Cloud site, as per the required RPO, RTO and replication strategy.*
   - *vi. In the event of a site failover or switchover, DR-Cloud site will take over the active role, and all the requests will be routed through that site.*
   - *vii. Application data and application states will be replicated between the two sites so that when an outage occurs, failover to the surviving DR-Cloud can be accomplished within the specified RTO. This is the period during which the compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC-Cloud shall be provided.*
   - *viii. The security at the DC-Cloud and DR-Cloud shall be same.*
   - *ix. The CSP shall conduct DR drill once in every three months of operation wherein the DC-Cloud has to be deactivated and complete operations shall be carried out from the DR-Cloud site. However, during the change from DC-Cloud to DR-Cloud or vice versa (or regular planned changes), there should not be any data loss.*
   - *x. Automated switchover/ failover facilities (during DC-Cloud failure & DR Drills) to be provided*
   - *xi. The switchback mechanism shall also be automated.*

xii. *The (CSP) is responsible for provisioning all necessary software and solutions to successfully fulfill the scope of work and objectives outlined in the RFP without additional cost.*

7. ***In case during DR activity if storage exceeds allocated the differential part MSI should invoice separately.***

8. The Primary DC (RailTel Customer Data Centre) and the DRC 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. DR Database/Storage shall be replicated on an ongoing basis and

   Shall be available in full (100% of the **PDC**) as per designed RTO/RPO and replication strategy. The Storage should be 100% of the capacity of the Primary Data Centre (PDC) site
9. 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 centers so that when an outage occurs, failover to the surviving data Centre can be accomplished within the specified RPO/RTO
10. 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.
11. The bidder shall conduct DR drill at the interval of every quarter. Total duration of drill activity performed during contract period of three years should be minimum 10 hours. During drill 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 DRC or vice-versa (regular planned changes), there should not be any data loss.
12. Bidder has to demonstrate one successful DR drill before Go-Live.
13. The bidder shall clearly define the procedure for announcing DR based on the proposed DR Cloud solution. The bidder 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.
14. The bidder 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.**
15. The bidder 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.
16. Bidder shall provide access of web console/dashboard to monitor the SLA and availability of resources.
17. Bidder shall provide Sufficient (to meet RPO & RTO Defined as per Scope in this RFP) private dedicated link/bandwidth connectivity between RailTel Customer Data Centre and CSP premise/Data Centre where DR is going to be hosted with unlimited upload and download of data in High Availability Mode.

18. Bidder 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 RailTel Customer. Bidder shall be responsible for the security of the "guest" Operating System (OS) and any additional software including the applications running on the guest OS.
19. 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.
20. deleted
21. Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.
22. Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.
23. Bidder shall create non-production environments and segregate (in a different VLAN) nonproduction environments from the production environment such that the users of the environments are in separate networks
24. 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.
25. Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures.
26. The respective Government Department / Railel shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.
27. The respective Government Department / RailTel Customer Data Centre retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
28. The respective Government Department / RailTel retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.
29. RailTel Customer shall be provided access rights (including the underlying secure connection) to the user administration / portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc.
30. CSP shall not provision any unmanaged VMs for the applications.
31. CSPs shall provide interoperability support with regards to available APIs, data portability etc., for the Government Department to utilize in case of Change of, migration back to in-house infrastructure, burst to a different for a short duration or availing backup or DR services from a different service provider.
32. Should adhere to the ever-evolving guidelines as specified by CERT-IN (http://www.cert- in.org.in/)
33. 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.

35. Bidder shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.
36. The empaneled cloud service offerings must comply with the additional guidelines / standards (applicable for the Empaneled Cloud Service Offerings) as and when such guidelines / standards are published by MeitY at no additional cost to retain the empanelment status.
37. Bidder shall provide a self-service/orchestration platform so that RailTel Customer team can provision IT resources like virtual machines, storage volume, archival data as they require

4. Detailed Scope of Work for Cloud Services

4.1 Resource Management

1. Adequately size the necessary compute, storage and other cloud services required, building the redundancy wherever necessary into the architecture and load balancing to meet the service levels.
2. While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information provided in the RFP, subsequently, it is expected that the Bidder, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, and storage as per the performance requirements of the Cloud solution and meet the SLAs using the auto-scaling features (through an user-friendly dashboard) provided by the CSP.
3. In addition to auto-scaling, for any major expected increase in the workloads, carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the Cloud solution.
4. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by RailTel. The Service Provider shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.

4.2 Virtual Machine Requirements

1. Service shall provide auto-scalable, redundant, dynamic computing capabilities of virtual machines
2. Service shall allow Government Department/ CUSTOMER authorized users to procure and provision computing services or virtual machine instances online with two factor authentications via the SSL through a web browser
3. Service shall allow users to securely and remotely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet.
4. Perform an Image backup of Customer VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into a Government Department's approved image format
5. Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the

SSL VPN clients only as against the public internet.

6. In case of suspension of a running VM, the VM shall still be available for reactivation for reasonable time without having to reinstall or reconfigure the VM for the Government Department solution. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered.
7. The bidder shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions.
8. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
9. CPU (Central Processing Unit) - CPU options shall be provided as follows:
    - A minimum equivalent CPU processor speed of 2.4GHz shall be provided.
    - The CPU shall support 64-bit operations
10. Provide hardware or software based virtual load balancer Services (VLBS) through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform.
11. Provide hardware or software based virtual load balancing as a service to provide stateful failover and enable Customers to distribute traffic load across multiple servers.
12. Operating System (OS)
    - Service shall support one or more of the major OS such as Windows, LINUX. o Management of the OS processes and log files including security logs retained in guest VMs;
    - Provide anti-virus protection;
    - Provide OS level security as per CSP standard operational procedures as defined in the Information Security Controls for Cloud Managed Services and supporting documentation;
13. Persistence
    - Persistent Bundled Storage is retained when the virtual machine instance is stoppedor
    - Non-Persistence – Non-Persistence Bundled Storage is released when the virtual instance is stopped. If quoting Non-Persistence VM, the CSP shall provide VM Block storage
14. RAM reserved for virtual machine instance or Computing supporting a minimum of 1GB of RAM. Memory (RAM) requirement should be different for different type of servers such as web servers and database servers.
15. RailTel retains the right to request full copies of these virtual machines at any time.
16. RailTel Customer retains ownership of Department loaded software installed on virtual machines and anyapplication or product that is deployed on the Cloud by the Government Department.
17. Support a secure administration interface - such as SSL/TLS or SSH - for the Government Department designated personnel to remotely administer their virtual instance
18. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption
19. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing
20. Cloud provider should offer fine-grained access controls including role-based access control, use of SSL certificates, or authentication with a multi-factor authentication.
21. Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
22. Government Department should be permitted to bring and upload additional properly licensed non-

operating system software for operation in cloud as required for the Government Departmentsolution for use within the Services by installing it directly on a VM.

23. Provide facility to configure virtual machine of required vCPU, RAM and Disk.
24. Provide facility to use different types of disk like SAS, SSD based on type of application.

8.3.3 Cloud Storage Service Requirements

1. Service shall provide users with the ability to procure storage with two factor authentications via the SSL through a web browser and manage storage capabilities remotely via the SSL VPN clients as against the public internet.
2. Data Transfer Bandwidth: Bandwidth utilized to transfer files/objects in/out of the providers infrastructure supporting a minimum of 100GB of data transferred (in and out) within 1 hour via the network
3. There shall not be any additional costs associated with data transfer over and above the ordinary bandwidth charges, or for bulk transfer for ITDA.

8.3.4 Data Management

1. The CSP should provide tools and mechanism to the ITDA or its appointed agency for defining their backup requirements & policy.
2. The CSP should provide tools and mechanism to the ITDA or its appointed agency for configuring, scheduling, performing and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.
3. Transfer data back in-house either on demand or in case of contract or order termination for any reason
4. Provide and implement security mechanisms for handling data at rest and intransit.
5. Bidder shall not delete any data at the end of the agreement (for a min of 60 days beyond the expiryof the Agreement) without the approval of the State.
6. When the State or CSP (with prior approval of the state Government/ ITDA) scales down the infrastructure services, CSP is responsible for deleting or otherwise securing Government Department's Content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.

8.3.6 Monitoring Performance and Service Levels

1. Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues
2. Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels
3. Monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service Detecting and reporting service level agreement infringements
4. Monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access within the 's boundary

8.3.7 Usage Reporting and Billing Management

1. Track system usage and usage reports

2. Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects
3. Provide the relevant reports including real time as well as past data/information/reports to validate the billing and SLA related penalties

8.3.8 Backup

1. Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by RailTel.
2. Restore from the backup whenever required.

8.3.9 Business Continuity Services

Provide business continuity services in case the primary site becomes unavailable.

8.3.10 Support for third party audits

Enable the logs and monitoring as required to support for third party audits

8.3.11 Miscellaneous

1. Advise on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.
2. Interface with the (s) on behalf of RailTel for all activities including monitoring the reports (e.g., usage, security, SLA,), raising (or escalating) tickets / incidents and tracking the same to resolution.

8.3.12 Regular Reporting and Support to RailTel Customer

1. Bidder should provide training to RailTel nominated officials/personnel on usage of the Console/ Infrastructure etc and any other technical aspect for monitoring of project.
2. Bidder shall implement the audit & compliance related cloud services to enable RailTel to monitor the provisioned resources, performance, resource utilization, and security compliance:
    - Availability of the cloud services being used
    - Summary of alerts that are automatically triggered by changes in the health of those services.
    - Summary of event-based alerts, providing proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources
    - Reports providing system-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources
    - Auto-scaling rules and limits
    - In case of any un-authorized access, the Agency should provide logs of all user activity within an account , with details including the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing
    - Report of all of the provisioned resources and view the configuration of each.
    - Summary of notifications, triggered each time a configuration change
    - Incident Analysis in case of any un-authorized configuration changes.
    - Summary of alerts with respect to security configuration gaps such as overly permissive access to

certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies

- Summary of security assessment report that identifies the possible improvements (prioritized by the severity) to the security and compliance of applications deployed on cloud

Report on upcoming planned changes to provisioning, either possible optimizations, if any, indicating how the underutilized services can be reduced to optimize the overall spend, or required enhancements (e.g., upgrade to additional storage) to meet the service levels definedin the RFP.

- Summary of resource usage in a console and the charging/billing monthly on basis of pay per use.

8.3.13 Patch & Configuration Management

Manage the instances of storage, compute instances, and network environments. This includes department-owned & installed operating systems and other system software that are outside of the authorization boundary of the CSP. Bidder is also responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations

8.3.14 User Administration

1. Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.
2. Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the useraccount
3. Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it

8.3.15 Server Security & HIPS

1. The server security solution should support state full Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring and Recommended scan in single agent for physical, virtual and cloud instances.
2. The server Security solution should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Eg. Selecting rules, configuring policies, updating policies, etc.) And provide automatic recommendation of removing assigned policies if vulnerability no longer exists - For Example - If a patch is deployed unwanted signatures should be un-assigned automatically.
3. The server Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub- directories, and other features and Solution Should have pre and post execution machine Learning and should have Ransom ware Protection in behavior Monitoring.
4. The Server Security Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window.
5. Should support prevention against script-based attacks used to deliver malware such as ransomware
6. The server security solution should protect against Distributed DoS attack and Solution should have the ability to lock down a computer (prevent all communication) except with management server.

The Server security HIPS Solution Should not have the need to provision HIPS Rules from the Policy Server as the Rules should be automatically Provisioned and recommended according to vulnerabilities.

. The Server Security solution should support pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.

8.3.16 Security Administration

1. Appropriately configure the security groups in accordance with the RailTel Customer Data Centre's networking policies.
2. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
3. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
4. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.
5. Properly implementing anti-malware and host-based intrusion detection systems on their instances,as well as any required network-based intrusion detection systems in accordance with the RailTel Customer Data Centre's Security policies.
6. Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their RailTel Customer Data Centre's Security policies.
7. Review the audit logs to identify any unauthorized access to the RailTel Customer Data Centre's systems.

8.3.17 Legal Compliance Requirements

1. Meet the ever-evolving security requirements as specified by CERT-In and GCC compliance
2. All services acquired under this application document including data will be guaranteed to reside inIndia only.
3. There shall not be any legal frameworks outside Indian Law applicable to the operation of the service.
4. CSPs should be prepared to submit the necessary artifacts and the independent verification within the timeframe determined by State once the guidelines & standards are published by Cert- in/State.
5. CSP is responsible for all costs associated with implementing, meeting, assessing, documenting and maintaining the empanelment/ proving the service.
6. If the CSP fails to meet the guidelines & standards as set by State, the state reserves the right to terminate the contract and request to move to a different CSP that meets the mandatory guidelines & standards at no additional cost to state. The Exit Management provisions shall come into effect insuch a scenario.
7. CSP shall not publish or disclose in any manner, information, without the State's written consent, thedetails of any safeguards either designed or developed by the CSP under the agreement or otherwiseprovided by the state.
8. CSP shall adhere to the privacy safeguards as laid down by the State and Government Department etc.
9. To the extent required to carry out a program of inspection to safeguard against threats and hazardsto the security, integrity, and confidentiality of any non-public Government data collected and storedby the CSP, the CSP shall afford the state or its nominated agency access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.

   If new or unanticipated threats or hazards are discovered by either the state or Government Department, Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of CERT-In and the other party.

8.3.18 Change Management

1. Basic scope of work shall be as per the complete requirements as detailed in this RFP document.
2. Any change in scope of work shall be handled separately by the CSP under the supervision of Composite Team/ RailTel Customer.
3. Any change/addition/deletion in scope shall be mutually agreed between RailTel Customer and CSP. The

same should be approved by the Department of IT.

4. The RailTel Customer may at any time, by a written order can make changes to the current scope of the work with the mutual agreement with CSP.
5. Any such changes resulting in increase or decrease in cost or time lines of any part of the work under the contract, an equitable adjustment shall be made in the contract value / time schedule or both and the contract shall be amended accordingly.
6. Any claims by the CSP for adjustment under this clause must be ascertained within seven (7) days from the date of receipt of the change order from RailTel Customer.

8.3 Support in Migration of existing applications and data to Cloud DR:

1. Design the To-Be architecture for deployment on Cloud along with the Day-1 requirements.
2. Provision the necessary compute, storage, and other necessary cloud services on the cloud to host the applications/websites.
3. Provide support to RailTel Customer in migration of the applications/websites from the existing infrastructure to the cloud infrastructure as per the defined To-Be architecture. The migration shall also include the migration of underlying data & files from the current database(s) / storage into the database(s) / storage on the cloud.

Note: The ownership of the Purchaser's Content related to Application, Databases etc., at any point of time during the contract or expiry or termination of the contract, shall rest with RailTel Customer.

8.4 Roles & Responsibilities

8.5.1 Cloud Service Provider (CSP)

Following are the responsibilities of the CSP but not limited to:

CSP shall be responsible for provisioning the underlying system software, infrastructure, and cloud services for deployment and hosting of all the Client applications on the infrastructure provided by leading in the form of Infrastructure as a Service (IaaS)

- CSP shall be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP
- CSP shall be responsible for DR drill on each quarter for the period of minimum 10 hours as specified in this RFP with the approval from RailTel Customer. For any actual Disaster Recovery CSP shall get written approval from RailTel Customer to trigger DR.
- CSP shall coordinate with the RailTel Customer for hosting of applications and migration of data to the proposed cloud environment.
- The CSP shall be responsible for provisioning the necessary compute, memory, and storage as per the recommendations of the Composite Team
- For any additional software procured, the CSP shall provide the Annual Technical Support (ATS) from the OEM during the entire period of the contract.
- Shall provide Infrastructure-as-a-Service (IaaS) with the required operating system.
- CSP shall be responsible for overall co-ordination with OEM shall assist CUSTOMER in all ongoing operations.
- CSP shall report to SDC Project Manager / Co-Ordinator appointed by the Railtel Customer for entire contract duration.

- RailTel Customer shall not bear any AMC / CAMC cost during the entire contract period. RailTel Customer shall pay only the usage charges as per final bidding price on quarterly basis after completion of the each quarter, CSP shall submit the tax invoice.

8.5.2 RailTel Customer Composite Team

Following are the responsibilities of the RailTel Customer /Composite Team

- Project Manager appointed by the RailTel Customer /Composite Team shall approve the DR drill window suggested by CSP for each quarter and ensure CSP integrate well to host services from cloud within defined time limits
- Shall assist CSP for data migration from existing RailTel Customer Data Centre to CSP DR
- Shall assist CSP for getting all the necessary details from existing RailTel Customer Data Centre which shall be required to setup DR on cloud
- Shall assist to resolve all the issue reported by CSP time to time
- Participate in all scheduled project activities, attend scheduled meetings and promptly respond to new meeting requests, requests for information, technical support or other necessary communication activities;

on or permits required for performing works in the project area;

- Shall assist in obtaining necessary permits or permissions for any activities requiring outside authorization;
- Timely acquisition of required technical data from DCO or other parties;
- Obtaining any new, changed, or updated operational information necessary for the CSP to configure and initialize the system; and
- Client shall have dedicated access to all virtual machines, templates, clones, and scripts/applications created for various applications, any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or shall be able to retrieve) full copies of these virtual machines at any time.

8.5.3 PMC (Project Management Consultant) / RailTel Customer Data Centre

- Project Management and Monitoring to ensure conformity to Industry Specific standards.
- Weekly Status/ fortnight/monthly Reports for the works of the selected CSP including progress,issues, risks, support required etc.
- Shall ensure conformity to designated standards and specifications through Quality Control and Assurance
- Shall be responsible for change Control Management to ensure consistent integration betweenthe Design and Implementation.
- Shall be responsible for Overall governance and co-ordination
- Shall be responsible for SLA calculation and payment recommendation on the basis of system generated reports

Shall be responsible for Final acceptance testing. A detailed roles & responsibility of RailTel Customer has been defined in Annexure- VI: RASCI Matrix.

8.5 Exit Management / Transition-Out Services

Continuity and performance of the Services at all times including the duration of the Agreement and postexpiry

of the Agreement is a critical requirement of RailTel Customer. It is the prime responsibility of Bidder toensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded. Responsibilities of the Bidder with respect to exit management / transition-out services include:

1. Provide a comprehensive exit management plan
2. Provide necessary handholding and transition support for any other service provider to ensure the continuity and performance of the services to the complete satisfaction of RailTel Customer
3. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date

Migration of the VMs, data, content and any other assets to the new environment created by the RailTel Customer or any Agency (on behalf of RailTel Customer) on alternate 's offerings to enable successful deployment and running of the applications / websites on the new infrastructure by providing a mechanism to Department for the bulk retrieval of large amounts of data, scripts, software, virtual machine images, and so forth using secure appliances into and out of the CSP's cloud without incurring high network costs, long transfer times and security concerns

5. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest with RailTel Customer only
6. Ensure that all the documentation required by RailTel Customer for smooth transition including configuration history are and all such logs are handed over to RailTel Customer during the exit managementprocess.
7. Shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiryof the Agreement) without the express approval of RailTel Customer. RailTel Customer shall pay for the cost for retaining the data as per the prices discovered in the commercial bid
8. Once the exit process is completed, remove the RailTel Customer Data's data, content and other assets from thecloud environment and certify that the VM, Content and data deletion to RailTel Customer
9. There shall not be any additional costs associated with the Exit / Transition-out process other than the cost of cloud services utilized for such transition. The managed services cost to support the exit management / transition should be factored in the commercial bid of the bidder

10. Train and transfer the knowledge to the RailTel Customer team to ensure similar continuity and performance of the Services post expiry of the Agreement

11. RailTel Customer shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.
12. RailTel Customer retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right torequest (or should be able to retrieve) full copies of these virtual machines at any time.
13. RailTel Customer retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.
14. RailTel Customer shall be provided access rights (including the underlying secure connection) to the user administration / portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the.
15. CSP shall not provision any unmanaged VMs for the applications.
16. CSPs shall provide interoperability support with regards to available APIs, data portability etc., for the Government Department to utilize in case of Change of, migration back to in-house infrastructure, burst to a different for a short duration or availing backup or DR services from a different service provider.
17. Should adhere to the ever-evolving guidelines as specified by CERT-IN (http://www.cert- in.org.in/)

18. 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.

19. Bidder shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.

20. The empaneled cloud service offerings must comply with the additional guidelines / standards (applicable for the Empaneled Cloud Service Offerings) as and when such guidelines / standards are published by MeitY at no additional cost to retain the empanelment status.

21. Bidder shall provide a self-service/orchestration platform so that RailTel Customer Data Centre team can provision ITresources like virtual machines, storage volume, archival data as they require.

********* End of document **********