Indian Railways
ICT
Security Policy
(2019)

Preface

Railway Board had set up a Committee vide its Order No. ERB-I/2017/23/3 dated 11.10.2017 to finalize and review the existing IT Security Policy.

Based on the suggestions and recommendations incorporated from various stakeholders, IT Security Policy has been prepared and is submitted herewith.

(Dr.R.Badri Narayan) ED(C&IS) Railway Board	(Shalabh Goel) EDEE(M) Railway Board	(Sunil Gupta) ED(Tele.Dev.) Railway Board	(Pradeep M Sikdar) ED/Sig.(Dev.) Railway Board
(Gaurav Sharma) DME(C&IS) Railway Board	(V. Devnath) GM(I&S) CRIS	(Raman Bansal) CPE/CN CRIS	

S NO 42/2

Table of Contents

S.No 42/3

This Policy document is dynamic, and will undergo changes as per organisational and technological changes to the ICT environment of Indian Railways, as and when required.

1 Purpose :-

This document constitutes the Information Security Policy that all Indian Railways' Zones, Units, and Departments shall observe and follow.

The policy statements are developed for all levels of Employees, acting in different roles within Railways, including Management Employees, IT administrators, and general IT end users. It is the responsibility of all Employees to read through the entire document to understand and follow IT security policies accordingly. The Policy is also applicable for third party vendors implementing Indian Railways ICT infrastructure.

This document is a top-level directive statement that sets the minimum standards of a security specification for all Indian Railways' zones, units, and departments. Thus, the Baseline IT Security Policy can be treated as a set of basic rules which must be observed as mandatory. Other desirable measures to enhance the security can be enforced in addition to these rules.

Based on the Baseline IT Security Policy, individual IT Security Managers nominated by the competent authority will frame their own IT Security Policies as part of the Information Security Management System of the unit under their control.

This Information Security Policy shall only be revised by C&IS Directorate, Railway Board. Exemptions against the policy can be given only by Railway Board. Deviations of a minor nature can be granted by the concerned IT Security Manager as defined in clause 4.

2 Scope :-

The scope of this policy includes all information held by Indian Railways in electronic form as part of internal information systems covering business, operations, accounting etc. or information systems used for providing Services of Parcel, Freight and Passenger Services to Nation. It includes reports etc. generated from these information systems and held in paper form as printouts.

This Policy applies to all information systems purchased, developed and/or managed by Indian Railways or its various Units as well as the activities of any individual accessing Indian Railways' information assets whether directly employed by the Indian Railways, Units, Partner organizations or Contractors. This also includes entire gamut of Information Systems in Indian Railways like Information Technology, Operational Technology, Internet of Things, services etc.

The Security Policy is only generic in nature and organization/ Railway units specific customization of these policies will have to be done by steering committee, CISO as mentioned on clause on 4.

S.No. 42/4

3 Objective of Policy :-

- To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's/customer's data and for reducing economic losses due to cyber crime or data theft. To reduce the risk to critical Information infrastructure by applying Security controls to mitigate the effect of intrusions, attacks, natural or manmade disasters.
- To enhance and protect the Critical Information Infrastructure of Indian Railways.
- To provide uninterrupted IT dependent Critical Services to Nation by achieving Cyber Resilience.

4 Information Security Roles and Responsibility

The Policy envisages an overall security organization that will consist of the central IT Security Organization alongwith Indian Railways Computer Emergency Response Team (CERT-Rail) in Railway Board and supported by Security Team at each Unit. Each Zonal Railway, unit, or department, possessing significant information technology assets, (examples of units are Production Units, Construction organizations, RE units, etc.) should nominate one or more person to take up the roles given below.

- ***IT Security Managers***
- ***Incident Response Teams (IRT), with designated team leaders.***
- ***IT Security Monitoring and Implementation teams***

In smaller units, two persons might divide the responsibilities of these roles between them. However, one person should not assume all three roles in the interest of overall security. As far as possible, Security Implementation team should be separate from CERT. However, close coordination and information exchange has to be established between the teams.

A description of the roles and responsibilities of IT Security personnel and other managers and employees is given below. "Information owners" are the users of an information system who "own" the data within the system.

Size of IT Security Organization:

Administrative Head	1. GM/AGM Level Officer

IT Security Manager/ CISO	1 Establish and maintain an information protection program to assist all employees using IT equipment in the protection of the information they use 2. Lead in the establishment, maintenance and implementation of information security policies, standards, guidelines and procedures 3. Coordinate with CERT-Rail, NCIIPC, other units and departments on IT security issues 4. Disseminate security alerts on impending and actual threats from CERT-Rail to responsible parties within the unit 5. Ensure that information security risk assessments and audits are performed as necessary 6. Promote security awareness within the unit 7. Initiate investigations and rectification in case of breach of security 8. He should be at least JAG level officers reporting directly to the head of the unit.

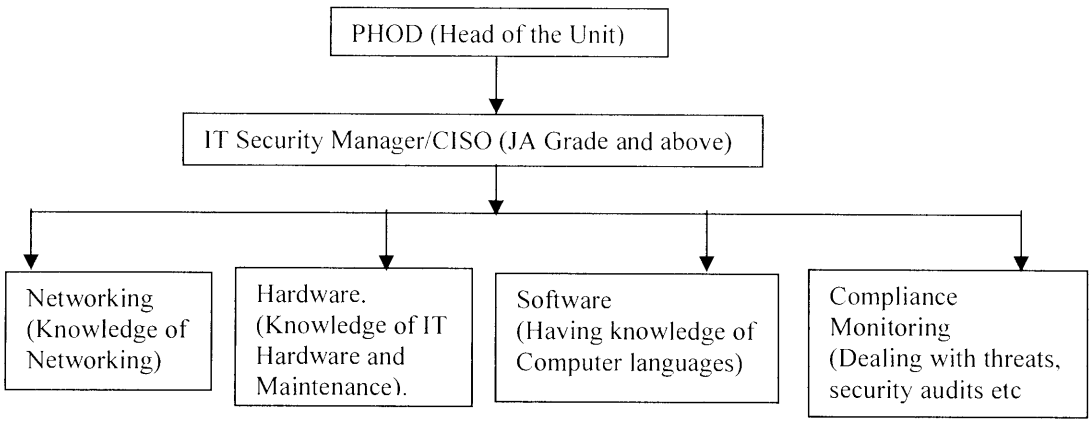
IT Security Monitoring Team	1. Maintain control and access to the system 2. Check and manage audit logs 3. Maintain user accounts
Incident Response Team (IRT) leader	1. Provide overall supervision and co-ordination of information security incident handling for all Information Systems within the unit or department 2. Make decisions on critical matters such as system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery etc. 3. Trigger the departmental disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the unit / department 4. Provide management endorsement on the provision of resources for the incident handling process 5. Provide management endorsement in respect of publicity on the incident 6. Collaborate with CERT-Rail, NCIIPC and CERT-In in the reporting of information security incidents for central recording and necessary follow up actions 7. Facilitate experience and information sharing within the unit or unit on information security incident handling and related matters

CERT-Rail (Railway Board)	1. Provide top-level information security policy to Zonal Railways / units. 2. Define criteria for deciding Critical Application and Classification of same as per NCIIPC guidelines. 3. Identification of Legal, Regulatory and Privacy Requirement for all Application/System under Indian Railways. 4. Constantly remain in contact with CERT-In and NCIIPC and other agencies to update threat perceptions and vulnerability assessments and communicate these down to IT Security Managers
CRIS IT Security Technical Group	1. Provide technical support/assistance to units in case of any Info-Sec Events in system managed by CRIS.

4.1 Following are the roles of Information Owners, System Administrator, Application Developer & Users:

Information owners	1. Determine the security requirements and data classifications, usage and protection of the information within the information systems within their control. 2. Defining of Data Retention and Archival Policy. 3. Classification of Data
System administrators /network administrators	1. Implement the security mechanisms in accordance with procedures / guidelines established by the concerned IT Security Managers.
Application Development/ Maintenance Team	1. Liaison with the information owner in order to agree on system security requirements 2. Define the solutions to implement these security requirements
Users	1. Know, understand, follow and apply all the possible and available security mechanisms to the maximum extent possible 2. Prevent unauthorized access to their computers and workstations

Organization Chart:- Following is an illustration of IT Organization for a unit.



4.2 Protected System:-

"**Protected System**" means any computer system or computer network of any railway organization as notified under section 70 of the Act, in the official gazette by appropriate Government

Section 70 of the Act states declaring any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure to be a protected system. "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety

4.2.1 Information Security Practices and Procedures for "Protected System".

(a) The organisation having "Protected System" shall constitute an Information Security Steering

Committee under the chairmanship of Chief Executive Officer or Head of /Managing Director/Secretary of
the organisation.

(b) The composition of Information Security Steering Committee(ISSC)

shall be as under:-

(i) IT Head or equivalent;

(ii) Chief Information Security Officer (CISO);

(iii) Financial Advisor or equivalent;

(iv) Representative of National Critical Information Infrastructure Protection Centre (NCIIPC);

(v) Senior Officers from CRIS as expert (s) to be nominated.

(1) The Information Security Steering Committee (ISSC) shall be the apex body with roles and responsibilities as follows: -

(a) All the Information Security Policies of the "Protected System "shall be approved by

Information Security Steering Committee.

(b) Significant changes in network configuration impacting "Protected System" shall be approved by the Information Security Steering Committee.

(c) Each significant change in application(s) of the "Protected System" shall be approved by Information Security Steering Committee.

(d) A mechanism shall be established for timely communication of cyber incident(s) related to "Protected System" to Information Security Steering Committee.

(e) A mechanism shall be established to share the results of all information security audits and compliance of "Protected System" to Information Security Steering Committee.

(f) Assessment for validation of "Protected System" after every two years.

4.2.2 **The organisation having "Protected System" shall**

(a) Nominate an officer as Chief Information Security Officer (CISO) with roles and responsibilities as per latest "Guidelines for Protection of Critical Information Infrastructure" and "Roles and Responsibilities of Chief Information Security Officers (CISOs) of Critical Sectors in India" released by NCIIPC;

(b) Plan, establish, implement, operate, monitor, review, maintain and continually improve Information Security Management System (ISMS) of the "Protected System" as per latest "Guidelines for Protection of Critical Information Infrastructure" released by the National Critical Information Infrastructure Protection Centre or an industry accepted standard duly approved by the said National Critical Information Infrastructure Protection Centre;

(c) Ensure that the network architecture of "Protected System" shall be documented. Further, the organisation shall ensure that the "Protected System" is stable, resilient and scalable as per latest National Critical Information Infrastructure Protection Centre "Guidelines for Protection of Critical Information Infrastructure". Any changes to network architecture shall be documented;

(d) Plan, develop, maintain the documentation of authorized personnel having access to "Protected System" and the same shall be reviewed at least once a year, or whenever required, or according to the Information Security Management System(ISMS) as suggested in clause(b);

(e) Plan, develop, maintain and review the documents of inventory of hardware and software related to "Protected System";

(f) Ensure that Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of "Protected System" shall be carried out at least once a year. Further, Vulnerability/Threat/Risk (V/T/R) Analysis shall be initiated whenever there is significant change or upgrade in the system, under intimation to Information Security Steering Committee;

(g) Plan, establish, implement, operate, monitor, review, and continually improve Cyber Crisis Management Plan (CCMP) in close coordination with National Critical Information Infrastructure Protection Centre;

(h) Ensure conduct of internal and external Information Security audits periodically according to Information Security Management System(ISMS) as suggested in clause (b). The Standard Operating Procedure (SOP) released by National Critical Information Infrastructure Protection Centre (NCIIPC) for

"Auditing of CIIs/Protected Systems by Private/Government Organisation" shall be strictly followed;

(i) Plan, develop, maintain and review documented process for IT Security Service Level Agreements (SLAs). The same shall be strictly followed while designing the Service Level Agreements with service providers;

(j) Establish a Cyber Security Operation Center (C-SOC) using tools and technologies to implement preventive, detective and corrective controls to secure against advanced and emerging cyber threats. In addition, Cyber Security Operation Center is to be utilised for identifying unauthorized access to "Protected System", and unusual and malicious activities on the "Protected System", by analyzing the logs on regular basis. The records of unauthorised access, unusual and malicious activity, if any, shall be documented;

(k) Establish a Network Operation Center (NOC) using tools and techniques to manage control and monitor the network(s) of "Protected System" for ensuring continuous network availability and performance;

(l) Plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting "Protected System" and the logs shall be handled as per the Information Security Management System(ISMS) as suggested in clause (b).

4.2.3 **Roles and Responsibilities of "Protected System(s)" towards National Critical Information Infrastructure Protection Centre:-**

(1) The Chief Information Security Officer (CISO) shall maintain regular contact with the National Critical Information Infrastructure Protection Centre(NCIIPC) and will be responsible for implementing the security measures suggested by the said National Critical Information Infrastructure Protection Centre(NCIIPC) using all available or appropriate ways of communication.

(2) The Chief Information Security Officer (CISO) shall share the following, whenever there is any change, or as required by the National Critical Information Infrastructure Protection Centre (NCIIPC), and incorporate the inputs/feedbacks suggested by the said National Critical Information Infrastructure Protection Centre (NCIIPC):-

	(a)	Details of Critical Information Infrastructure (CII) declared as "Protected System", including dependencies on and of the said Critical Information Infrastructure.
	(b)	Details of Information Security Steering Committee (ISSC) of "Protected System".
	(c)	Information Security Management System (ISMS) of "Protected System".
	(d)	Network Architecture of "Protected System".
	(e)	Authorised personnel having access to "Protected System".
	(f)	Inventory of Hardware and Software related to "Protected System".
	(g)	Details of Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of "Protected System".
	(h)	Cyber Crisis Management Plan(CCMP).

S.No 42/17

	(i)	Information Security Audit Reports and post Audit Compliance Reports of "Protected System".
	(j)	IT Security Service Level Agreements (SLAs) of "Protected System".
(3)	(a)	The Chief Information Security Officer (CISO) shall establish a process, in consultation with the National Critical Information Infrastructure Protection Centre (NCIIPC), for sharing of logs of "Protected System" with National Critical Information Infrastructure Protection Centre (NCIIPC) to help detect anomalies and generate threat intelligence on real time basis.
	(b)	The Chief Information Security Officer shall also establish a process of sharing documented records of Cyber Security Operation Center (related to unauthorised access, unusual and malicious activity) of "Protected System" with National Critical Information Infrastructure Protection Centre(NCIIPC) to facilitate issue of guidelines, advisories and vulnerability, audit notes etc. relating to "Protected System".
(4)	(a)	The Chief Information Security Officer (CISO) shall establish a process in consultation with National Critical Information Infrastructure Protection Centre (NCIIPC), for timely communication of cyber incident(s) on "Protected System" to the said National Critical Information Infrastructure Protection Centre (NCIIPC).
	(b)	In addition, National Critical Information Infrastructure Protection Centre's latest Standard Operating Procedure (SOP) on Incident Response shall be strictly followed in case of cyber incident(s) on "Protected System".

5 ICT Assets Management:-

The Policy under this section will help Indian Railways to identify data, personnel, devices, systems, and facilities that enables IR to achieve its purposes. Policy shall ensure that identified ICT Assets are managed in consistent way according to their relative importance to IR's objectives and risk strategy.

- Every Units/Zonal Railways shall maintain, updated inventory of all the Physical Assets and Systems associated with Information and Information Processing Facilities as defined in scope.
- Units shall periodically update Inventory of Software Platform and Application within the organization along with versions in use currently.
- All the assets should be classified based on its criticality and its business value. (Reference can be taken from CII-2013 Policy)
- Assets maintained in Inventory should be owned and owner can be entity or individual who has approved Management Responsibility of managing whole lifecycle of assets.
- Assets, software and hardware shall not be taken out of office premise unless it is authorized by competent person in unit. Separate policy may be issued by units.
- Asset ownership table to be issued by the respective directorates of Railway Board with clear cut roles and responsibilities as per guidelines issued by Railway Board.

6 Business Environments :-

- The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.
- Every unit will identify all the dependencies and critical functions delivering critical services as identified by Railway Board (MoR).
- Unit shall prepare Business Continuity Plan for all dependencies and critical functions used in delivery critical service.
- Unit shall communicate BCP/DR plan to all stakeholders in organization.
- Unit shall establish cyber resiliency requirement for delivering critical services.

7 Governance:-

- The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cyber security risk.
- Information Security Policy, Procedure, Standard and Guidelines shall be established in every Unit/Zonal Railways. Abstract guidelines to be provided by Railway Board and units can customize it as per their requirements.
- Railway Board (MoR) shall identify all Legal, Regulatory and Privacy requirement as per Indian Laws and same shall be communicated to the concerned unit.
- Information Security Roles and Responsibility shall be defined, documented and communicated to all concerned Stakeholders.
- MoR (Railway Board) shall define the Data Classification Level and its handling mechanism and same shall be communicated to all Units on Indian Railways. Suggested Levels for Data Classification may be Public, Sensitive Personnel Data, Internal Business Data and Confidential.
- Units shall classify their Data based upon Levels defined by IR and implement its handling Mechanism.
- Review of information security policies, standards, guidelines and procedures shall be conducted periodically. Periodicity shall not exceed a Year. Info-Security Policy may be reviewed in between either due to change in external factor like Technology, Legal / Regulatory or Privacy requirement or due to change in internal factor like risk etc.
- Units shall ensure that the provision for necessary security safeguards and resources are covered in their budgets.
- Units shall ensure that security protection is responsive and adaptive to changing environment and technology.

- Units shall include in their IT Security procedures a provision advising employees that if they contravene any provision of the procedures they would be subjected to disciplinary action under the Discipline and Appeal Rules, severity of the action taken depending on the severity of the breach.

- Units shall also include in their IT Security procedures a provision advising all non-railway persons (e.g. third party maintenance personnel, developers, and trainers) that if they contravene any provision of the procedures, they would be penalized or their contracts would be terminated, depending on the severity of the breach.

8 Supplier, Contractor and Outsourcers Risk :-

The Policy procedure and processes required to manage outsourcing agreement are identified.

- Outsourcing or third party service providers shall observe and comply with the unit's own IT Security related procedures, apart from other IT security requirements issued by the Railway Board / concerned IT Security Manager.
- Units shall monitor and review the outsourcing or third party service providers' adherence to IT security procedures to ensure that security operations are managed properly.
- Information Security requirement of Application/Data/System/Services should be mentioned in any outsourced agreement.
- Unit should have a right to audit the Third party (ex Third Party Premises, Operation Center, Development Center, Data Center etc.) for ensuring compliance with Unit/IR Information Security Policy.
- Service Level Agreement should be defined with appropriate response time and Escalation matrix depending upon criticality of application.
- Information Security Policy shall be applicable for contractor and its subcontractor also if there is any. Compliance from both i.e. contractor and subcontractor shall be ensured.

9 Risk Assessment and Security Audit :-

This Policy will help organization to understand the cyber security risk to its operations (including mission, functions, image, or reputation), organizational assets, and individuals.

- Security risk assessments for information systems and production applications shall be performed at least once every two years. A security risk assessment shall also be performed prior to major enhancements and changes associated with these systems or applications. All contracts, outsourcing proposals to include this provision.
- Use of software and programs for security risk assessment analysis shall be restricted and controlled.
- Unit shall ensure Periodic VAPT of Critical Information Systems by CERT-In Empanelled Auditors and Periodicity shall not exceed a year.

- Engagement with Non Indian firm for Security Audit should be done once NOC is obtained from MHA.
- Every auditing firm and its auditors engaged should be required to sign NDA before being allowed to commence the Cyber Security Auditing.
- Any data collected during the audit work and report prepared therefore is not allowed to be taken out of the organization.
- Auditing of compliance of computer and network security policies shall be performed periodically and after any major change of assets.
- Risk acceptance criteria shall be documented and same shall be approved by asset owner.
- Unit shall ensure that Threat and Vulnerability information related to assets is received by them from various credible sources like CERT-In, NCIIPC, OEMs of Software Application etc.
- Unit shall document all identified threat, vulnerability and its impact on its asset.
- All residual risk shall be communicated and accepted by respective asset owner.

10 Physical Security Control for Data Centre :-

The objective of this Policy is to ensure the physical security of Data Center and Assets hosted in it.

- A list of persons who are authorized to gain access to data centers, computer rooms or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and be reviewed periodically.
- All visitors to data centers or computer rooms shall be monitored at all times by an authorized member of Railway Employees.
- Unit shall ensure that Information System component of CII is prevented from Power, cooling and other failure caused by failure in Supporting utilities etc.
- Unit shall have Smart Card /Biometric or other Access Control mechanism in place to prevent unauthorized access of Data Center.
- Careful site selection and accommodation planning of a purpose-built computer installation shall be conducted. All data centers / computer rooms shall be provided with appropriately conditioned environment and power.
- Data centers and computer rooms shall have good physical security and strong protection from disaster and security threats, whether natural or caused by other reasons, in order to minimize the extent of loss and disruption. Fire protection systems suitable for use in a computer centre shall be used in all areas where critical IT assets are located.
- Data centers and computer rooms shall be restricted areas and only authorized persons will be allowed into the premises. Suitable access control systems should be put in place to restrict entry into the premises. All entries into the premises must be logged.

S.No 42/9

- Physical access of employee post retirement/completion of engagement/termination/transfer needs to be revoked with proper change management process and audited periodically.

11 Access Control :-

The Policy under this section will ensure that access to assets and associated facilities is limited to authorized users, processes, or devices and to authorized activities and transactions.

- Access to information shall not be allowed unless authorized by the relevant information owners.
- Data access rights shall be granted to users based on a need-to-know basis.
- Data access rights shall be clearly defined and reviewed periodically. Periodicity shall not exceed a Year by Information Owners.
- Access to any Information System containing confidential information shall be strictly controlled.
- All access keys, cards, passwords, etc. for entry to any of the computer systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures.
- Automatic protection features (e.g. password protected screen saver, keyboard lock) in Significant IT Assets (servers, computer terminals and workstations) should be activated if there has been no activity for a predefined period of time to prevent illegal system access attempt. Alternatively, the logon session and connection should be terminated. Also, user workstation should be switched off, if appropriate, before leaving work for the day or before a prolonged period of inactivity.
- All Employees with separate personal offices that can be directly accessed from public areas and that contain Information Systems should lock or otherwise secure the doors, or ensure that they are kept under watch, when these offices are not in use.
- The display screen of an Information System on which classified information can be viewed shall be carefully positioned so that unauthorized persons cannot readily view it.
- Units shall apply sufficient segregation of duties to avoid execution of all security functions of any Significant IT Asset by a single individual.
- Units shall enforce the principle of least privilege when assigning resources and privileges of Information Systems to users.

12 Password Policy :-

The policy under this section will ensure necessities of having strong password to prevent attack.

- Unit shall define a strict password policy that details at least, minimum password length, initial assignment, restricted words and format, password life cycle, and include guidelines on suitable system and user password selection.

- Passwords shall not be shared or divulged unless necessary (e.g. helpdesk assistance, shared PC and shared files). Any shared passwords should be changed promptly when the need no longer exists and should be changed frequently if sharing is required on a regular basis.

- Passwords shall always be well protected when held in storage. Passwords shall be encrypted when transmitted over an un-trusted communication network. Compensating controls shall be applied to reduce the risk exposure of Information Systems to an acceptable level if encryption is not implementable.
- Employees shall not capture or otherwise obINcretain, in an unauthorized manner, passwords, decryption keys, or any other access control mechanism, which could permit unauthorized access.
- All vendor-supplied default passwords shall be changed before any Information System is put into operation.
- All passwords shall be promptly changed if they are suspected of being compromised, or disclosed to vendors for maintenance and support.
- Password of all network components/ applications needs to be changed periodically, depending on the criticality of the system or application. Email password protection mechanism is also required to be mentioned in this section.
- The above policy customization shall be carried out by IT Security Manager (clause 4).

13 Protection against Computer Virus and Malicious Code :-

The Policy Process and Procedure require to manage the Antivirus/Antimalware are identified and implemented in units.

- Anti-virus software shall always be enabled and regularly updated on all local area network servers and personal computers, and computers connecting to the internal network via remote access channels.
- Units shall protect their Information Systems from computer viruses and malicious codes. Virus signatures, malicious code definitions as well as their detection and repair engines shall be updated regularly and whenever necessary.
- Storage media and files from unknown source or origin shall not be used unless the storage media and files have been checked and cleaned for computer viruses and malicious codes.
- Users shall not intentionally write, generate, copy, propagate, execute or involve in introducing computer viruses or malicious codes.
- Units shall implement proper measures to protect their wireless or mobile computing devices against computer viruses and malicious codes.
- It is the IT Security Manager's responsibility to ensure that appropriate anti-virus / desktop firewall software is procured and installed in all IT equipment under his purview. Users shall ensure that in no case are desktop PCs / laptops unprotected by licensed anti-virus software / desktop firewall software. Users shall also ensure that such software is updated regularly.

S.No:42/10

- Zonal HQ units to issue necessary guidelines directing IT Security Managers to procure antivirus from reputated vendors.

14 Awareness and Training:-

The organization's personnel and partners are provided cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with IR's policies, procedures, and agreements.

- Unit shall ensure that any new joinee gets Info-Sec Awareness Session as part of Induction Training Program.
- All training institutes like ZRTI/RTI/CTIs should include a module of Information Security Awareness Sessions
- Employee shall sign acknowledgement of being aware of Info-Sec Policy and his/her roles and responsibility.
- Unit shall ensure that employees working in Information Security Domain are either certified in Info-Sec domain or having relevant IT Experience.
- Unit shall identify skill development needs to protect Critical Information Infrastructure and ensure implementation of required Security Control.
- Unit shall conduct periodic Information Security Awareness Program for its employees.
- Information security is the responsibility of every member of the Railway Employees. As such, units shall educate users about the IT Security procedures and strengthen their security awareness.
- Units shall ensure that all employees / members have been advised of their IT security responsibilities upon being assigned a new post, and periodically throughout their tenure on that post.
- Employees handling classified systems or systems containing classified information shall sign Non-Disclosure Agreement.
- Employees working in Information Security should be sent for training to various IT firms/government organizations that are leaders in Information Security.

15 Data Security :-

Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- Information about Information Systems that would compromise the security of those systems should not be disclosed to users, or any other third parties, except on a need-to-know basis.
- Employees shall not disclose information about specific systems that have suffered from damage caused by computer crimes and computer abuses, or the specific methods used to exploit certain system vulnerabilities, to any people other than those who are handling the incident and responsible for the security of such systems, or authorized investigators involving in the investigation of the crime or abuse.

- Data shall be kept secure during storage, transmission, processing, and destruction.
- Employees shall ensure that Data Handling mechanism is followed as defined by MoR (Railway Board).
- Development, Testing and Production Environment shall be physically/logically segregated.
- Unit shall ensure that Data storage location adheres to Indian laws applicable from time to time and shall not be located outside India Unit shall use appropriate encryption algorithm for the protection of confidential/sensitive data in Rest (the storage devices) or in transit as per Indian Laws applicable from time to time. For this, appropriate key management mechanisms shall also be in place.

16 Software and Patch Management Process :-

Application and system software are updated with latest version, security patches and are consistent with organisation risk strategy.

- Computers and networks shall only run software that comes from trustworthy sources.
- The IT Security Manager shall decide the types of application programs that can be run on any computer network.
- Unit / departments shall protect their Information Systems from known vulnerabilities by applying the latest security patches recommended by the product vendors or implementing other compensating security measures.
- Before security patches are applied, proper risk evaluation and testing should be conducted to minimize the undesirable effects to the Information Systems.
- Security patches shall be applied on Testing Environment before applying it on Production Environment.

17 Email Security :-

Each unit / units shall clearly define and communicate to users its policy in relation to acceptable email usage.

- Systems administrators shall establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages and accompanying logs.
- Incoming / outgoing email shall be screened for computer viruses and malicious codes.
- Internal email address lists containing entries for authorized users shall be properly maintained and protected from unauthorized access and modification.
- Email transmission of confidential information shall be allowed only on an Information System approved by the Information Security Manager
- Emails from suspicious sources should not be opened or forwarded.
- GOI email policy should be used for all official correspondence.

- Suitable Email password protection mechanism should be in place for the users.

18 Acceptable Use of ICT Assets :-

Acceptable use of Assets shall prevent misuse of Organisation Assets and reduce the copyright / trademark violation.

❖ ***ICT Equipment :-***

- IT equipment owned by Indian Railways shall not be moved out of Railway premises, unless specifically issued for the purpose, such as laptop computers, PCs and other equipment placed in the residence of nominated officers and employees for official use or data transfer devices.
- Official data or information may on occasion be transferred via email / data transfer devices / other means to personal equipment for the purpose of speed and efficiency of working. However, in no case should secret or confidential data / information be allowed to reside in any public / personal data processing equipment.

❖ ***Internet and email use :-***

- Internet use should be encouraged as a means of obtaining information, as well as establishing quick and inexpensive contact with the public.
- Email use should be similarly encouraged to speed up intra-organizational as well as extra-organizational communication.
- However, regular use of internet services provided in the office for non-official use, browsing of inappropriate content, use of lottery or trading sites, or the use of internet chat services for personal use should not be made. It is the responsibility of each individual user to ensure that he or she makes only appropriate use of Internet and email facilities.
- The IT Security Manager must ensure that all practical measures are taken to provide appropriate perimeter filters to eliminate the possibility of inappropriate content being viewed over an official network.
- All software and files downloaded from Internet shall be scanned with up-dated antivirus software. Anti-phishing software shall also be used to detect and block phishing attacks.
- Users shall not execute mobile code or software downloaded from the Internet unless the code is from a known and trusted source.

❖ **Licensed software**

- Only licensed and legally valid software should be loaded onto Indian Railways' computer systems.
- The IT Security Manager must set up procedures to ensure that unlicensed software is not available on the equipment under his purview. However, it continues to remain the responsibility of the individual users not to use unlicensed / illegal software.

19 Data Leak Prevention Policy :-

- Unit shall develop data loss / leakage prevention strategy to safeguard secret / confidential information.
- Protection of data shall be ensured in both transit or in rest whether it is in online system or in offline.
- Unit shall ensure similar security control / arrangement at vendor premise / site in case of outsourcing.

20 Information Disposal and Transfer Policy :-

The Policy procedure for information disposal and transfer shall be identified to prevent leakage of confidential data.

- Media containing confidential / sensitive information shall be securely disposed off.
- Unit shall define retention policy for Data (Wherever Guidance from MoR is not available) they are handling.
- Unit shall securely disposed/wiped/shred the data once retention period is over.
- Unit shall sign Non-Disclosure Agreement with third party before transfer of any information.
- Unit shall define Secure Disposal Process for disposing of media containing data.

21 Secure Development and Application Security :-

- Unit shall ensure that developed applications are free from OWASP top 10 vulnerability.
- System development, testing, and production shall be performed in separate environment.
- Unit shall document the Information Security requirement for all information system under their purview.
- Unit shall monitor the resource utilization (CPU, Memory, Disk etc.) of IT system periodically. Projections shall be made of future capacity requirements to ensure adequate performance.
- The development of software by third parties shall be done under the supervision of respective unit.
- The development of software by third parties shall be governed by a contract or a Service Level Agreement (SLA) that includes security requirements.
- CERT-In empanelled auditor shall audit the application/system in use currently.

S.N. 42/12

- Access to program source code and associated items (e.g. designs, specifications, verification plans, validation plans etc.) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

- Unit shall follow Change Management Process and Procedure for all changes in production or in development application/system.
- Production data shall not be used in testing/development environment to prevent leakage of SPD or confidential information.
- Applications based locks should be available for finding & analyzing threat analysis.
- Unit shall remove non-production or default application accounts, user IDs, and passwords before applications become active or are released to customers.

22 Database Security :-

- User Access right should be reviewed periodically and dormant / unnecessary account should be disabled. Periodicity shall not exceed a year.
- Privileges to database users should be given as per their role, keeping in mind the principle of least privilege.
- Unit shall remove default user accounts, schema and change the default password.
- Unit shall ensure database service is running under Least Privilege Account (non root user).
- Auditing should be configured at user and object level for at-least admin/sys users and tables containing critical information.
- DBMS must be in archive mode (RPO-Zero), for proper recovery.
- Authorization of clients should be done by their IP address and User ID to database server.

23 System Security :-

- User Access right should be reviewed periodically and dormant/unnecessary account should be disabled. Periodicity shall not exceed a year.
- Privileges to OS users should be given as per their role, keeping in mind the principle of least privilege.
- Unit shall remove default user accounts and change the default password.
- Unit shall disable unnecessary Services/Ports.
- All administrator or root access must be logged.
- Audit logs of all systems needs to be enabled.
- Time synchronization among all ICT assets must be ensured.

24 Network and Communication Security:-

- Internal network addresses, configurations and related system or network information shall not be publicly released without the approval of the concerned Information Security Manager.
- All internal networks with connections to other networks or publicly accessible computer networks shall be protected at the network gateways.
- Perimeter security mechanisms should be laid down in the policy clearly specifying both proactive and reactive monitoring mechanisms. Wherever critical IT applications are web enabled, these should include an appropriate combination of :
    - Screening of the traffic by using appropriate packet filters at the boundary / gateway router level.
    - IP address spoofing filters should be configured on the gateway routers.
    - Zoning of the private network, demilitarized zone (DMZ) and the public untrusted network by implementing an appropriate firewall solution.
    - Implementation of an appropriate intrusion detection/prevention system.
    - Appropriate processes should be in place to monitor and react to Events& Alarms/Logs generated by the above devices on the internet gateway.
    - Gateway level antivirus / anti-spyware system with associated monitoring / corrective processes.
    - The packet filtering / traffic treatment policies on the Internet Gateway should be clearly defined, documented and periodically reviewed.
- Security measures shall be in place to prevent unauthorized remote access to the systems and data.
- Employees are prohibited from connecting workstations to external network by means of communication device, such as dial-up modem, wireless interface, or broadband link, if the workstations are simultaneously connected to a local area network (LAN) or another internal communication network, unless with the approval of the concerned Information Security Manager.
- Employees shall not connect any unauthorized Information System device (such as a pen drive, external disk, floppy disk etc.) to an official Information System with the intent to copy confidential information. Employees shall ensure that in no case can malicious code be injected into the network by the use of such device. The concerned Information Security Manager shall disallow connection of such devices to networks he considers sensitive.
- Proper configuration and administration of information / communication systems is required and shall be reviewed regularly.
- Connections and links made to other network shall not compromise the security of information processed in either network.

S.No 42/13

- Connecting privately owned computer resources to Railways' internal network requires approval from the concerned IT Security Manager.
- Confidential information shall be encrypted when transmitted over an un-trusted communication network.
- Secret information shall be transmitted and stored only under encryption.
- For critical networks, routing update sources shall be authenticated by using an appropriate mechanism.
- IP broadcast packets shall be disallowed unless required by a specific application.

Policy framework for Network Wireless Security:

Wireless Network Security Policy framework is to address all the usage options of wireless networks and the types of information that can be transmitted. It starts with Design phase and continues till Disposition phase. Few of the key elements of each phase are as under:

- DESIGN / PROCUREMENT PHASE :
  - To keep Track of Development for Wi-Fi Standards.
  - Perform Security Risk Assessments and Audits to Identify Security Vulnerabilities.
  - Security assessments and audits for checking the security status of a wireless network and identifying any corrective action necessary to maintain an acceptable level of security.
- IMPLEMENTATION PHASE:
  - To Implement Strong Physical Security Controls to avoid the loss or theft of network equipment.
  - Avoid Excessive Coverage of Wireless Networks
  - Secure Access Points Access points are the core of a wireless network and regime to change regularly-
    - Default configuration settings;
    - Encryption keys ;
    - All access points to have strong, unique administrative passwords and change the passwords
    - Disable all insecure and unused management protocols on access points.
    - Activate logging features and direct all log entries to a remote logging server;
    - Enable wireless threshold parameters, such as inactivity timeouts and maximum supported associations.
- OPERATIONS AND MAINTENANCE PHASE :
  - To Educate Users about the Risks of Wireless Technology User awareness is always a critical success factor in effective information security.
  - To Keep an Accurate Inventory of All Wireless Devices
  - To Develop Security Configuration Standards for Access Point To simplify daily operations and ensure all access points are protected with appropriate measures
  - Administrators to develop a set of in-house procedures for incident response and update these procedures from time to time to address new potential security threats.

- DISPOSITION PHASE:

    - To Remove All Sensitive Configuration Information before Disposal During disposal of wireless components.
    - To erase all sensitive configuration information, such as pre-shared keys and passwords, on the devices that are being disposed of.

25 SCADA "Operation Technology" for Security Policy :-

ICT enabled information and management systems of SCADA are subjected to many common information security risks and threats like-

(a) Hardware failure/ malfunction of systems, fire, flooding;
(b) Software failure/ malfunction of systems,
(c) Power failure/ malfunction feeding to these systems;
(d) Human resources threats: ignorance, mal-intent, sabotage, convenience;
(e) Malware: sophisticated programs targeted on SCADA systems

To mitigate above risks, following strategies are suggested-

A. Protection from Hardware failures, Fires, Floods, etc.

- Use of only OEM equipments and spares,
- Availability of comprehensive AMC with 100% spares availability,
- Installation & Functionality Fire Protection System in TPC,
- Flood prevention by raised equipment/ Floor/ Building, Drainage etc.

B. Protection from Software failures

- Use of only licensed system software like the OS
- Keeping these system software's always updated with patches from OEMs, with a comprehensive ATS with them if necessary
- Non-loading/removing any non required software from official systems, including the free/trial softwares from OEMs.
- Only one licensed Antivirus/Anti- malware software loaded and kept updated.
- Prohibiting any external media like the CDs/DVDs, USB drives etc. connecting and loading software. Disabling of all external ports in SCADA server except one CD/DVD drive for loading/unloading of software/Data. These may be disabled in the BIOS and locked with password.
- Keeping regular back-up of critical data & full zero-level backup of Operating System, whenever there is major update.

C. Protection from Power failures

- Reliable and adequate capacity UPS, provided with in-built protection for power quality.
- Redundancy in input power such as DG-set, and also in the UPS system to avoid single point of failure.
- Adequate curtailing of system and also UPS, for functioning during summer season. High cost PAC is not required due to low concentration of heat.
- Full chain of UPS and DG-Set power backups be tested every month.

D. Protection from Internal & Human failures

- Restricted/Authorized entry into the SCADA systems areas;

S.No 42/14

- Separate server room for SCADA servers other than the TPC room where MMIs are kept. Entries to the SCADA server room are to be biometric/password lock protected to prevent entry of unauthorized person into SCADA server room.
- Server & Router kept under physical lock and key without authorized entry;
- Video surveillance of TPC, Server area, connected to main Video systems for security.
- DAR procedure for violation of these Codes.

E. Protection from Malware (Sophisticated Programs)

- Strict policy of not disturbing SCADA systems with unauthorised connection,
- Disconnect Internet, both through Rail-net or Broad-band.
- Keep a PC with Internet separate from those of SCADA systems in the TPC, for any Railnet/Internet work like e-mail & browsing. The same PC can also be used for DVD & USB Drive data loading.

Implement Anti-Malware in the SCADA systems, which can control software risks mentioned above. Such software may be available from the SCADA OEMs.

26 Internet Usage Policy :-

- All Internet access shall be through designated suitably hardened Internet gateways. In circumstances where this is not feasible, units should consider allowing Internet access through stand-alone machines, provided that there is an approval and control mechanism at appropriate level.
- Units should consider the value versus inconvenience of implementing technologies to block non-business web sites. The ability to connect with a specific web site does not in itself imply that users of systems are permitted to visit that site.
- Each unit / units shall clearly define and communicate to users its policy in relation to acceptable Internet usage.
- All software and files downloaded from the Internet shall be screened and verified with anti-virus software.
- Employees should not execute mobile code or software downloaded from the Internet unless the code is from a known and trusted source.

27 Information Protection Processes and Procedure :-

Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.

- Unit shall define and document Change Management Process and Procedure to be used in unit for any changes in application, system and network.
- Unit shall document backup and restoration procedure.
- Unit shall also define document and Implement Other Process, Procedure as mentioned in Security Policy.

28 Maintenance :-

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

- Unit shall ensure that AMC / ATS of Information System components is maintained.

29 Cloud Security :-

- Unit shall ensure that Cloud Service Provider is using strong encryption algorithms for data at rest as well as in motion.
- Data backup shall be ensured by unit itself in cloud or otherwise.
- Critical Information Infrastructure as declared by MoR (Railway Board) shall be Physically/Logically separate from other application (from Different Organization) hosted by same Cloud Service Provider.
- Unit shall ensure that Data/System is accessible only to authorized person only.
- Access to information, network services, operation system, application and system shall be controlled and authorized by its Asset Owner only.
- Unit shall cover Security related issues/aspects under Service Level Agreements (SLA).
- Cloud Service Provider shall ensure compliance with latest MEITY and GOI Laws and Policies e.g. IT Act 2008 etc.

30 Security Continuous Monitoring :-

- Unit shall establish Cyber Security Operation Center for Critical Information Infrastructure serving Critical Applications in Indian Railways.
- Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time.
- Unit shall monitor the Network, Application, and System for any anomalies or cyber attack.
- Unit shall monitor Physical Environment of Data Centre and ensure appropriate environment as specified by OEMs.
- Unit shall establish and manage a baseline for Network/Application/System traffic and its operations so that deviations from same can be detected.
- Unit shall document the Procedure for monitoring, detecting, Analyzing and reporting of Security Events.
- Unit shall clearly document Roles and Responsibility for detection and Analysis of Security Events.

S No 42/15

31 Logging :-

- Units shall define policies relating to the logging of activities of Information Systems under their control according to the business needs and data classification.
- Any log kept shall provide sufficient information to support comprehensive audits of the effectiveness of, and compliance of, security measures. At the same time, event logging should be so configured that only significant or unusual events are logged so that these can be detected easily for quick corrective measures.
- Logs shall be available for at least last 3 Months. During this period, such logs shall be secured such that they cannot be modified, and can only be read by authorized persons.
- Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity supported by the IT Security Manager.
- Regular checking of log records, especially on system/applications where confidential information is processed / stored, shall be performed, not only on the completeness but also the integrity of the log records. All system and application errors which are suspected to be triggered as a result of security breaches shall be reported and logged.
- Clock synchronization should be configured to keep clocks of critical Information Systems synchronized.
- Unit shall review the logs periodically for any unusual/Malicious activity. Periodicity shall not exceed a week.

32 Incident Response Process and Procedure:-

- The designated Incident Response Teams shall establish incident detection and monitoring mechanism to detect, contain, and ultimately prevent security incidents.
- Incident Response Teams shall ensure that system logs and other supporting information are retained for the proof and tracing of security incidents.
- Incident Response Teams shall establish, document and maintain a security incident handling / reporting procedure for the Information Systems in their ambit.
- Employees shall be made aware of the security incident handling / reporting procedure that is in place. Employees shall observe and follow it accordingly.
- Unit shall identify Single Point of Contact for reporting of network or systems software malfunctions, information security alerts, warnings, suspected vulnerabilities, and suspected network security problems in existing Application/System/Network or physical Controls.
- All, shall be reported immediately only to the responsible party according to the incident handling procedure.
- Immediate follow-up actions are required on suspected system intrusion according to security incident handling / reporting procedures.
- The Security Incident Response processes should integrate with the general problem management process of each application.

- Unit shall have Incident Response Plan with clear Roles and responsibilities and clearly demarcated Escalation Matrix.
- Unit shall keep common Inventory of Knowledge gained from analyzing and resolving of Information Security Incident. Common Inventory shall be available to all stakeholders in Organization.

33 Cyber Crisis Management Plan:-

Unit shall report Major Security Incident as defined by the IT Security Manager (clause 4) of the unit, to Railway Board on real time basis. Root cause analysis along with corrective actions of the same should be sent within 15 working days. Reporting to NCIIPC, CERT-In et al shall be dealt by Railway Board Cyber Crisis Management Plan :-

- Unit Shall prepare and implement its Cyber Crisis Management Plan to mitigate Cyber Risk.
- Unit shall ensure that Cyber Crisis Management Plan is aligned with BCP/DR of Application/System or Services provided by respective Unit.
- Cyber crisis Management Plan shall cover four Components i.e. Detect, Respond, Recover and Containment of Cyber Risk.

34 Backup:-

- Backup and recovery procedures shall be well documented, properly implemented, and tested periodically. Periodicity shall not exceed once in every six months.
- Backup and Restoration Procedure document shall be available on Primary Site, DR Site as well as on Cloud.
- Backups shall be carried out at regular intervals. Periodicity shall not exceed once in year
- Backup activities shall be reviewed regularly.
- Integrated copies of backups shall be stored at a remote distance from the system and be protected. Backup media should also be protected against unauthorized access, misuse or corruption during transportation.
- Unit shall ensure Backup of Application (Source Code),Configuration files and Database at remote site.
- Backup media containing business essential and / or mission critical information shall be sited at a safe distance from the main site in order to avoid damage arising from a disaster at the main site.
- Physical Access Control must be in place to protect the Backup Data from unauthorized Access.
- Transmission of backup media from onsite to offsite location should be done by authorized Person/Employee of IR/Unit.
- This Policy is applicable to other IT based systems like SCADA, RRJ, SSI, E-I etc.

S.No 62/16

35 Business Continuity Planning and Disaster Recovery :-

- Business Continuity should be planned for all critical applications and all significant IT assets. The Business Continuity procedures should be clearly understood by all concerned employees and officers.
- The conditions under which Business Continuity provisions shall be invoked should be clearly written down and understood by all concerned employees and officers.
- Business Continuity procedures should be drawn up in such a way that the costs of setting up and operating the BCP system do not exceed the likely benefits of having such a system. A practical approach should be taken for smaller and less critical systems.
- For critical systems, the scope of each incident apprehended (that is, system-level, building-level, region-level) should be set off against the probability of occurrence of such an incident. The expected downtime for each apprehended incident, and the cost of such downtime, should be estimated, in order to arrive at the expected cost of a likely disaster scenario. The expected cost of the disaster scenario should exceed the cost of mitigating the disaster through the Business Continuity Plan by a factor of at least three
- Unit shall identify two important parameter i.e. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for every critical application managed by them.
- Unit shall also identify appropriate Disaster Recovery Strategy for achieving the desired RTO and RPO.
- Periodic DR Mock Drill shall be conducted for testing the effectiveness of DR Strategy. Periodicity shall not exceed a year.
- Lessons learned from DR Mock Drill shall be documented and shall be updated in DR Manual.
- A Updated copy of DR/BCP/System Manual shall be kept both at Primary and DR Site for ease of access and security purpose.

36 Encryption :-

- All above references to encryption of data & communication shall be compliant with extant national guidelines issued by MEITY.

37 Penalty and D&R :-

- Violation and penalties related to ICT incidents shall be defined and issued through Establishment Directorate of Railway Board.

References :-

Following documents have been used as reference, in establishing the Information Security Policy for Indian Railways -

1) ISO 27001:2013 - Information Security Management System.
2) National Cyber Security Policy - India, 2013
3) NCIIPC guidelines for Critical Information Infrastructure, version 2.0.
4) Report of Rly Board Committee on CII in Rlys, Feb' 2013.
5) NIST Cyber-Security Framework, latest version on website.

This Policy document is dynamic, and will undergo changes as per organisational and technological changes to the ICT environment of Indian Railways, as and when required.