RailTel Corporation of India Limited

Cyber Security Policy for User

Ver. No. – 1.1

Document Statistics

Type of Information	Document Data
Document Title	**Cyber Security Policy for User**
Document Code	RailTel/POL/Cyb-Sec-User
Date of Release	02/05/2019
Document Revision No	1.1
Document Owner	DC Team
Documents Author(s)	Jatin Nagpal
Document Change Reviewer	Vikas Jain/ Anjana Choudhary
Document Classification	Internal
Document Status	Final

Document Version History

Ver. #	Ver. Date	Review Date	Description for Change	Reason for Change	Affected Section	Author	Reviewed By	Approved By
1.0	02/05/2019	-	-	New Document	--	Jatin Nagpal	Vikas Jain/ Anjana Choudhary	Haritima Jaipuriar
1.0	--	01/05/2020	Document Review – No change	--	--	Jatin Nagpal	Vikas Jain/ Anjana Choudhary	--
1.1	15/06/2021	15/06/2021	Changed document layout and Section	Document Improvement	Added User Registration Procedure, Backup Policy	Ashutosh Gupta	Vikas Jain/ Anjana Choudhary	Haritima Jaipuriar
1.1	--	15/06/2022	Document Review- No Change	--	--	Ashutosh Gupta	Vikas Jain/ Anjana Choudhary	Haritima Jaipuriar
1.1	--	15/06/2023	Document Review -No Change	--	--	Ashutosh Gupta	Vikas Jain	Haritima Jaipuriar

The policy aims at providing secure and acceptable use of Client Systems.

1. Administrative activities on the Client System

1.1. User shall use account with limited privileges on client system and shall not use administrator privileges.

1.2. For any administrative activities, whether performed by the User or designated System Administrator, *Security Policy for System Administrator* shall be adhered to.

2. Acceptable Use of Client Systems

2.1. A User shall register the Client System and obtain one-time approval from the competent authority before connecting the System to the RailTel Network.

2.2. User shall be responsible for the activities carried out on the client system, using the accounts assigned to him /her.

2.3. User's network access shall be subjected to monitoring / filtering for malicious / unauthorized activities.

2.4. Backup of important files shall be taken by the user at regular interval.

2.5. System / media containing official information shall be physically secured.

2.6. User shall not leave system unattended. The user shall lock out his / her system before leaving the system. Additionally, system idle timeout shall be configured on the client system.

2.7. Maintenance or rectification of faults in the client system shall be carried out under close supervision of the user.

2.8. User shall check that the system time is as per IST. Any variation shall be reported to the System Administrator / Network Security Administrator.

2.9. User shall not engage in any of the following activities:

2.9.1. Circumventing security measures

2.9.2. Unauthorized access to Systems / Data /Programs Harassing other users by accessing or modifying their data / resources on the system

2.9.3. Creating, accessing, executing, downloading, distributing, storing or displaying any form of anti-national, offensive, defamatory, discriminatory, malicious or pornographic material

2.9.4. Making copies of software / data for unauthorized use

2.9.5. Impersonation

2.9.6. Phishing

2.9.7. Social engineering

2.9.8. Unauthorized use of software license

2.9.9. Providing official e-mail address on Internet mail groups / bulletin boards for personal use

2.9.10. Any activity that is in violation of *Central Civil Services (Conduct) rules*

2.10. User shall report security incidents to the System Administrator / Network Security Administrator.

2.11. User shall ensure that unauthorized Peer to Peer file sharing software is not installed.

2.12. User shall ensure that the system is configured as follows:

2.12.1. User shall not share client system with anyone, by default. However, if necessary for any specific reason (such as client system used in shift-duty), following shall be ensured:

2.12.1.1. Explicit approval of competent / designated authority is taken for each client system and every user accessing it.

2.12.1.2. Every user on the shared client system has a separate account.

2.12.1.3. File / Folder access permission is limited to meet functional requirement of the user.

2.12.2. User shall not share hard disk or folders with anyone, by default. However, if necessary, only the required folders shall be shared with specific user.

2.12.3. By default, all interfaces on the client system are disabled and only those interfaces which are required are enabled.

2.13. User shall ensure that if his/her Client System is formatted due to any reason, that system shall be first disconnected / quarantined from the network. The system shall connect to the network after ensuring security compliance (such as, antivirus, patch management agents, etc.).

2.14. If *User Office* does not have centrally managed patch management solution for any reason, auto-update feature shall be enabled on the Client System so that the software updates can be downloaded from Internet. This would only be a temporary arrangement till centrally managed Patch Management solution gets operationalized.

2.15. User shall allow the installation / updation of security solutions by responding to the instructions (pop-up instructions) displayed on the screen of system by the centrally managed security solutions.

3. Internet Usage

3.1. The user shall use latest version of Internet browser.

3.2. The "save password" and auto-complete features of the browser should be disabled.

3.3. Cookies should be allowed from the trusted web sites only and any cookies from third party should be blocked.

3.4. Running of active content, such as, ActiveX, JSP, PHP etc., should be restricted to trusted sites only.

3.5. Users authorized to access Social Media shall refrain from commenting on official matters on the Social Media.

3.6. The files downloaded from the Internet or accessed from the portable storage media should be scanned for malicious contents before use.

3.7. To ensure integrity of the downloaded files, digital signatures / hash values should be verified wherever possible.

3.8. Sensitive information pertaining to the user, such as login password, credit card number, etc., should be sent through an encrypted channel only.

3.9. Before accepting an SSL certificate, the user should verify the authenticity of the certificate.

3.10. The user should log-out from web-based services, like web mail, before closing the browser session.

3.11. After completing the activity in the current web based application, the browser session should be closed.

3.12. User should not:

3.12.1. Download or distribute malicious software and tools.

3.12.2. Propagate virus or malicious software.

3.12.3. Violate any copyright or license agreement by downloading and distributing.

4. Social Media

4.1. Use of social networking sites is governed by "Framework and Guidelines for use of Social Media for Government Organizations" available at http://deity.gov.in.

4.2. User shall comply with all the applicable provisions under the IT Act 2000, while posting any data pertaining to the Government on social networking sites.

4.3. User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

4.4. User shall always use high security settings on browser while using social networking sites.

4.5. User shall not post any material that is offensive, threatening, obscene, defamatory, hateful, harassing, bullying, discriminatory, racist, and sexist, infringes copyright, or is otherwise unlawful.

4.6. User shall not make any comment or post any material that might otherwise cause damage to the organization's reputation.

5. E-mail Use

5.1. Only the E-mail account provided by the User Office shall be used for official communication.

5.2. Official E-mail account should be used for official purpose.

5.3. Official E-mail shall not be forwarded to personal E-mail account.

5.4. E-mail password shall not be shared even for official purpose.

5.5. User shall not attempt any unauthorized use of E-mail services, such as:

- 5.5.1 Distribution of messages anonymously.
- 5.5.2 Misusing other user's E-mail address.
- 5.5.3 Using a false identity.
- 5.5.4 Sending messages to harass or intimidate others.

5.6. Password used for online forms / services / registrations / subscriptions shall not be the same as the password of official E-mail account.

5.7. Users should exercise caution while handling any unsolicited mail content and/or attachment. In case of suspicious E-mail / attachments, it should be reported to the System Administrator / Security Administrator.

5.8. To avoid exploits HTML E-mail, Text E-mail should be used.

6. Securing from Virus & Malicious Code (adware, spyware, malware) by deploying security agents

6.1. User shall ensure that client system is configured with the authorized anti-virus software.

6.2. User shall ensure that anti-virus software and the virus pattern files are up-to-date.

6.3. User shall ensure that anti-virus scan is configured to run at regular intervals. In case a virus does not get cleaned, incident shall be reported to the SOC of Railtel.

6.4. User shall ensure that Host based firewall (aka Desktop firewall) is enabled. Only required logical ports (such as, 80, 443, etc.) shall be enabled on the host-based firewall.

6.5. User should ensure that Host Intrusion Prevention System (HIPS), Network Access Control (NAC) and Application control is implemented.

7. Hardware, Operating System and Application Software

7.1. User shall use only the software / hardware which are authorized by the User Office.

7.2. The User shall ensure the following:

7.3. Operating System and other software is installed using authorized source or Original Equipment Manufacturer (OEM) media with valid license.

7.4. While installing the Operating System and other software packages, only the required utilities are installed /enabled.

7.5. Latest available service packs, patches and drivers are installed.

7.6. Booting from removable media is disabled.

7.7. Auto-run on all removable drives is disabled.

7.8. User shall allow the installation of service packs and patches provided by the patch server.

8. Password Security

8.1. The following are general recommendations for creating a Strong Password:

8.1.1. A Strong Password should -

8.1.1.1. Be at least 8 characters in length

8.1.1.2. Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)

8.1.1.3. Have at least one numerical character (e.g. 0-9)

8.1.1.4. Have at least one special character (e.g. ~!@#$%^&*()_-+=)

8.1.2. 8.1.2. A Strong Password should not -

8.1.2.1.1. 8.1.2.1. Spell a word or series of words that can be found in a standard dictionary

8.1.2.1.2. 8.1.2.2. Spell a word with a number added to the beginning and the end

8.1.2.1.3. 8.1.2.3. Be based on any personal information such as user id, family name, pet, birthday, etc.

8.2. The User shall ensure the following:

8.2.1. Passwords are enabled on BIOS, System login and Screensaver levels.

8.2.2. Auto-logon feature on the client system is disabled.

8.3. User account is locked after three number of failed login attempts.

8.4. User shall not share or reveal passwords.

8.5. Passwords shall be changed at every 90 days.

8.6. If a password is suspected to have been disclosed / compromised, it shall be changed immediately and a security incident shall be reported to the RailTel SOC.

8.7. Dormant/Inactive Account will be disabled after one year.

9. Portable Storage Media

9.1. User shall use officially issued portable storage media only.

9.2. User shall return the portable storage media, if it is no longer a functional requirement or in case of damage /malfunctioning.

9.3. User shall ensure that portable storage media used is free from virus.

9.4. User shall ensure that the execution of software from portable storage media is not done.

9.5. Official portable storage media should be used for official purpose.

9.6. Official portable media should not be handed over to unauthorized person.

9.7. Official portable storage media should be kept in a secure place.

9.8. In case of loss of official portable storage media, it should be reported to the competent authority at the earliest.

10. Network Access Policy applicable for the user

10.1. User shall take prior approval from the competent authority to connect the client system to the network. User has to provide his/her MAC Address to be registered for accessing RailTel Network. In similar way if any employee leave from RailTel, user MAC address needs to be removed from the list.

10.2. HR department inform the IT Team in case of any employee joins, transfers or resigns, Access revocation or access modification is done based on the requirement.

10.3. A client system authorized to connect to one network shall not connect to any other network.

10.4. User should be aware that his / her Client system discovered to be infected by a malware / virus may be quarantined.

11. Unattended Client Systems

11.1. Console of Desktops and Laptops should be locked in case they are left unattended to prevent them from unauthorized usage, e.g. for Windows XP, use 'Ctrl+Alt+Del' keys to select 'Lock Computer' or a combination of 'Windows' key and'L'.

11.2. Password-protected screen saver should be enabled on the client systems. It should be activated if the client system is left idle for 5 minutes.

11.3. All the assets assigned to the employee must be returned to IT Team prior to leaving the company in case of either transfer or resignation.

12. Additional Security Measures for Laptops

12.1. Laptops should not be left unattended.

12.2. Physical access to the laptop should be restricted to authorized users only.

12.3. In case of loss of the laptop, it should be reported to the competent authority at the earliest.

13. Client System Log

13.1. User shall not disable/delete the audit trails / logs on the client system

14. Backup Policy

14.1. Users may be provided "own cloud" access with user credential to back-up their important data in RailTel owned cloud storage.

14.2. Access privilege in the data will be with the respective user only. Other users cannot access the data of other users of own cloud.

14.3. Users with their credentials can import/export their data from/to own cloud storage.

14.4. 14.4 Own cloud storage is located in Data Center which is protected with all physical security measures Like Guard, Access Control, CCTV, WLD, VESDA System, Fire Extinguisher etc.

14.5. 14.5 Users are advised to take backup of their important data once in a week, however users can also take backup of their important data at any time of interval.