



Government of India,
Ministry of Railways
Research Designs &
Standards Organisation
Manak Nagar, Lucknow -
226011

Telephone: 2465763,
42805(Off.)
Fax: 91-0522-
2465763
E-mail:
psi.ti@rdso.railnet.gov.in



No. RDSO-TI0LKO(PSI)/11/2021-O/o PED/TI/RDSO

Dated: As signed

To,

As per the mailing list attached

Sub: Uploading of Instruction No. TI/IN/0052 regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways for SCADA System.

It is informed that the Technical Instruction No. TI/IN/0052 regarding Standard Operating Procedure (SOP) for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to Supervisory Control and Data Acquisition System for 25kV and 2x25kV Single phase 50 Hz AC Traction Power Supply has been uploaded on RDSO public Website and Rail Saver for downloading and necessary action please.

This is issued with the approval of the Competent Authority.

Digitally Signed by
Jitendra Kumar
Date: 11-02-2025 20:03:51
Reason: Approved

(Jitendra Kumar)
Director / TI-III
For Director General (TI)

Copy to:

ED/EEM, Rly. Board: For kind information, please.

Mailing List

| SN | Railways/ PSUs | E-mail id |
|-----|---|--|
| 1. | Principal Chief Electrical Engineer, Central Railway., 2 nd floor, Electrical Branch, Parcel Office Bldg. Mumbai - 400 001. | cee@cr.railnet.gov.in |
| 2. | Principal Chief Electrical Engineer, Eastern Railway, Fairlie Place, Kolkata-700 001 | cee@er.railnet.gov.in |
| 3. | East Central Railway, Hajipur (Bihar).844101 | cee@ecr.railnet.gov.in |
| 4. | Principal Chief Electrical Engineer, East Coast Railway, B-Rental Colony, Chandrashekharapur, Bhubaneswar (Orissa)-751 023 | cee@ecor.railnet.gov.in |
| 5. | Principal Chief Electrical Engineer, Northern Railway, Baroda House, New Delhi - 110 001 | cee@nr.railnet.gov.in |
| 6. | Principal Chief Electrical Engineer, North Central Railway, Block-A, Subedarganj, Prayagraj 211 033. | cee@ncr.railnet.gov.in |
| 7. | Principal Chief Electrical Engineer, North Eastern Railway, Gorakhpur (UP).220 055 | cee@ner.railnet.gov.in |
| 8. | Principal Chief Electrical Engineer, Northeast Frontier Railway, Maligaon, Guwahati - 781011 | cee@nfr.railnet.gov.in |
| 9. | Principal Chief Electrical Engineer, North Western Railway, Jaipur (Raj.) – 302017 | cee@nwr.railnet.gov.in |
| 10. | Principal Chief Electrical Engineer, Southern Railway, Park Town, Chennai - 600 003 (TN) | cee@sr.railnet.gov.in |
| 11. | Principal Chief Electrical Engineer, South Central Railway, Rail Nilayam, Secunderabad – 500 371 | cee@scr.railnet.gov.in |
| 12. | Principal Chief Electrical Engineer, South Eastern Railway, Garden Reach, Kolkata-700 043 | cee@ser.railnet.gov.in |
| 13. | Principal Chief Electrical Engineer, South East Central Railway, Bilaspur (Chhattisgarh).4950 04 | cee@secr.railnet.gov.in |
| 14. | Principal Chief Electrical Engineer, South Western Railway, DRM's Office, Hubli , Karnataka | cee@swr.railnet.gov.in |
| 15. | Principal Chief Electrical Engineer, Western Railway, Churchgate Stn. Bldg, Mumbai - 400 020 | cee@wr.railnet.gov.in |
| 16. | Principal Chief Electrical Engineer, West Central Railway, Jabalpur-482 001 (M.P) | cee@wcr.railnet.gov.in |
| 17. | Director /Electrical, Delhi Metro Rail Corporation Metro Bhawan,8 th Floor,Fire Brigade lane, Barakhamba Road, New Delhi-110001. | eoffice@dmrc.org. |
| 18. | CAO, CORE Central Organisation for Railway Electrification, 1, Nawab Yusuf Road, Civil Lines, Prayagraj -211001 | dceemp@core.railnet.gov.in dyceemp@gmail.com, dyceemp1@gmail.com, dyceemp2@gmail.com, ceempcore@gmail.com, |
| 19. | Chairman and Managing Director RITES LTD, Shikhar, Plot No.01, Sector 29, Gurgaon, Haryana, India-122001 | info@rites.com |
| 20. | Principal Chief Electrical Engineer, Konkan Railway Corporation Limited, Belapur Bhavan, Plot No 6, Sector 11, CBD Belapur, Navi Mumbai – 400614. | cee@krcl.co.in |



सत्यमेव जयते

भारत सरकार GOVERNMENT OF INDIA

रेल मंत्रालय MINISTRY OF RAILWAYS

अनुदेश संख्या: टीआई/आईएन/0052

Instruction No: TI/IN/0052

भारतीय रेल में महत्वपूर्ण सूचना अवसंरचना (सीआईआई) की सुरक्षा के लिए स्काडा सिस्टम में साइबर सुरक्षा दिशानिर्देशों को लागू करने हेतु मानक संचालन प्रक्रिया के संबंध में तकनीकी अनुदेश

**Technical Instruction regarding Standard Operating Procedure for
implementing Cyber Security guidelines
for protection of Critical Information Infrastructure (CII)
of Indian Railways w.r.t SCADA System**

फरवरी, 2025 में जारी (संस्करण 1.0) / Issued in: February, 2025 (Version 1.0)

| | | हस्ताक्षर/Signature |
|----------------------------|---|---------------------|
| अनुमोदित Approved by | प्रधान कार्यकारी निदेशक (कर्षण संस्थापन) Principal Executive Director (TI) | |
| अनुशंसित Recommended by | कार्यकारी निदेशक (कर्षण संस्थापन) Executive Director (TI) | |

जारी कर्ता/ ISSUED BY:

कर्षण संस्थापन निदेशालय

TRACTION INSTALLATION DIRECTORATE,

अनुसंधान अभिकल्प और मानक संगठन

RESEARCH DESIGNS & STANDARDS ORGANISATION,

मानक नगर, लखनऊ- 226011

MANAK NAGAR, LUCKNOW-226011

NOTE: This guideline is the property of RDSO. No reproduction shall be done without the permission of DG (TI) RDSO.

| | Prepared By | Checked By | Issued by |
|-------------|-------------|------------|----------------|
| Signature | | | |
| Date | 11.02.2025 | 11/02/2025 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|--------------|--|--|
| Page 2 of 76 | File No. RDSO-TI/LKO(PSI)/11/2021 O/o PED/TI/RDSO Instruction No. TI/IN/0052 (Version 1.0) | Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|--------------|--|--|

INSTRUCTION FOR: Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System

Instruction No. TI/IN/0052


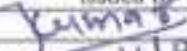
Amendment History

| Version | Instruction No. | Total pages | Date of issue | Reasons for Amendment/ Revision |
|---------|-----------------|-------------|---------------|---------------------------------|
| 1.0 | TI/IN/0052 | 76 | 14/02.2025 | - |

The SCADA System of Indian Railways has been declared as Critical Information Infrastructure (CII) as per directives of National Security Council Secretariat (NSCS), Government of India. Accordingly, the Railway Board has issued Cybersecurity Guidelines for Protection of Critical Information Infrastructure (CII) of Indian Railways (SCADA, CTC/TMS & TCAS), vide File No. 2019/RBCC/7/7/ISSC-CII (Computer No. 3307386).

This Instruction has been prepared to define the Standard Operating Procedures (SOP) for implementing the above Cyber Security Guidelines in Zonal Railways. Therefore, this SOP should be read in conjunction with the latest Cyber security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways (SCADA, CTC/TMS & TCAS) issued by Railway Board and governing RDSO SCADA Specification TI/SPC/RCC/SCADA/0134 or latest.

Further, this guideline is a dynamic document and would change as mandated by the Government of India.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/02/2025 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

INDEX

| S.No. | CONTENTS |
|-------|---|
| 1. | INTRODUCTION |
| 2. | SCOPE |
| 3. | CYBER SECURITY POLICY |
| 4. | INVENTORY AND "IN-USE" ASSET LIFECYCLE MANAGEMENT |
| 5. | USER/DEVICE ACCOUNT LIFECYCLE MANAGEMENT (IDENTIFICATION, AUTHENTICATION, AUTHORIZATION AND ACCESS CONTROL) |
| 6. | VULNERABILITY AND PATCH MANAGEMENT |
| 7. | CONFIGURATION AND CHANGE MANAGEMENT |
| 8. | BACKUP AND DISASTER RECOVERY MECHANISM |
| 9. | SECURITY EVENT / LOG MANAGEMENT |
| 10. | SECURE REMOTE ACCESS |
| 11. | CYBER SECURITY INCIDENT MANAGEMENT |
| 12. | CYBER SECURITY AUDIT |
| 13. | SECURITY OPERATIONS |
| 14. | SERVICE PROVIDER MANAGEMENT |
| 15. | PHYSICAL AND ENVIRONMENTAL SECURITY |
| 16. | CYBER CRISIS MANAGEMENT |
| 17. | CYBERSECURITY AWARENESS AND SKILL TRAINING |

ANNEXURES

| ANNEXURE NO. | DESCRIPTION |
|--------------|---|
| 1. | FORMAT FOR HARDWARE INVENTORY MANAGEMENT |
| 2. | FORMAT FOR SOFTWARE INVENTORY MANAGEMENT |
| 3. | EQUIPMENT ASSETS |
| 4. | COMMUNICATION ASSETS |
| 5. | INFORMATION ASSETS |
| 6. | AREA ACCESS RIGHTS |
| 7. | ELECTRONIC ACCESS RIGHTS |
| 8. | SECURITY TRAINING & BACKGROUND CHECKS |
| 9. | SERVERS & PCs REQUIRING PERIODIC SCANNING |
| 10. | LOCAL AREA NETWORK CONNECTIONS |
| 11. | WIRELESS ACCESS POINTS |
| 12. | WIDE AREA NETWORK CONNECTIONS |
| 13. | TELEPHONE CONNECTIONS (MODEMS) |
| 14. | ENTRY POINTS INTO SENSITIVE AREAS |

| | | | |
|-------------|-------------|------------|----------------|
| Signature | Prepared By | Checked By | Issued by |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|--------------|--|--|
| Page 4 of 76 | File No. RDSO-TIOLKO(PSI)/11/2021 O/o PED/TI/RDSO (Version 1.0) | Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|--------------|--|--|

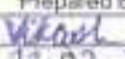

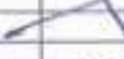
Cybersecurity Policy for SCADA Systems in Indian Railways

1. Introduction

This policy outlines the cybersecurity measures and standard operating procedures for implementing best practices for implementing Cyber Security Guideline in SCADA systems. SCADA system is a critical component of Indian Railways that monitor and control various processes and operations. Various measures such as effective inventory management, patch management, configuration and change management, cyber crisis management etc., are crucial to ensure the availability, integrity, and confidentiality of SCADA system components and to mitigate potential cybersecurity risks.

2. Scope

This policy applies to all personnel involved in the management, operation, and maintenance of SCADA systems, including system administrators, engineers, technicians, and third-party vendors or contractors of Indian Railways.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 17-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

3. Cyber Security Policy

3.1 The CII Entity shall have a Cyber Security and Cyber Resilience Policy drawn upon the guidelines issued by Railway Board, RDSO and NCIIPC.

3.1.1 Version controlled Cyber Security guidelines to be maintained by Zonal Railway.

3.1.2 Review of the guidelines to be done on the following basis:

- On receiving changed guidelines from RB/RDSO/NCIIPC.
- Periodically to be reviewed every 12 months.

3.2 The CII entity shall mandatorily adhere to following key principles while framing Cyber Security and Cyber Resilience policy.

3.2.1 Hard isolation of OT Systems from any internet facing IT system.

3.2.1.1 Zonal Railways shall define policy for implementing strict network segmentation measures to ensure the hard isolation of Operational Technology (OT) systems from any internet-facing Information Technology (IT) systems.

3.2.1.2 It shall be ensured that OT networks are connectivity wise separated from IT networks using firewalls, data diodes etc. to prevent direct communication or access between them.

3.2.2 Transferring of data/information from any internet facing IT system to CII systems should be reduced to the minimum. If absolutely necessary for operational purpose, it should be done only through whitelisted device with scanning for any virus/malware on standalone system as per the SOP laid down. Digital logs are to be retained under the custody of CISO for at least 6 months for such activities and should be readily available to carry out the forensic analysis, if asked by any investigation agency.

3.2.2.1 Guideline for ensuring that transferring data/information from any internet-facing IT system to Critical Information Infrastructure (CII) systems is minimized to the absolute necessary for operational purposes should be laid down. Guidelines for firmware/configuration updates, Anti-virus installation to be laid.

3.2.2.2 Establish a rigorous authorization process requiring justification and approval from appropriate authorities before any data transfer is initiated.

3.2.2.3 Mandate that if data transfer is deemed necessary, it must be conducted exclusively through whitelisted devices with scanning for any virus/malware on standalone systems only.

3.2.2.4 Ensure that the digital logs are kept under the custody of the Chief Information Security Officer (CISO) for a minimum of 6 months for all such activities, ensuring they are readily accessible for forensic analysis upon request by any investigation agency.

3.2.3 List of whitelisted IP addresses for each firewall connected in CII environment should be maintained by CISO and each firewall is configured for allowing communication with the whitelisted IP addresses only.

| | | | |
|-------------|--------------------|--------------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>V. K. Singh</i> | <i>R. K. Singh</i> | <i>J. Kumar</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

- 3.2.3.1 Nominate the Chief Information Security Officer (CISO) as responsible for maintaining a comprehensive list of whitelisted IP addresses for each firewall connected in the Critical Information Infrastructure (CII) environment.
- 3.2.3.2 Regularly review and update the list of whitelisted IP addresses to ensure it reflects current operational requirements and security policies.
- 3.2.3.3 IT security team should be instructed to configure each firewall in the CII environment to allow communication only with the whitelisted IP addresses maintained by the CISO.
- 3.2.4 All ICT based equipment/system deployed in infrastructure/system mandatorily in CII are sourced from the list of the "Trusted Sources" as and when drawn by Railway Board / RDSO.**
- 3.2.4.1 Guidelines for mandating that all Information and Communication Technology (ICT) based equipment/systems deployed in the infrastructure/system of the Critical Information Infrastructure (CII) must be sourced from the list of "Trusted Sources" drawn by the Railway Board / RDSO.
- 3.2.4.2 Ensure strict compliance with procurement policies and guidelines established by the Railway Board / RDSO to ensure the procurement of ICT equipment from trusted and reliable sources.
- 3.2.4.3 Document and maintain records of the sourcing process, including verification of the source against the trusted sources list, to ensure transparency and accountability in the procurement of ICT equipment for the CII infrastructure/system.
- 3.2.4.4 To make sure that the addition / deletion in the "Trusted Sources" list to be done only after approval from Railway Board/RDSO.
- 3.2.5 The cyber security policy should include the following process to identify, assess and manage cyber security risks;**
- 'Identify' critical IT assets and risks associated with such assets.
 - 'Protect' assets by deploying suitable controls and tools.
 - 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
 - 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack.
 - 'Recover' from incident through incident management, disaster recovery, and business continuity framework.
- 3.2.5.1 SCADA Already identified as Critical IT asset
- 3.2.5.2 Necessary protection controls / tools already deployed as per RDSO specifications.
- 3.2.5.3 Periodic checking of firewall/data diode logs, patch management logs, Logs of configuration tools for detecting incidents/attempts of attacks, recording & publishing of any anomalies and actions required thereof.
- 3.2.5.4 Implement Intrusion detection systems (IDS), Security information and event management (SIEM) solutions, and threat intelligence feeds to enhance detection capabilities and enable timely response to security incidents.
- 3.2.5.5 Develop and maintain an incident response plan outlining procedures and responsibilities for responding to security incidents, anomalies, or attacks, e.g.,

| | | | |
|-------------|---------------|---------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>R.D.P.</i> | <i>J. Singh</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

- a) Attack from internet
 - b) Potential threat of attack through Physical breach
 - c) Unauthorized firmware/configuration update etc.
- 3.2.5.6 Establish a designated incident response team trained to assess, contain, and mitigate the impact of security incidents promptly. It should have a documented plan for commonly known incidents
- 3.2.5.7 Implement incident management, disaster recovery, and business continuity frameworks to facilitate timely recovery and restoration of affected IT assets and business operations.
- 3.2.5.8 Conduct post-incident reviews and lessons learned exercises to identify areas for improvement and enhance cyber resilience for future incidents.

3.2.6 Following of IT Rules 2018 for Protected Systems.

- 3.2.6.1 Ensure all relevant personnel are aware of the provisions outlined in the IT Rules 2018 for Protected Systems.
- 3.2.6.2 Establish processes and controls to ensure compliance with the specific requirements outlined in the IT Rules 2018 for Protected Systems.
- 3.2.6.3 Regularly review and update internal policies and procedures to align with the requirements of the IT Rules, ensuring ongoing compliance with regulatory obligations.

3.2.7 Designating a senior official as Chief Information Security Officer (CISO) whose function would be to manage cyber security risks, respond to incidents, enforcement of IT rules 2018, implementation of processes and procedures as per the cyber security policy approved by the Railway Board.

- 3.2.7.1 Nominate a senior official within the organization to serve as the Chief Information Security Officer (CISO).
- 3.2.7.2 Ensure that the appointed individual possesses the necessary knowledge to effectively manage cyber security risks and enforce compliance with IT rules 2018.
- 3.2.7.3 Define and document the roles and responsibilities of the CISO.

3.3 Provision of dedicated cyber security division, skilled manpower and sufficient annual cyber security specific budget.

- 3.3.1. Version controlled guidelines defining the purpose, responsibilities, size, manpower allocation, budget planning & approval for dedicated cyber security division to be maintained.
- 3.3.2. Nomination of responsible person at Zonal/Divisional level for monitoring of processes and guideline under cyber security division and its implementation at division level.
- 3.3.3. Review of the guidelines to be done on the following basis:
- 3.3.4. To reflect changes in organizational needs, industry standards, and regulatory requirements.
- 3.3.5. Based on the feedback for identifying areas of enhancement and implement continuous improvement initiatives.

| | | | |
|-------------|---------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Atul</i> | <i>Jyoti</i> |
| Date | 21.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

3.4 The CII Entity shall ensure annual review of their Cyber Security Policy by subject matter expert and changes shall be made therein only after obtaining the due approval from Railway Board.

- 3.4.1. Nominate a qualified consultant to conduct an annual review of the Cyber Security Policy.
- 3.4.2. The consultant should assess the policy's effectiveness, identifies necessary changes and prepares recommendations for improvement.
- 3.4.3. Submit the proposed changes to the Cyber Security Policy to the Railway Board for review and approval.

3.5 The process of Access Management for all Cyber Assets owned or under control of the CII Entity shall be detailed in the Cyber Security Policy.

- 3.5.1. Frame common access management guidelines for SCADA related assets in consultation with Zonal Railway. Assets supplied under SCADA is detailed in the Cyber Security Policy.
- 3.5.2. Specify access control measures, procedures for granting and revoking access rights and guidelines for user authentication and authorization.
- 3.5.3. Policy to be updated annually to address changes in technology, regulations, or organizational requirements, ensuring alignment with best practices and industry standards.

3.6 The CII Entity shall be solely responsible to get Cyber Security Policy implemented through its Information Security Division (ISD).

- 3.6.1. Designate the Information Security Division (ISD) as solely responsible for implementing the Cyber Security Policy.
- 3.6.2. Organizational framework required at RB/Zonal HQ/Division level to be put in place for implementation of Cyber Security. The roles and responsibilities of the ISD as a whole/of various officials should be clearly outlined for overseeing the implementation process.
- 3.6.3. The ISD should coordinate with relevant departments and stakeholders to ensure effective implementation within specified timelines including training, awareness programs and compliance monitoring.

3.7 The CISO shall record the reason(s) for exemption required, if any, in case unable to comply with any of the provision(s) of the Cyber Security Policy. Any exception shall be approved by Railway Board with provision(s) of compensatory control(s).

- 3.7.1. The Chief Information Security Officer (CISO) shall document the reason(s) for exemption required if unable to comply with any provision(s) of the Cyber Security Policy.
- 3.7.2. Expert/Consultant's view to be taken on exception.
- 3.7.3. The justification for the exemption should be recorded, including any mitigating factors or operational constraints in a designated exemption log or documentation system.
- 3.7.4. All the request for exemption should be submitted along with the documented justification to the Railway Board for review and approval.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | 11/11/25 | Jumna |
| Date | 11.02.2025 | | 11/02/25 |
| Designation | JE/TI | AOE/TI-3 | DIRECTOR/ TI-3 |

3.8 CII Entity shall ensure that cyber security issues are taken up as agenda items in the ISSC meetings of Protected Systems conducted quarterly.

- 3.8.1. The CII Entity shall collect and document the cyber security issues to be presented in the quarterly review in ISSC meeting.
- 3.8.2. It should ensure through timely communication that cyber security issues are included as agenda items in the Information Security Steering Committee (ISSC) meetings of Protected Systems conducted quarterly.
- 3.8.3. The agenda items should encompass discussions on current cyber security threats, vulnerabilities, incidents, risk assessments and mitigation strategies relevant to Protected Systems.
- 3.8.4. The Information Security Division (ISD) should prepare relevant materials and reports on cyber security issues to be presented during ISSC meetings.
- 3.8.5. The reports presented by ISD should highlight key findings, recommendations and action plans to address identified cyber security challenges, facilitating informed decision-making by the committee members.

3.9 Dedicated policy for protection of cloud infrastructure, if any.

- Not applicable in case of SCADA system.

| | | | |
|-------------|---------------|--------------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>R. K. Singh</i> | <i>J. Kumar</i> |
| Date | 11-02-2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

4. Inventory Management

4.1 Establish and Maintain Detailed Hardware Asset Inventory: The organization shall prepare an IT and OT asset inventory register to document all the information assets such as PCs, laptops, servers, database, Printer, Network devices, Firewall, Storage devices related to CII systems along with the details of Vendor, Model number, Serial Number, software version installed, AMC partner details and the exact location of the asset.

- 4.1.1. Maintain an accurate and up-to-date inventory of all SCADA system hardware components, including control systems, programmable logic controllers (PLCs), human-machine interfaces (HMIs), Remote Terminal Units (RTUs), and communication devices. (Refer Annexures).
- 4.1.2. Nomination of a responsible team or individual at division level to maintain the SCADA asset inventory register.
- 4.1.3. A standardized template to be developed to document all information assets, including PCs, laptops, servers, printers, network devices, firewalls, Data Diodes, Biometric Terminals, storage devices, RTUs related to CII systems.
- 4.1.4. Inventory register should be updated regularly to reflect changes in hardware assets, such as additions, removals or modifications.
- 4.1.5. The inventory register should have all relevant details including vendor information, model numbers, serial numbers, software versions, subscription related information, if any, installation date, End of Life information, AMC partner details and asset locations, accurately documented and kept up-to-date.
- 4.1.6. Assign unique identifiers (e.g., asset tags, serial numbers) to each hardware component for tracking purposes.

4.2 The inventory shall include assets connected to the infrastructure physically, virtually, remotely and those within cloud environments. Additionally, it includes assets that are regularly connected to the organization's network infrastructure, even if they are not under control of the organization. Review and update the inventory of all assets regularly. These shall be countersigned by a senior official on a regular basis.

- 4.2.1. The inventory should include all SCADA assets connected to the organization's infrastructure physically, virtually & remotely. A few examples are:
 - a) S&T channels related to RTU communication.
 - b) S&T's ST1 equipment, network switches, EI equipment, OFC converters etc. related to RTU communication.
 - c) Railnet links related to SEMC connectivity.
- 4.2.2. The inventory should also include assets that are regularly connected to the organization's network infrastructure, even if they are not under direct control of the organization, to maintain a comprehensive overview of the asset landscape.
- 4.2.3. Proper schedule to be established for reviewing and updating the inventory of all assets on a regular basis, such as quarterly or half yearly, to ensure accuracy and identify any discrepancies or unauthorized modifications.
- 4.2.4. It should be mandatory that the updated inventory records should be countersigned by a senior official within the organization to validate the accuracy and completeness of the inventory data.

| | | | |
|-------------|----------------|--------------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>V. Kach</i> | <i>R. K. Singh</i> | <i>J. Kumar</i> |
| Date | 11-02-2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

4.3 Maintain a detailed inventory of all software: Maintain an accurate and up-to-date inventory of all SCADA system software components, including operating systems, application software, firmware, and configuration files.

- 4.3.1. A guideline for maintaining the detailed inventory of all software installed on hardware assets should be formed.
- 4.3.2. All the essential details should be documented such as URLs, version(s), deployment mechanisms & dates, vendor, version, patch levels, installation date and decommission dates for each software application.
- 4.3.3. Software inventory should be regularly updated to reflect changes in installed software, including new installations, updates and uninstallations.
- 4.3.4. Implement a secure software update and patch management process to ensure that software components are kept up-to-date with the latest security patches and updates.
- 4.3.5. Regularly review and update the software inventory to ensure accuracy and identify any discrepancies or unauthorized modifications.

4.4 The organization shall prepare a network/system design architecture of critical assets with their associated hardware clearly depicting the connectivity between various assets.

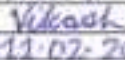

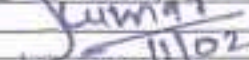
- 4.4.1. Nominate a team of qualified personnel to prepare the network/system design architecture of SCADA assets.
- 4.4.2. They should gather necessary information about SCADA assets, including hardware specifications, connectivity requirements and dependencies to create a comprehensive architecture.
- 4.4.3. Utilize standardized visualization tools or diagrams to illustrate the interconnections, interfaces, and data flows among critical assets, ensuring clarity and comprehensiveness.

4.5 The network/system design architecture shall be readily available with Section-in-charge of critical areas like data logger room, Server room etc.

- 4.5.1. The network/system design architecture should be readily available with Section-in-charge of critical areas such as the server room, Remote control centre etc.
- 4.5.2. Copies of the architecture should be distributed to designated personnel responsible for managing and overseeing critical areas to ensure easy access and reference.
- 4.5.3. Maintain the network/system design architecture up-to-date with any changes or modifications in the infrastructure.

4.6 Address Unauthorized Hardware or Software Asset: Ensure that a process exists to address unauthorized assets on regular basis.

- 4.6.1. Implementation of proactive process for monitoring and detecting unauthorized hardware or software assets within the organization's infrastructure.
- 4.6.2. Automated scanning tools should be utilized, network monitoring solutions and regular audits should be done to identify any unauthorized assets promptly.
- 4.6.3. Guidelines to be defined for addressing unauthorized assets upon detection, action to be taken for investigating the origin and purpose of the unauthorized asset.
- 4.6.4. Process to implement appropriate remediation measures, such as removal from the network, disabling access, or uninstalling unauthorized software to be defined.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

4.7 Utilize an Active Discovery Tool: Utilize an active discovery tool to identify hardware and software assets connected to the organization's network. Configure the active discovery tool to execute daily, or more frequently, if required.

- 4.7.1. Functionality of discovery tool(s) be defined.
- 4.7.2. Configuration of these active discovery tool to execute daily or more frequently if required, to ensure comprehensive coverage and timely detection of assets.
- 4.7.3. Process to be defined for monitoring of the results generated by the active discovery tool on a regular basis to identify new assets, changes or anomalies in the network environment.
- 4.7.4. Analyse the discovered assets to verify their legitimacy, ensure compliance with organizational policies and address any unauthorized or unmanaged assets promptly.

4.8 Allow list of Authorized Software, libraries and scripts: Use technical controls to ensure that only authorized software, libraries and scripts, such as specific .dll, .ocx, .so, .ps1, .py, etc., files are allowed to load into a system process. Block unauthorized libraries and scripts from loading into a system process. Reassess bi-annually, or more frequently, if required.

- 4.8.1. Develop a comprehensive allow list of authorized software, libraries, and scripts, including specific file types such as .dll, .ocx, .so, .ps1, .py, etc., that are permitted to load into system processes. OEM's requirements to be taken care.
- 4.8.2. Implement robust technical controls to enforce the allow list, ensuring that only authorized software, libraries and scripts are permitted to execute within the organization's environment, while blocking unauthorized ones.
- 4.8.3. Conduct half yearly or more frequent if required, reassessments of the allow list to ensure its accuracy and effectiveness in reflecting the organization's current software and script requirements.
- 4.8.4. Update the allow list as necessary to accommodate changes in authorized software, libraries, and scripts, and to mitigate emerging security risks or vulnerabilities.

4.9 System Development Lifecycle: Link asset management to system development lifecycle (SDLC) which includes five phases planning, procurement / acquisition, implementation, operation & maintenance and disposal. It provides many benefits such as, a means to identify milestones for an asset (e.g. software testing completion, facility upgrade), early identification of potential vulnerabilities in assets, awareness of potential challenges in the assets as the designs are reviewed, documentation of resilience decisions for each SDLC phase.

- 4.9.1. Incorporate asset management practices into each phase of the System Development Lifecycle (SDLC), including planning, procurement/acquisition, and implementation as per guiding standards, operation & maintenance and disposal in accordance with RDSO Specifications.
- 4.9.2. Ensure that asset-related milestones, such as software testing completion or facility upgrades, are identified and tracked throughout the SDLC process to facilitate effective asset management.
- 4.9.3. Link the integration of asset management with SDLC to enable early identification of potential vulnerabilities in assets and awareness of challenges during the design phase.

| | | | |
|-------------|---------------|--------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Rishi</i> | <i>Sumar</i> |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | AOE/ TI-3 | DIRECTOR/ TI-3 |

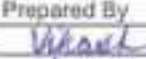

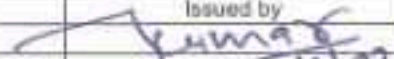
4.10 Secure Configuration of Assets: Establish and maintain the secure configuration of hardware assets, software assets and Network Infrastructure. Following configurations should be implemented on immediate basis.

4.10.1. Implementation of the following configurations on an immediate basis to ensure the secure configuration of hardware assets, software assets, and network infrastructure:

- Enable application whitelisting to prevent unauthorized applications from running on the system.
- Permanently block/disable unused ports to minimize potential attack surfaces.
- Ensure that all workstations have active and updated antivirus software with the latest signatures.
- Configure firewalls with appropriately tailored rules to protect CII systems against cyber security threats and reduce potential attacks.
- Update firewall signatures regularly, and prohibit default configurations while implementing whitelisting and geo-fencing as per operational requirements.
- Restrict access rule management of firewalls to authorized personnel responsible for firewall administration.
- Install only genuine operating systems and required software with the latest updates to mitigate vulnerabilities.
- Disable remote access to databases, application servers, and PCs related to CII systems to minimize unauthorized access risks.
- Segment and segregate networks and functions to enhance security and control access.
- Harden network devices and implement secure access measures such as Multi-Factor Authentication (MFA) and least privilege principles.
- Certify the integrity of assets by RDSO before deployment to mitigate supply chain risks.
- Harden servers and desktops before deployment to enhance their security.

4.10.2. Document all configurations implemented as part of the secure configuration process, including details such as dates of implementation and responsible personnel.

4.10.3. Establish procedures for regular monitoring and auditing of configurations to ensure ongoing compliance with security standards and regulatory requirements.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 21.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 14 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

5. User/ Device Account Lifecycle Management (Identification, Authentication, Authorization and Access Control):

5.1. Establish and follow a process, preferably automated for granting access and revoking access to critical assets. Only authorized Personnel shall be permitted to enter in critical areas like Data logger room, Server Rooms, signalling room, Electrical Equipment rooms etc.

- 5.1.1 Establishing a formal process, preferably automated, for granting and revoking access to SCADA assets such as Server Rooms, control centre etc.
- 5.1.2 Zonal Railways shall define clear procedures outlining the steps for requesting access, approval workflow, access provisioning, periodic review, and revocation of access rights.
- 5.1.3 It shall be ensured that only authorized personnel with legitimate business needs to access critical areas.
- 5.1.4 Implementation of access control measures such as key card access, biometric authentication or access codes to restrict entry to authorized personnel only.
- 5.1.5 Regularly monitor access logs and conduct audits to ensure compliance with access control policies and promptly revoke access for personnel who no longer require access or whose access privileges have been revoked.

5.2. Only authorized users shall be granted permission to access in the network, application, database etc.




- 5.2.1 Establishing a formal process for authorizing user access to the network, applications, databases, and other resources.
- 5.2.2 Define clear criteria and procedures for granting access permissions, including user roles, responsibilities, and the level of access required for each resource.
- 5.2.3 Implement robust authentication mechanisms, such as username/password, multi-factor authentication (MFA), or biometric authentication, to verify the identity of users.
- 5.2.4 Enforce strict authorization controls to ensure that only authorized users with valid credentials are granted access to the network, applications, databases, and other resources, while unauthorized access attempts are promptly detected and prevented.

5.3. Review of all privileged accounts at periodic intervals (not more than a year).

- 5.3.1 Conduct periodic reviews of all privileged accounts at regular intervals, not exceeding one year, to ensure compliance with security policies, identify any unauthorized access or changes, and promptly revoke access for any inactive or unnecessary privileged accounts.

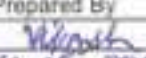
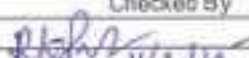
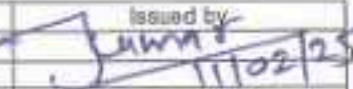
5.4. Role based access control must be exercised and access must be given only on need-to-know basis with least privilege mechanism. Centralize access control should be implemented.

- 5.4.1 Define roles within the organization based on job responsibilities, and assign access permissions accordingly.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 15 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 5.4.2 Ensure that access is granted only on a need-to-know basis, following the principle of least privilege, where users are given the minimum level of access required to perform their duties effectively.
- 5.4.3 Implement a centralized access control mechanism to manage and enforce access policies consistently across the organization.
- 5.4.4 Centralize user authentication and authorization processes, such as user provisioning, role assignment, and access revocation, to ensure uniformity, ease of administration, and enhanced security.
- 5.5. Administrator privileges on attendant IT systems (desktops/servers) shall be given to only section-in-charge.**
- 5.5.1 Limit administrator privileges on SCADA systems, including desktops and servers, to only the designated section-in-charge personnel.
- 5.5.2 Implement strict access controls and authentication mechanisms to ensure that only authorized section-in-charge personnel have administrative access to the systems.
- 5.5.3 Regularly monitor and audit administrator access activities to detect any unauthorized access attempts or suspicious activities and take immediate corrective actions as necessary.
- 5.6. User login to the network shall be controlled and monitored.**
- 5.6.1 Implement robust controls to regulate and monitor user login activities on the network, including authentication mechanisms, user access policies, logging of login events, and regular monitoring of user login activities to detect and respond to any unauthorized access attempts or suspicious behaviour promptly.
- 5.7. The Department must have a policy to define different user levels and privileges.**
- 5.7.1 Establish a policy within the department to define different user levels and associated privileges based on job roles, responsibilities, and access requirements.
- 5.7.2 Document the policy comprehensively, outlining the criteria for each user level, the privileges granted to users at each level, and the process for requesting, approving, and revoking access privileges.
- 5.7.3 Assign access privileges to users according to their designated user levels, ensuring that access is granted on a need-to-know basis with the principle of least privilege, and periodically review and update access privileges as necessary to maintain security and compliance.
- 5.8. HMI frames must be password protected. Admin privileges must be restricted.**
- 5.8.1 Ensure that all Human-Machine Interface (HMI) frames are password protected to prevent unauthorized access.
- 5.8.2 Restrict administrator privileges for HMI frames to authorized personnel only, such as system administrators or designated operators.
- 5.9. The department must maintain an inventory of user authentication and authorization levels for accessing logs and data.**

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | AOE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 16 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 5.9.1 Establish a centralized inventory system to document user authentication and authorization levels for accessing logs and data within the department.
- 5.9.2 Clearly define the categories of users, their roles, and the corresponding access privileges required to access logs and data.
- 5.9.3 Conduct periodic reviews of the inventory to ensure accuracy and compliance with security policies, and promptly revoke access for users who no longer require it or whose roles have changed.

5.10. The Department must maintain accounting and audit trail log monitoring system.

- 5.10.1 Establish an accounting and audit trail log monitoring system within the SCADA system to track and record all relevant activities, including user logins, access attempts, data modifications, and system configurations.
- 5.10.2 Configure the monitoring system to capture and store logs securely, ensuring their integrity and availability for audit and analysis purposes.
- 5.10.3 Regularly monitor and review the accounting and audit trail logs to detect any unauthorized or suspicious activities, compliance violations, or security breaches.
- 5.10.4 Implement automated alerts or notifications to promptly notify designated personnel of any anomalous activities, enabling timely investigation and response to mitigate potential risks or threats.

5.11. The management of log data and its security must be assigned to an individual who should be a regular employee of the Department.

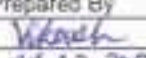
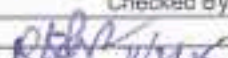
- 5.11.1 Nominate a regular employee of the department to be responsible for the management of log data and its security.
- 5.11.2 Ensure that the appointed individual possesses the necessary skills, expertise, and knowledge to effectively manage log data and adhere to security protocols.
- 5.11.3 Clearly outline the responsibilities of the assigned individual, including the collection, storage, protection, and analysis of log data, as well as ensuring compliance with relevant security policies and regulations.

5.12. Wi-Fi access on CII systems and devices connected with them must be disabled.

- 5.12.1 Configure SCADA systems and associated devices to disable Wi-Fi access by default.
- 5.12.2 Ensure that Wi-Fi adapters on SCADA systems are physically disabled or software-controlled to prevent unauthorized activation.
- 5.12.3 Regularly monitor SCADA systems and devices to ensure Wi-Fi access remains disabled.
- 5.12.4 Implement periodic audits and inspections to verify compliance with the Wi-Fi access policy, and promptly address any instances of non-compliance through corrective actions or additional safeguards.




5.13. Strict password management policy should be framed and implemented. Strong password should have the following characteristics:

- a. Must contain both upper and lower case characters and digits, special characters, as well as at least 12 alphanumeric characters long.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 14.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 17 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- b. **Must not be a word in any language, slang, dialect, jargon etc. not based on personal information, names of family etc.**
 - c. **All system level passwords (e.g. root, enable, administrator, application administration accounts etc.) shall be changed at least every 30 days. Set periodicity of others.**
- 5.13.1 Develop a strict password management policy that adheres to industry best practices and regulatory requirements.
- 5.13.2 Implement the policy across all systems, applications, and services within the organization to ensure uniformity and consistency in password management practices.
- 5.13.3 Require all users to create passwords that meet the specified criteria, including:
- a) Containing both upper and lower case characters, digits, and special characters.
 - b) Being at least 12 characters long and not based on easily guessable personal information.
- 5.13.4 Implement technical controls to enforce these password requirements, such as password complexity rules and regular password expiration policies.
- 5.14. Implement MFA for externally exposed applications, Remote network access and administrative access.**
- 5.14.1 Implement Multi-Factor Authentication (MFA) for externally exposed applications, remote network access, and administrative access to enhance security by requiring users to verify their identity using multiple factors such as passwords, biometrics, smart cards, or tokens, thereby reducing the risk of unauthorized access and protecting sensitive information from potential cyber threats.
- 5.15. Bring Your Own Device (BYOD) to be strictly prohibited and monitored for compliance. In case of operational requirements its policy for proper use from limited device and monitoring be approved.**
- 5.15.1 Access to all external devices such as CDs/USB ports etc. to be kept disabled.
- 5.15.2 Undertaking to be taken from relevant staff members/Maintenance staff of Railway/OEMs for not using any external device on SCADA computers except for loading software/configuration patches for patch management.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|--|
| Page 18 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System. |
|---------------|---|--|

6. Vulnerability and Patch Management

6.1 Establish and maintain a documented vulnerability management process for all assets, especially CII assets. Review and update documentation annually, or when significant changes occur that could impact this safeguard.

- 6.1.1 Zonal Railways shall develop a documented vulnerability management process for the SCADA assets, with a particular focus on Critical Information Infrastructure (CII) assets.
- 6.1.2 Define clear procedures for identifying, assessing, prioritizing, mitigating and monitoring vulnerabilities across the SCADA infrastructure, including regular vulnerability scans and assessments.
- 6.1.3 Conduct an annual review of the vulnerability management process documentation to ensure its accuracy, effectiveness, and alignment with current security practices and organizational requirements.
- 6.1.4 Update the documentation as necessary to reflect any significant changes in the SCADA infrastructure, technology landscape, regulatory requirements or security posture that could impact the effectiveness of the vulnerability management safeguard.

6.2 Patches to the CII systems shall be applied as per RDSO's instruction and OEM's recommendations as and when released to ensure that the systems are protected against the recent cyber security threats.

- 6.2.1 Adhere to the instructions provided by Zonal Railway regarding patch application for CII systems.
- 6.2.2 Follow the recommendations and guidelines issued by SCADA vendors for patching CII systems, promptly applying patches as and when released to mitigate vulnerabilities and protect against emerging cyber threats.
- 6.2.3 Establish a systematic process for identifying, testing, and deploying patches to CII systems in a timely manner, prioritizing critical patches that address high-risk vulnerabilities or known exploits.
- 6.2.4 The SCADA Vendor shall first test their patches internally and submit the internal test report to RDSO. RDSO shall verify the test report and upon finding it satisfactory, the patches may be tested in the test environment of SCADA System of Indian Railways.
- 6.2.5 The patches before deploying in live environment shall be tested in a test environment under the monitoring and supervision of the Competent Authority of Zonal Railways (not below Sr. DEE/TRD or Dy. CEE/TRD). The Zonal Railways shall submit the Joint test report of (OEMs & Zonal Railways) to RDSO. RDSO shall verify the test report and, only upon finding it satisfactory, shall the patches be deployed in live environment/ SCADA System.
- 6.2.6 Regularly monitor patch releases from Zonal Railway and SCADA vendors and promptly apply patches to CII systems following thorough testing and validation procedures to minimize disruption to critical operations while ensuring effective security enhancements.

6.3 The proprietary software of the OEMs should be certified by RDSO. An independent third party certification (CERT-In empanelled institutions) is recommended.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | | 11.02.25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 19 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

6.3.1 Ensure relevant certifications have been done by approved agencies with respect to Operational Technology (OT) infrastructure, wherever applicable and the same shall be verified by RDSO.

6.4 Proper backup of the system should be taken before deploying the patch to ensure service continuity.

6.3.1 Before deploying any patch, ensure that a proper backup of the system is taken to safeguard against potential issues or failures during the patching process and to facilitate restoration in the event of service disruption or data loss, thereby ensuring service continuity and minimizing the impact of patch deployment on critical operations.

6.5 Any changes in system/application related to CII systems including patch update, modification/enhancement must be tested in Test environment and certified by RDSO before moving into live environment. Log for all such changes should be maintained.

6.5.1 Prior to implementation in the live environment, all changes to system/application related to SCADA systems, including patch updates, modifications, or enhancements, must undergo thorough testing in a dedicated test environment.

6.5.2 Conduct comprehensive testing to verify the functionality, performance, and compatibility of the changes with existing systems and processes, ensuring that any potential issues or conflicts are identified and addressed prior to deployment.

6.5.3 This shall be done under the monitoring and supervision of the Competent Authority of Zonal Railways. The Zonal Railways shall submit the test report to RDSO.

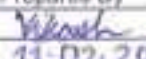
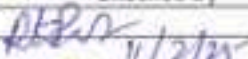
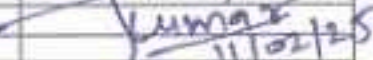
6.5.4 RDSO shall verify the test report by validating compliance with established standards, specifications, and security requirements and only upon finding it satisfactory, shall the patches be deployed in the live environment.

6.5.5 Maintain detailed logs documenting all changes made to SCADA systems, including patch updates, modifications, or enhancements, along with corresponding testing results, certification status, and any relevant information pertaining to the change process, to ensure transparency, accountability, and traceability of system modifications.

6.6 RDSO should validate any new technology, both for Industrial Control Systems and their associated software that may be introduced.

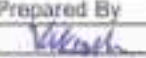

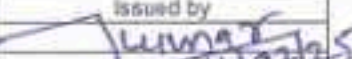
6.5.6 Before introducing any new technology, including Industrial Control Systems (ICS) and associated software, RDSO validation is mandatory. This process ensures that the technology meets established standards, specifications, and security requirements, providing assurance of compatibility, reliability, and resilience within the critical infrastructure environment.

6.7 The department shall ensure, as part of Service Level Agreements (SLA) that the service provider (OEMs/AMC) should implement all the patches with respect to IT & OT required for all security control measures in time bound manner to address the latest vulnerabilities and insecurities released by NCIPC/CERT-In and other LEAs which could impact the system adversely or result in information disclosure or destruction.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11-02-2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 26 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 6.7.1 Incorporate specific provisions within Service Level Agreements (SLAs) with service providers, including OEMs and AMC vendors, requiring them to implement all security control measures in a timely manner.
- 6.7.2 Clearly outline the responsibilities and obligations of the service provider regarding the implementation of security controls to address the latest vulnerabilities and insecurities identified by the NCIIPC, CERT-In, and other Law Enforcement Agencies (LEAs).
- 6.7.3 The SCADA vendors shall check whether the patches released for the IT system are compatible with their OT system and correspondingly upgrade the OT system with respect to patches in the IT system. This shall be done periodically, every six months. In instances where the patches released or issued for the IT system are incompatible with the OT system, the SCADA vendors are required to provide a detailed explanation for this incompatibility. Additionally, they must outline the impact of these patches on the OT system and specify the timeline for their implementation. Furthermore, they shall furnish a biannual report on the complete details of all the patches released for the IT system and any compatibility issues with the OT system (if any) to ZRs, including RDSO.
- 6.7.4 Define time-bound requirements within SLAs for the implementation of security control measures by the service provider, specifying deadlines and milestones for addressing identified vulnerabilities and insecurities.
- 6.7.5 Regularly monitor and assess the service provider's compliance with SLA requirements, ensuring that all security control measures are implemented promptly to mitigate potential risks and safeguard critical infrastructure systems against adverse impacts, information disclosure, or destruction.
- 6.8 Establish and maintain a risk-based remediation strategy with periodic reviews.**
- 6.8.1 Develop and maintain a risk-based remediation strategy that identifies, prioritizes, and addresses security vulnerabilities and risks within the SCADA infrastructure, systems and processes, conducting periodic reviews to reassess risks, update remediation priorities, and ensure alignment with evolving threats, industry best practices, and regulatory requirements.
- 6.9 Patch and update management with staging mechanism be implemented.**
- 6.9.1 Implement a patch and update management process that includes staging mechanisms to systematically deploy and test patches and updates in controlled environments before rolling them out to production systems, ensuring thorough validation of patch compatibility, functionality, and stability to minimize disruption and mitigate potential risks to critical operations and services.
- 6.10 Perform periodic automated vulnerability scans of intranet assets and externally exposed assets.**
- 6.10.1 Establish a schedule for performing periodic automated vulnerability scans of both intranet assets (internal network resources) and externally exposed assets (public-facing systems).
- 6.10.2 Define the frequency of scans based on risk assessment and regulatory requirements, ensuring that scans are conducted regularly to identify and address vulnerabilities in a timely manner.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

File No.RDSO-TI0LKO(PSI)/11/2021-O/o PED/TI/RDSO

| | | |
|---------------|--|---|
| Page 21 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

- 6.10.3 Configure the vulnerability scanning tools to cover all relevant intranet and externally exposed assets, including servers, workstations, network devices, web applications, and other critical infrastructure components.
- 6.10.4 Ensure that the scans are comprehensive, covering a wide range of vulnerabilities and attack vectors, and utilize up-to-date vulnerability databases and scanning techniques to accurately identify potential security weaknesses and threats.

| | | | |
|-------------|------------------------------|-------------------------|---------------------------|
| Signature | Prepared By <i>Vikash</i> | Checked By <i>RK</i> | Issued by <i>Suman</i> |
| Date | 21-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 22 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

7. Configuration and Change Management:

7.1. Establish and maintain a configuration and change management plan for CII assets (Hardware, Software, Networking Infrastructure etc.).

- 7.1.1 Zonal Railways shall develop a comprehensive configuration and change management plan specifically tailored for SCADA assets, including hardware, software and networking infrastructure.
- 7.1.2 Define the scope of the plan, outlining which assets are covered, the roles and responsibilities of personnel involved, and the procedures for documenting, reviewing, approving, and implementing configuration changes.
- 7.1.3 Regularly maintain and review the configuration and change management plan to ensure its effectiveness and relevance in mitigating risks and maintaining the security, integrity and availability of SCADA assets.
- 7.1.4 Continuously monitor and track configuration changes, documenting any modifications or updates made to SCADA assets and conduct periodic audits and assessments to verify compliance with established configuration standards.

7.2. These changes should be permitted only following an approved process where competent authority is defined for each kind of change.




- 7.2.1 Develop a standardized process for approving changes, ensuring that all modifications to systems, software, or infrastructure are subject to review and authorization.
- 7.2.2 Define the competent authority responsible for approving each type of change, assigning roles and responsibilities to individuals or teams with the appropriate expertise and authority to assess and authorize changes effectively.
- 7.2.3 Facilitate thorough evaluation of change requests by the competent authority, considering factors such as impact assessment, risk analysis, compliance requirements, and business objectives, before granting approval for implementation.

7.3. Strict security vetting of the proposed changes should be implemented.

- 7.3.1 Conduct a thorough security vetting process for all proposed changes, including modifications to SCADA systems, software, or infrastructure.
- 7.3.2 Utilize security assessment tools, techniques, and methodologies to evaluate the potential impact of changes on the organization's security posture, identifying and mitigating any vulnerabilities or risks that may arise from the proposed modifications.
- 7.3.3 Require security vetting to be completed before changes are approved for implementation, ensuring that all security considerations are adequately addressed and that the organization's security controls remain effective and resilient against emerging threats.

7.4. As part of obtaining initial support for a configuration and change management plan, the organization should allocate a budget for ongoing planning and execution of changes.

- 7.4.1 Establish a structured process for allocating budget resources for configuration and change management activities as part of the organization's planning and budgeting cycle.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 23 of 76 | Instruction No. TIIN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

- 7.4.2 Ensure that the budget allocation aligns with the strategic objectives and priorities of the organization, taking into account the anticipated costs associated with implementing and maintaining the configuration and change management plan.
- 7.4.3 Regularly review and adjust the budget allocation as needed to accommodate changes in organizational priorities, emerging risks, and evolving regulatory requirements, ensuring that adequate financial resources are available to support effective configuration and change management practices.
- 7.5. Map assets related to critical services and identify configuration items of the assets that will undergo change and require change and configuration management.**
- 7.5.1 Develop a systematic process for mapping assets related to SCADA system including hardware and software, to identify their roles and dependencies within the organization's IT environment.
- 7.5.2 Utilize asset management tools and techniques to create an inventory of critical assets, documenting key attributes such as asset type, location, ownership, and relationship to critical services.
- 7.5.3 Identify configuration items (CIs) associated with mapped assets that are subject to change and require change and configuration management.
- 7.5.4 Define criteria for selecting CIs based on factors such as their impact on critical services, frequency of changes, and dependencies with other assets, ensuring that all relevant CIs are accurately identified and managed throughout the change lifecycle.
- 7.6. Once all the configuration items have been identified then implement and control configuration changes.**
- 7.6.1 Develop a standardized process for implementing configuration changes to identified configuration items (CIs), ensuring that changes are carried out systematically and in accordance with established procedures.
- 7.6.2 Assign responsibilities to designated personnel or teams responsible for implementing configuration changes, specifying roles and tasks for each stage of the change implementation process.
- 7.6.3 Utilize change management tools and workflows to document and track change requests, approvals, implementation status, and associated activities, ensuring that changes are reviewed, authorized, and implemented in a controlled and transparent manner to minimize risks and disruptions to critical services.
- 7.7. Monitor Configuration Changes. In this phase, ensure that changes are identified, proposed, reviewed and tested prior to implementation.**
- 7.7.1 Establish monitoring mechanisms to identify and capture proposed configuration changes, ensuring that all changes are documented and submitted through the designated change management process.
- 7.7.2 Require stakeholders to submit change requests detailing the proposed modifications, including the rationale, scope, and expected impact of the changes, for review and approval by the designated change management authority.

| | | | |
|-------------|-------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vishnu | [Signature] | [Signature] |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 24 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

- 7.7.3 Conduct thorough reviews and assessments of proposed configuration changes to evaluate their potential impact on critical services, systems, and infrastructure.
- 7.7.4 Prioritize changes based on their urgency and significance, and ensure that all changes undergo testing and validation procedures to verify their effectiveness and compatibility with existing configurations before implementation, mitigating risks and ensuring operational stability.
- 7.8. Use automated tools whenever possible to perform configuration changes.**
- 7.8.1 Identify and select appropriate automated tools capable of performing configuration changes efficiently and accurately, taking into account factors such as compatibility with existing systems, scalability, and ease of use.
- 7.8.2 Integrate selected automated tools into the organization's configuration management framework, ensuring seamless interoperability with other tools and systems involved in the change management process.
- 7.8.3 Configure automated tools to adhere to predefined change management policies and procedures, ensuring that changes are implemented consistently and in accordance with established standards and best practices, while minimizing the risk of errors or discrepancies.
- 7.9. Modelling and testing of configuration changes should be done in a test environment before committing to production environment.**
- 7.9.1 Develop a modelling process to simulate configuration changes in a controlled test environment before applying them to the production environment.
- 7.9.2 Utilize tools and techniques to create accurate representations of the proposed configuration changes, allowing stakeholders to visualize and evaluate the potential impact of the changes before implementation.
- 7.9.3 Conduct comprehensive testing of configuration changes in a dedicated test environment to assess their functionality, compatibility, and stability.
- 7.9.4 Execute test scenarios designed to validate the effectiveness of the proposed changes and identify any potential issues or conflicts that may arise during implementation, ensuring that changes are thoroughly vetted and validated before being deployed to the production environment.
- 7.10. Establish a plan for addressing Emergency Changes to Configurations.**
- 7.10.1 Establish a structured plan for addressing emergency changes to configurations, outlining the procedures and protocols to be followed in response to urgent situations requiring immediate modification.
- 7.10.2 Define criteria for identifying emergency changes, such as critical system failures, security breaches, or regulatory compliance issues, and establish escalation procedures for initiating emergency change processes.
- 7.10.3 Implement expedited processes for reviewing, approving, and implementing emergency changes to configurations, ensuring swift action and minimal disruption to critical services.
- 7.10.4 Designate authorized personnel or emergency response teams responsible for evaluating and approving emergency change requests, prioritizing rapid response and effective mitigation of risks or impacts associated with urgent configuration modifications.

| | | | |
|-------------|-------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | [Signature] | [Signature] |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 25 of 76 | Instruction No. TFIN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

8. Backup and Disaster Recovery (DR) Mechanism:

8.1. Disaster recovery policy and procedures should be formalized for all CIIs.

- 8.1.1 Zonal Railways shall develop a comprehensive disaster recovery policy that outlines the organization's approach to mitigating the impact of disasters on SCADA system.
- 8.1.2 Document the policy in detail, specifying objectives, scope, roles and responsibilities, regulatory requirements, and the overarching strategy for disaster recovery, ensuring clarity and alignment with organizational goals and objectives.
- 8.1.3 Establish detailed procedures for executing the disaster recovery policy, including step-by-step instructions for initiating, coordinating, and executing recovery activities in response to different types of disasters.
- 8.1.4 Define specific actions, timelines, and communication protocols for each phase of the disaster recovery process, such as assessment and planning, response and recovery, restoration of services and post-recovery evaluation, ensuring preparedness and efficiency in managing adverse events impacting SCADA systems.

8.2. Natural and environmental threats should be considered for DR site.

- 8.2.1 Conduct a comprehensive risk assessment to identify and evaluate natural and environmental threats that could potentially impact the disaster recovery (DR) site.
- 8.2.2 Assess the likelihood and potential impact of threats such as earthquakes, floods, hurricanes, wildfires, and other environmental hazards on the DR site infrastructure, systems, and operations.
- 8.2.3 Develop mitigation and preparedness measures to address identified natural and environmental threats and minimize their impact on the DR site.
- 8.2.4 Implement protective measures such as site selection criteria, structural reinforcements, environmental monitoring systems, emergency response plans, and contingency arrangements to safeguard the DR site infrastructure and ensure its resilience against adverse events.

8.3. Proper roles and responsibilities with resource allocation should be clearly defined for the work from disaster recovery site.

- 8.3.1 Define clear roles and responsibilities for personnel working from the disaster recovery (DR) site, outlining the specific tasks, duties, and authorities assigned to each role.
- 8.3.2 Identify key stakeholders, including DR site coordinators, technical support staff, communication liaisons, and other relevant personnel, and specify their roles in managing and executing recovery activities.
- 8.3.3 Allocate resources effectively to support operations at the DR site, including personnel, equipment, facilities, and technology infrastructure, based on predefined roles and responsibilities.

8.4. Basic amenities of water, electricity, transportation, internet connectivity etc. should also be checked before the selection of DR site.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | R.P.S. | Sumar |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 26 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

- 8.4.1 Conduct a thorough assessment of basic amenities including water supply, electricity availability, transportation accessibility, and internet connectivity at potential disaster recovery (DR) site locations.
- 8.4.2 Evaluate the reliability, capacity, and resilience of each amenity to meet the operational requirements and support uninterrupted business continuity during disaster recovery operations.
- 8.4.3 Prioritize sites with robust infrastructure and amenities, considering factors such as proximity to primary operations, redundancy of utilities, accessibility for personnel and equipment, and availability of alternate communication channels, to enhance the effectiveness and resilience of the DR strategy.

8.5. Periodic reviews and audit of the disaster recovery should be done.

- 8.5.1 Establish a schedule for conducting periodic reviews and audits of the Disaster recovery (DR) plan, specifying the frequency and scope of assessments.
- 8.5.2 The Periodic reviews and audit of the disaster recovery should be done by the competent authority, preferably CISO at the Zonal/Headquarter level.
- 8.5.3 Define the roles and responsibilities of personnel responsible for overseeing the review and audit process, including designated auditors or review teams tasked with evaluating the effectiveness and compliance of the DR plan.
- 8.5.4 Conduct scheduled reviews and audits of the DR plan according to the established plan, following standardized procedures and methodologies.
- 8.5.5 Evaluate key aspects of the DR plan, including documentation completeness, currency, alignment with business requirements, adequacy of recovery strategies, effectiveness of recovery procedures, and compliance with regulatory requirements.
- 8.5.6 Document review findings, identify areas for improvement or corrective actions, and develop remediation plans as needed to address deficiencies and enhance the resilience and effectiveness of the DR program.

8.5.7 Disaster Recovery Plan:

- 8.5.73. In case of natural, environmental disasters or Cyber Security related attacks, Emergency alert escalation and DRP (Disaster Recovery Plan) activation procedure shall be followed. Necessary communication to the CISO regarding the same shall be done.
- 8.5.74. For SCADA System, the provision should be made to set up the disaster recovery site or Backup Control Centre in another room (preferably another floor in the same headquarter building or it should be set up at AEE's Office/ Depot Site Engineer's office and should be decided by ZRs as per site's availability and convenience.
- 8.5.75. In case of disaster related emergency or Cyber related attacks, SCADA and TPC operations shall be carried out from Disaster Recovery Site/Backup Control Centre so as to mitigate the impact.
- 8.5.76. In case of such incidence or emergency, provision should be made to deploy sufficient manning staffs at TSS/SP and crucial/critical SSP to perform manual operation, if needed. The list of manning staff and their supervisors with their contact numbers shall be displayed in each Depot and field officer's office.
- 8.5.77. In the disaster recovery site/Backup Control Centre, minimally required provision of Servers (1 No. of Front end server, 1 No. of SCADA Server, 1 No. NMS Server),

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | 11/12/25 | 11/12/25 |
| Date | 11-02-2025 | | |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 27 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

Workstations (single machine with single monitor for every 15 RTUs), UPS (1 No.), Network Switches (2 Nos.), firewall (1 No.), communication channels and other accessories shall be done for efficient functioning of the Backup Control Centre. Further, backup of data shall be kept in Network Attached Storage in RAID 1 Configuration. Provision for SCADA availability should be made to cater TSS, SP and crucial SSPs at Disaster Recovery Site. RDSO Specification TI/SPC/RCC/SCADA/0134 or latest shall be referred in this regard.

- 8.5.78. The provision of SCADA Software with full configuration of TSS, SP, and SSP shall be made in the Disaster Recovery Site/Backup Control Centre. The governing RDSO Specification TI/SPC/RCC/SCADA/0134 or latest shall be followed in this regard.
- 8.5.79. Timely drill (preferably quarterly) shall be done to carry out the operation of TPC from Disaster Recovery Site to ascertain the smooth functionality and operation of the Backup Control Centre and provide maintenance, if needed.
- 8.5.710. The hardware and software provided in the Backup Control Centre shall be recorded in the inventory. Further, the timely operation from the Backup Control Centre shall be reported in Internal Audit Report.

8.6. Periodic trainings and mock drills of the employees for resuming the operations from the DR site should be done.

- 8.6.1 Develop a comprehensive training program for employees aimed at preparing them to resume operations from the disaster recovery (DR) site in the event of a disaster.
- 8.6.2 Define the objectives, content, and curriculum of the training program, including topics such as DR plan overview, roles and responsibilities, emergency procedures, communication protocols, and technical skills required for working from the DR site.
- 8.6.3 Conduct periodic mock drills to simulate disaster scenarios and practice the procedures for transitioning to and operating from the DR site.
- 8.6.4 Coordinate with relevant stakeholders to plan and execute mock drills, ensuring realistic scenarios, participation of key personnel, and adherence to predefined timelines and objectives.

8.7. For SCADA System, the provision should be made to set up the disaster recovery site or Backup Control Centre in another room (preferably another floor in the same headquarter building or it should be set up at AEE's Office/ Depot Site Engineer's office and should be decided by ZRs as per site's availability and convenience. (Clause no. 3.6 of the Railway Board Cybersecurity Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways, Version 1.0 or latest shall be followed for the same.)

8.8. Establish and implement a backup policy.

- 8.8.1 Develop a backup policy document outlining the organization's approach to data backup, retention, and recovery.
- 8.8.2 Define the scope, objectives, and requirements of the backup policy, including the types of data to be backed up, backup frequency, retention periods, storage locations, and recovery procedures.

| | | | |
|-------------|---------------|--------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Rishi</i> | <i>Sumit</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 28 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

8.8.3 Configure backup systems to automate the backup process, schedule regular backups based on predefined intervals, and ensure data integrity and security during backup and storage operations.

8.9. Keep the backup of your data and configurations and keep offline.

- 8.9.1 Regularly create backups of critical data and configurations, ensuring comprehensive coverage of all essential systems and information.
- 8.9.2 Store backup copies offline in secure and dedicated storage media or facilities, such as external hard drives, tape drives, or offline backup servers, to protect against data loss due to cyber threats, hardware failures, or disasters.
- 8.9.3 Implement strict access controls and security measures to safeguard offline backup storage, restricting unauthorized access and ensuring data confidentiality and integrity.
- 8.9.4 Regularly monitor and audit offline backup storage facilities to detect any anomalies or security breaches, and conduct periodic verification checks to ensure the integrity and usability of backup data when needed for recovery purposes.

8.10. To increase your chances of recovering lost or corrupted data, follow the 3-2-1 backup rule for CII assets:

3 – Keep 3 copies of any important file: 1 primary and 2 backups.

2 – Keep the files on 2 different media types to protect against different types of hazards.

1 – Store 1 copy offsite (e.g., offline at remote location)

- 8.10.1 Maintain three copies of important SCADA asset data, including one primary copy stored on the primary system and two additional backup copies stored on separate media.
- 8.10.2 Regularly create and update backup copies of critical data, ensuring redundancy and availability for recovery purposes in the event of data loss or corruption.
- 8.10.3 Store backup copies on at least two different types of media to mitigate the risk of data loss from various hazards, such as hardware failures, software errors, or physical damage.
- 8.10.4 Implement offsite storage for one backup copy, storing it at a remote location offline to protect against catastrophic events such as natural disasters, fires, or theft, ensuring geographic diversity and redundancy in backup storage locations.

8.11. Data at rest should be in encrypted form.

- 8.11.1 Develop a comprehensive encryption policy that mandates the encryption of data at rest to protect sensitive information from unauthorized access or disclosure.
- 8.11.2 Define the scope of the encryption policy, specifying the types of data that require encryption, encryption algorithms and protocols to be used, key management practices, and compliance requirements.
- 8.11.3 Implement encryption mechanisms and solutions to encrypt data stored on storage devices, databases, file systems, and other repositories according to the encryption policy.

| | | | |
|-------------|---------------|--------------|---------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Rishi</i> | <i>Juma</i> |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR TI-3 |

| | | |
|---------------|---|---|
| Page 29 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

8.12. The department shall maintain Backup register that contains complete records of the backup copies such as Site location, Device type, Name, Backup type, frequency, Backup location, date etc.

- 8.12.1 Develop a standardized backup register template that includes fields for recording essential information about backup copies, such as site location, device type, backup name, and backup type, frequency of backups, backup location, and backup dates.
- 8.12.2 Ensure completeness and accuracy of information recorded in the backup register, capturing details of all backup activities and configurations to facilitate tracking and management of backup copies effectively.
- 8.12.3 Designate responsible personnel or backup administrators to maintain the backup register, updating it regularly with new backup entries, modifications, or deletions as backup operations occur.

8.13. Periodic drills to ensure the restoration process should be undertaken.

- 8.13.1 Schedule and plan periodic restoration drills to test the effectiveness and readiness of the restoration process in the event of data loss or system failure.
- 8.13.2 Define the objectives, scope, and scenario for the restoration drill, specifying the systems, data sets, and recovery procedures to be tested, and identify key stakeholders and participants involved in the drill.
- 8.13.3 Execute the restoration drill according to the predefined plan and scenario, simulating a real-world disaster or data loss scenario to assess the organization's ability to restore critical systems and data.
- 8.13.4 Monitor and evaluate the performance of the restoration process, including the speed, accuracy, and completeness of data recovery, adherence to recovery time objectives (RTOs) and recovery point objectives (RPOs), and effectiveness of communication and coordination among involved teams.
- 8.13.5 Document observations, findings, and lessons learned from the restoration drill, identifying areas for improvement or refinement in the restoration process, and develop action plans to address identified deficiencies and enhance the organization's resilience and readiness for future recovery scenarios.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 12.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 30 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

9. Security Event / Log Management:

9.1. Establish and maintain log management policy that clearly defines mandatory requirements and recommendations for several aspects of log management.

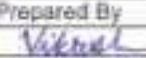
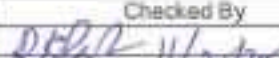
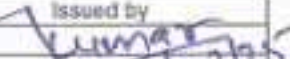
- 9.1.1 Zonal Railways shall develop a comprehensive log management policy document outlining mandatory requirements and recommendations for various aspects of log management, including log generation, collection, retention, monitoring, and analysis.
- 9.1.2 Define the scope, objectives, and key components of the log management policy, addressing factors such as types of logs to be collected, retention periods, access controls, log storage, monitoring frequency, and incident response procedures.
- 9.1.3 Establish mechanisms for monitoring and enforcing adherence to the log management policy, including regular audits, reviews, and assessments of log management practices, and take corrective actions as necessary to address non-compliance issues and improve overall effectiveness of log management processes.

9.2. Centralize log collection and retention for all ICT/OT assets should be implemented (e.g. syslog). Retain logs of all ICT/OT assets (in standard analysis formats) as per NCIIPC / CERT-In guidelines (minimum 06 months as of now).

- 9.2.1 Deploy a centralized log management system, such as syslog or a centralized logging server, to collect and aggregate logs.
- 9.2.2 Configure each SCADA asset to forward its logs to the centralized logging system using standard protocols and formats, ensuring consistent and uniform collection of log data from diverse sources.
- 9.2.3 Define log retention policies in alignment with NCIIPC/CERT-In guidelines, specifying the minimum retention period for log data (e.g., six months).
- 9.2.4 Ensure that all collected logs are retained for the specified duration in standard analysis formats, facilitating ease of analysis and investigation when required by regulatory authorities or incident response teams.

9.3. Real time monitoring and analysis of the logs should be done.

- 9.3.1 Deploy a real-time log monitoring system capable of continuously monitoring logs generated by SCADA assets.
- 9.3.2 Configure the monitoring system to ingest log data from centralized log sources, such as syslog servers or logging agents deployed on SCADA assets and enable real-time analysis and alerting functionalities.
- 9.3.3 Define monitoring criteria and thresholds based on security policies, regulatory requirements specifying parameters such as abnormal behaviour, security events, or performance anomalies to trigger alerts.
- 9.3.4 Establish procedures for analysing and responding to log events in real-time, including identifying security incidents, investigating anomalies, escalating critical alerts to incident response teams, and initiating remediation actions to mitigate risks or threats identified through log analysis.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 31 of 76 | Instruction No. TIIN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

9.4. Standardize time synchronization. Configure at least two synchronized time sources across organizations assets. Time synchronization must be done using Network Time Protocol Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL).

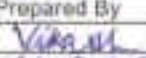
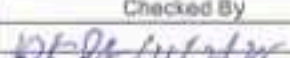
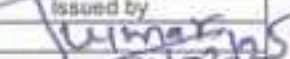
- 9.4.1 Configure at least two synchronized time sources, such as Network Time Protocol (NTP) servers, across all SCADA systems.
- 9.4.2 Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however, it is to be ensured that their time source shall not deviate from NPL or NIC (Para (i) of CERT-In directive issued vide No. 20(3)/2022-CERT-In dated 28.04.2022 may be referred for the same).
- 9.4.3 Implement mechanisms for automated time synchronization checks and alerts to promptly identify and address any deviations or failures in time synchronization, ensuring continuous alignment with the designated time sources and minimizing discrepancies in time across the SCADA systems.

9.5. Audit logs recording user activities, exceptions and information security events shall be produced and kept until the next audit is performed.

- 9.5.1 Configure systems and applications to generate audit logs recording user activities, exceptions, and information security events according to predefined criteria and security policies.
- 9.5.2 Implement a log retention policy specifying that audit logs shall be retained until the next audit is performed, ensuring that log data remains available for review and analysis during audit processes.
- 9.5.3 Conduct regular audits of audit logs to review recorded activities, exceptions, and security events, assessing compliance with security policies, detecting anomalies or suspicious activities, and identifying areas for improvement in information security practices.
- 9.5.4 Maintain audit logs in secure and tamper-evident storage, ensuring integrity and confidentiality of log data throughout the retention period and facilitating audit trail analysis and forensic investigations when necessary.

9.6. Audit logs should be reviewed to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

- 9.6.1 Establish a schedule for conducting regular reviews of audit logs to detect anomalies or abnormal events that may indicate potential security threats or breaches.
- 9.6.2 Conduct log reviews on a weekly basis or more frequently, depending on the organization's risk profile, regulatory requirements, and security policies, to ensure timely detection and response to security incidents.
- 9.6.3 Define criteria and thresholds for identifying anomalies or abnormal events in audit logs, such as unusual access patterns, unauthorized activities, or system errors, based on known security indicators and behavioural patterns.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 32 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

9.7. Logs of remote access to OEM / service provider must be analysed and retained as per NCIIPC / Cert-In guidelines.

- 9.7.1 Implement a logging mechanism to record all remote access activities to OEM/service provider systems, capturing relevant details such as user identities, timestamps, access attempts, and actions performed during remote sessions.
- 9.7.2 Ensure that logs of remote access activities are retained in accordance with NCIIPC/CERT-In guidelines, specifying the minimum retention period and storage requirements for remote access logs to facilitate analysis, audit, and investigation of security incidents or breaches.
- 9.7.3 Establish procedures for regular review and analysis of remote access logs to identify unauthorized or suspicious access attempts, unusual patterns of activity, or potential security threats.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | R.D. | J. Singh |
| Date | 12.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 33 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

10. Secure Remote Access:

10.1 Remote access by OEMs/Vendor/Third party entity etc. to database, application server and PCs related to OT systems, which are declared as 'Protected Systems' must be disabled.




- 10.1.1 Establish and enforce a strict access control policy framed by Zonal Railways that prohibits remote access by OEMs, vendors, third-party entities, etc., to SCADA servers and MMIs.
- 10.1.2 Configure access controls and security measures to prevent unauthorized remote access attempts, including firewall rules, network segmentation, and authentication mechanisms, to ensure the integrity and confidentiality of SCADA systems.
- 10.1.3 Implement continuous monitoring mechanisms to detect and prevent unauthorized attempts to access protected systems remotely, including regular review of access logs, intrusion detection systems, and security alerts.

10.2 Remote monitoring for all systems should be discouraged by exploring the possibility of setting the requisite facility locally. However, if requirement of allowing remote management is unavoidable, the same should be justified and approved by the competent authority along with necessary controls implemented for securing the access and accepting residual risk, if any.

- 10.2.1 Encourage the preference for local monitoring solutions over remote monitoring for all systems within the SCADA system.
- 10.2.2 Explore and evaluate the feasibility of setting up the necessary monitoring facilities locally to minimize reliance on remote monitoring solutions, ensuring better control and security of the monitoring process.

10.3 Security Level Agreement (SLA) should be done with the OEM/Vendor/Third party entity for remote access, which should include security measures to be put in place apart from the logging requirements and penalty clauses for non-compliance.

- 10.3.1 Develop a comprehensive Security Level Agreement (SLA) with the OEM, vendor, or third-party entity for remote access, outlining the security measures to be implemented to safeguard against potential risks and threats.
- 10.3.2 Include provisions in the SLA specifying the logging requirements for remote access activities, such as the types of logs to be generated, retention periods, and access control measures for log data, to ensure transparency and accountability in remote access management.
- 10.3.3 Define security measures and controls to be implemented by the remote access provider to secure the remote access infrastructure, including encryption protocols, authentication mechanisms, intrusion detection systems, and access controls, to protect against unauthorized access and data breaches.
- 10.3.4 Incorporate penalty clauses in the SLA for non-compliance with security requirements, specifying consequences and remediation actions for breaches of SLA terms, to incentivize

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11-02-2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 34 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

adherence to security standards and ensure accountability for maintaining the integrity and confidentiality of remote access systems and data.

10.4 The following protection strategy should be employed for remote access in control systems:

10.4.1 Organizational Information Security Policy should include both IT and OT (SCADA/ICS) security controls for remote access in conjunction with the management approved exceptions (if any).

- Remote connectivity procedures should be included in configuration and change management policy. Any configuration changes w.r.t. remote connection should result in a proper risk assessment process and suitable mitigation controls should be applied.
- The remote access must be with least possible time window and auto logoff features should be enabled.

10.4.1.1 Incorporate remote access security controls for both IT and OT, including SCADA system, within the organizational Information Security Policy which shall be framed by Zonal Railways.

10.4.1.2 Ensure that the policy outlines guidelines for remote access, including approved exceptions, and aligns with management-approved risk management processes to mitigate potential security risks associated with remote connectivity.

10.4.1.3 Integrate remote connectivity procedures into the organization's configuration and change management policy to ensure that any changes related to remote connections undergo a thorough risk assessment process.

10.4.1.4 The configuration changes pertaining to remote access are subjected to appropriate risk assessments, and suitable mitigation controls are implemented to address identified risks, thereby maintaining the security and integrity of control systems.

10.4.1.5 Implement stringent measures to restrict the time window for remote access, allowing access for the least possible duration necessary to perform required tasks.



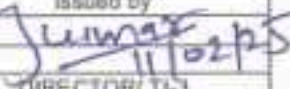
10.4.1.6 Enable auto-logoff features to automatically terminate remote sessions after a predetermined period of inactivity, reducing the risk of unauthorized access and ensuring that access privileges are revoked promptly when not in use.

10.4.2 Administrative/Privileged commands/access for remote access should be discouraged. If such access granted with due approval from competent authority for specific period, these should be monitored, controlled and recorded for required time frame so that there is full visibility of everything done during the period for which the remote access is given.

10.4.2.1 Discourage the use of administrative or privileged commands/access for remote access to systems, networks, or infrastructure components unless absolutely necessary.

10.4.2.2 Emphasize the principle of least privilege, limiting administrative access to only those individuals who require it to perform their job functions effectively and securely.

10.4.2.3 Obtain approval from the competent authority for any remote administrative or privileged access requests, ensuring that the need for such access is justified and documented.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11-02-2025 | | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR TI-3 |

| | | |
|---------------|---|---|
| Page 35 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

10.4.2.4 Retain logs of administrative access activities for the required time frame specified in organizational policies or regulatory requirements, enabling full visibility and accountability for all actions taken during the authorized remote access period.

10.4.3 Separate VPN connection for control system network access should be provided and they should be completely isolated from other networks.

10.4.3.1 Set up a dedicated Virtual Private Network (VPN) connection specifically for SCADA system network access, ensuring that it is distinct from other VPN connections used for general network access.

10.4.3.2 Configure the control system VPN connection to provide secure and encrypted communication channels for remote access to control system devices, applications, and data.

10.4.3.3 Configure firewall rules, access control lists (ACLs), and network policies to enforce strict isolation between the control system VPN network and other networks, preventing unauthorized access or communication between them.

10.4.4 Data in transit during remote access should be encrypted to ensure confidentiality and integrity.

10.4.4.1 Utilize industry-standard encryption protocols, such as TLS or Secure Shell (SSH), to encrypt data transmitted during remote access sessions.

10.4.4.2 Configure remote access systems, including VPN gateways, remote desktop services, and SSH servers, to enforce encryption for all data transmitted between the remote client and the target system.

10.4.4.3 Enable strong encryption algorithms and cryptographic techniques to safeguard the confidentiality and integrity of data transmitted over the network during remote access sessions.

10.4.4.4 Regularly review and update encryption configurations and protocols to address emerging security threats and vulnerabilities, ensuring continuous protection of data during remote access operations.

10.4.5 When not in use, remote connectivity ports should be disabled.

10.4.5.1 Implement a routine schedule for monitoring and managing remote connectivity ports to ensure that they are disabled when not in active use.

10.4.5.2 Conduct periodic audits or scans of network devices, routers, and firewalls to identify and disable any inactive or unused remote connectivity ports.

10.4.6 Un-trusted hosts should not be allowed to access the remote system.

10.4.6.1 Define access control policies that explicitly specify which hosts are considered trusted and allowed to access the remote system.

10.4.6.2 Implement firewall rules, network access control lists (ACLs), or access control mechanisms at the network perimeter to deny access attempts from untrusted hosts based on their IP addresses or network identifiers.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | Rishi | Juma |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 36 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

10.4.6.3 Segment the network infrastructure to create isolated zones or subnets for trusted hosts, separating them from untrusted or external networks.

10.4.6.4 Configure network devices, such as routers, switches, and firewalls, to enforce strict access controls and traffic filtering to prevent untrusted hosts from reaching the remote system or its associated services and resources.

10.4.7 Monitoring tools / applications should be used to monitor remote session activities and generate alerts in case of anomalies.

10.4.7.1 Deploy dedicated monitoring tools or applications capable of tracking and recording remote session activities in real-time.

10.4.7.2 Ensure that these monitoring tools are configured to capture relevant information such as user logins, session duration, commands executed, and file transfers during remote sessions.

10.4.7.3 Set up alert mechanisms within the monitoring system to promptly notify designated personnel or security teams in the event of detected anomalies, potential security breaches, or unauthorized activities during remote sessions.

10.4.8 Remote host should adhere to the security requirements of systems to which it can communicate.

10.4.8.1 Prior to establishing communication with remote systems, verify that the remote host meets the security requirements specified by the target systems.

10.4.8.2 Ensure that the remote host is configured to comply with security policies, access controls, authentication mechanisms, and encryption standards mandated by the target systems.

10.4.9 A complete inventory of remote access paths is to be maintained to ensure all entry points are protected.

10.4.9.1 Establish a centralized inventory system to document and track all remote access paths, including VPN connections, remote desktop services, SSH tunnels, and other remote access mechanisms.

10.4.9.2 Maintain detailed records for each remote access path, including its purpose, configuration details, associated users or accounts, and the systems or networks it provides access to.

10.4.9.3 Update the inventory promptly to reflect any changes or additions to remote access paths, such as new deployments, decommissioned connections, or modifications to existing configurations, ensuring that the inventory remains up-to-date for effective management and security monitoring.

10.4.10 Mechanism should be built to quickly revoke remote access in case of any incident.

10.4.10.1 Develop a predefined procedure and mechanism for swiftly revoking remote access privileges in the event of security incidents, policy violations, or other emergencies.

10.4.10.2 Ensure that the revocation process is well-documented, clearly defined, and easily accessible to authorized personnel responsible for managing remote access.

| | | | |
|-------------|-------------|-----------------|-------------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | R.P.S. 11/02/25 | J. Kumar 11/02/25 |
| Date | 11-02-2025 | | |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 37 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

10.4.10.3 Implement an immediate response protocol that enables authorized administrators or security personnel to initiate the revocation of remote access privileges without delay upon detection of a security incident or unauthorized activity.

10.4.10.4 Utilize centralized management tools or access control systems to expedite the revocation process, allowing administrators to remotely disable access accounts or terminate active sessions across all affected remote access paths promptly and efficiently.

10.4.11 Remote connection activity must be monitored and logs should be retained as per NCIIPC / Cert-In guidelines.

10.4.11.1 Deploy monitoring systems capable of tracking and recording remote connection activities in real-time, including logins, session duration, commands executed, and data transferred.

10.4.11.2 Ensure that monitoring tools are configured to capture relevant information according to guidelines provided by NCIIPC/CERT-In, including the retention period for log data.

10.4.11.3 Maintain logs of remote connection activity as per the specified guidelines from NCIIPC/CERT-In, ensuring compliance with data retention requirements.

| | | | |
|-------------|---------------|--------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Rishi</i> | <i>Sunil</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 38 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

11. Cyber Security Incident Management:

11.1. Even if an organization does not have resources to conduct incident response within an organization, there should be an Incident Response Plan. This would include the sources for protections and detections, a list of who to call upon for assistance and communication plans about how to convey information to leadership, employees, regulators and Govt. agencies.

11.1.1 Zonal Railways shall establish an Incident Response Plan (IRP) outlining procedures for responding to cybersecurity incidents, regardless of internal resource availability.

11.1.2 The IRP should detail sources for threat protections and detections, such as firewalls, intrusion detection systems (IDS), antivirus software, and security information and event management (SIEM) systems.

11.1.3 Define communication protocols for notifying relevant stakeholders, including internal leadership, employees, regulatory bodies, and government agencies, in the event of a cybersecurity incident.

11.1.4 Maintain a comprehensive list of contacts for external assistance, such as cybersecurity experts, law enforcement agencies, incident response teams, and legal counsel, ensuring clear channels of communication for requesting assistance and coordinating response efforts.

11.2. Designate personnel for incident management: one key person (preferably CISO) and at least one backup at the division level, who will manage the incident handling process. If using a third-party vendor for incident response, designate at least one person internal to the organization to oversee the third-party work.

11.2.1 Designate a primary Incident Manager, preferably the CISO, responsible for overseeing the incident handling process at the division level.

11.2.2 Additionally, designate at least one backup Incident Manager to ensure continuity of incident management responsibilities in the absence of the primary manager.

11.2.3 If leveraging third-party vendors for incident response services, assign at least one internal personnel to oversee and coordinate with the third-party team.

11.3. Maintain Contact Information for Reporting of cyber security incidents.

11.3.1 Create and maintain a centralized contact registry containing up-to-date information for reporting cybersecurity incidents.

11.3.2 Include contact details for internal stakeholders such as the CISO, Incident Response Team members, IT personnel, and department heads responsible for cybersecurity.

11.4. CII entities should be regularly in touch with respective CISOs of their Zone for keeping themselves updated on Cyber Security.

11.4.1 Define a communication protocol outlining the frequency and mode of interaction between CII entities and their respective CISOs within their Zone.

11.4.2 Determine the preferred channels for communication, such as email, phone calls, or virtual meetings, ensuring efficient and timely exchange of cybersecurity-related information.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | Rishi | J. Kumar |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|--|
| Page 39 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System. |
|---------------|---|--|

11.4.3 Establish regular intervals for updates and reporting between CII entities and Zone CISOs, facilitating the exchange of cybersecurity updates, threat intelligence, incident reports, and best practices.

11.5. Reporting and feedback Mechanism: Establish a process for reporting and feedback of cyber security incidents. Two-way exchange of information between organization having CII/PSs and Government agencies regarding possible cyber threat or post attack analysis is essential. Organization must always maintain strong communication channels with government agencies so as to get early information regarding emerging threats. This should include active participation of the organization in workshops, training or seminars conducted from time to time by government agencies.

11.5.1 Proper feedback mechanism between the CII organization and government agencies should be established.

- 11.5.1.1 Designate specific communication channels and points of contact within the CII organization for providing feedback to government agencies on cybersecurity matters.
- 11.5.1.2 Ensure that these channels are easily accessible and clearly communicated to relevant stakeholders, including designated government liaison officers.
- 11.5.1.3 Develop a structured process for providing feedback to government agencies, including timelines for response and escalation procedures.
- 11.5.1.4 Implement mechanisms for documenting and tracking feedback provided to government agencies, ensuring transparency and accountability in communication exchanges.

11.5.2 Any cyber security incident in CII should be reported to government agencies as per CERT-In guidelines.

- 11.5.2.1 Develop a formal process for reporting cyber security incidents within the SCADA systems, ensuring clear guidelines for incident classification, escalation, and notification procedures.
- 11.5.2.2 Define reporting channels, including designated contacts, email addresses or incident reporting platforms to facilitate efficient reporting of incidents by all stakeholders.
- 11.5.2.3 Familiarize all relevant personnel within the CII organization with the guidelines provided by CERT-In regarding the reporting of cybersecurity incidents.
- 11.5.2.4 Ensure strict adherence to the reporting timelines, formats, and protocols specified by CERT-In for different types of incidents.
- 11.5.2.5 Develop a standardized reporting process within the CII organization, clearly outlining the steps to be followed when a cybersecurity incident occurs.

11.5.3 CII should ensure the compliance of threat alerts sent by the government agencies.

- 11.5.3.1 Establish mechanisms to receive and promptly disseminate threat alerts issued by government agencies, such as CERT-In.

| | | | |
|-------------|-------------|-------------|---------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | R. B. Singh | J. M. Singh |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR TI-3 |

| | | |
|---------------|---|---|
| Page 40 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

11.5.3.2 Designate responsible personnel or teams within the CII organization to regularly monitor and review incoming threat alerts for relevance and potential impact on critical infrastructure.

11.5.4 Any advisories or feedback regarding the mock drills or penetration testing by the empaneled agencies should be communicated to the government.

11.5.4.1 Maintain comprehensive documentation of advisories and feedback received from mock drills and penetration testing conducted by empaneled agencies.

11.5.4.2 Ensure that all relevant information, including identified vulnerabilities, weaknesses, and recommendations for improvements, is accurately recorded and categorized for further action.

11.5.4.3 Establish a formal communication protocol for sharing advisories and feedback with relevant government agencies responsible for cybersecurity oversight.

11.5.5 Any major cyber security incident reported in the CII should be immediately notified to the government agencies through the feedback channel without any delay.

11.5.5.1 Define criteria and thresholds to classify cybersecurity incidents as major based on severity, impact, and potential risk to critical infrastructure and essential services.

11.5.5.2 Establish mechanisms for continuous monitoring and detection of cybersecurity incidents within the CII organization, enabling prompt identification of major incidents.

11.5.5.3 Upon identification of a major cybersecurity incident, initiate the notification process without delay.

11.5.6 Define communication mechanisms to communicate and report during a cyber-security incident. Mechanisms can include phone calls, emails or letters. Keep in mind that certain mechanisms, such as emails can be affected during a cyber-security incident.

11.5.6.1 Define and establish multiple communication mechanisms for reporting and communicating cybersecurity incidents, including but not limited to phone calls, emails, and letters.

11.5.6.2 Ensure redundancy in communication methods to mitigate the risk of disruption during a cybersecurity incident. For example, if email communication is affected, alternative methods like phone calls should be available.

11.5.6.3 Clearly outline the protocols and procedures for using each communication mechanism during a cybersecurity incident.

11.5.6.4 Specify the designated points of contact within the organization responsible for initiating and managing communication channels during different stages of the incident response process.

11.5.6.5 Regularly review and test the effectiveness of communication mechanisms to ensure they remain functional and reliable, even under adverse conditions such as network outages or compromised email systems.

11.6. Conduct periodic incident response exercises on latest threat scenarios.

| | | | |
|-------------|---------------|--------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Rohit</i> | <i>Sumit</i> |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 41 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 11.6.1 Schedule periodic incident response exercises to simulate various threat scenarios, ensuring coverage of the latest cybersecurity threats and attack vectors.
- 11.6.2 Actively participate in workshops, training sessions, and seminars conducted by government agencies to stay updated on emerging threats, best practices, and regulatory requirements, fostering collaboration and information sharing between the organization and government stakeholders.
- 11.6.3 Define the objectives, scope, and desired outcomes of the exercises, aligning them with organizational goals and priorities.
- 11.6.4 Identify the resources, including personnel, tools, and infrastructure, required to conduct the exercises effectively.
- 11.6.5 Simulate realistic cybersecurity incidents based on current threat intelligence and industry best practices, considering the organization's specific risk landscape.
- 11.6.6 Evaluate the performance of incident response teams and individuals involved in the exercises, identifying areas for improvement and corrective actions.
- 11.6.7 Document lessons learned and best practices from each exercise, incorporating feedback to enhance incident response capabilities and readiness for future incidents.
- 11.7. Certifications of ICS Infrastructure: - Security certifications deal with the validation of the security measures or controls taken for the ICS (Industrial Control Systems) infrastructure to protect the assets for smooth and error free operation. This validation is done by third party agencies which can be government or private empaneled agencies in consultation with RDSO/OEM. The certifications must also deal with enforcing or implementing any international security standards available globally for the protection of critical assets.**
- 11.7.1 Identify the ICS infrastructure components requiring certification based on their criticality and importance to operations.
- 11.7.2 Determine the applicable international security standards and regulatory requirements relevant to the ICS environment.
- 11.7.3 Establish contact with third-party certification agencies, whether governmental or private, approved by relevant authorities such as RDSO/OEM.
- 11.7.4 Prepare necessary documentation, including system architecture diagrams, security policies, procedures, and controls implemented within the ICS infrastructure.
- 11.7.5 Engage with the selected certification agency to initiate the assessment process, providing them with access to relevant ICS systems, documentation, and resources.
- 11.7.6 Facilitate on-site inspections and audits conducted by the certification agency to evaluate the effectiveness and compliance of security measures implemented within the ICS infrastructure.
- 11.7.7 Collaborate with the certification agency to address any identified vulnerabilities, gaps, or non-compliance issues, implementing remediation measures as necessary.
- 11.7.8 Review and validate the certification report provided by the agency, ensuring that all security requirements and standards have been adequately met.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vishakh | DEB | Jayant |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 42 of 76 | Instruction No. TITN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

11.7.9 Obtain the official certification or compliance documentation from the agency, demonstrating adherence to international security standards and regulatory guidelines for ICS infrastructure protection.

11.8. Legacy Systems: Systems in OT environment e.g. SCADA, CTC/TMS, requires specific skill sets which is different from typical IT skill sets. The systems have OEM specific Operating Systems, Protocols etc. and would run by the relevant control systems specialist rather than IT specialists. In this case, implementation of IT security controls on legacy systems has to be a well thought out process taking into consideration disruptions/downtime etc. Impact analysis of implications/ effects of placing IT security controls on legacy Control Systems should be done.

11.8.1 Conduct a thorough impact analysis to understand the implications of implementing IT security controls on legacy control systems.

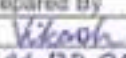
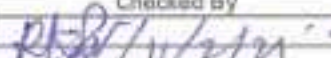
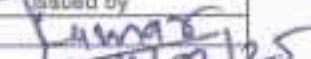
11.8.2 Identify and assess potential risks associated with disruptions, downtime, or compatibility issues resulting from the integration of IT security measures with legacy systems.

11.8.3 Develop a tailored implementation strategy that balances the need for IT security controls with the operational requirements and constraints of legacy systems.

11.8.4 Prioritize security controls based on risk assessment findings, focusing on measures that provide the most significant security improvements with minimal disruption to system functionality.

11.8.5 Conduct pilot testing or proof-of-concept deployments to validate the effectiveness and compatibility of selected security controls with legacy systems before full-scale implementation.

11.8.6 Monitor and evaluate the impact of implemented security controls on legacy systems, including performance, stability, and user experience, and adjust configurations as needed to optimize security posture while minimizing operational disruptions.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 21.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 43 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

12. Cyber Security Audit:

12.1. The cyber security audit policy should be established and reviewed periodically to validate effectiveness. Audit life cycle management should be implemented to get the most rigorous cyber security assessment.

- 12.1.1 Zonal Railways shall develop a comprehensive cyber security audit policy outlining the objectives, scope, frequency, and methodologies of audits.
- 12.1.2 Periodically review and update the audit policy to ensure alignment with evolving cyber threats, regulatory requirements, and organizational changes.
- 12.1.3 Implement an audit life cycle management process to ensure the effectiveness and rigor of cyber security assessments.
- 12.1.4 This includes planning and scoping audits, conducting audits using appropriate methodologies and tools, analysing findings, remediation of identified vulnerabilities, and reporting results to relevant stakeholders.

12.2. External audit should be conducted annually by CERT-In empanelled agencies. Empanelled agencies should be selected on Quality Cost Based Selection (QCBS) basis and not just L1 basis.

- 12.2.1 An external audit by CERT-In empanelled agencies (Article 14, Para (b) of the CEA Guidelines, 2021 or latest by Ministry of Power shall be referred in this regard) should be conducted annually to assess the organization's cybersecurity posture and compliance with relevant standards and regulations.
- 12.2.2 The audit schedule should be planned in advance to ensure timely completion and adherence to regulatory requirements.
- 12.2.3 Empanelled agencies should be selected through a process based on Quality Cost Based Selection (QCBS) criteria rather than just the Lowest Bid (L1) basis.
- 12.2.4 Criteria for selection should include factors such as technical expertise, experience in cybersecurity auditing, methodology, past performance, and cost-effectiveness, ensuring that the chosen agency can deliver high-quality audit services within budget constraints.

12.3. Cybersecurity audit shall be as per ISO/IEC 27001 along with sector specific standard. Scope of audit must be clearly defined by the CII.

- 12.3.1 All cybersecurity audits shall align with the ISO/IEC 27001 standard, which provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
- 12.3.2 In addition to ISO/IEC 27001, audits shall also incorporate sector-specific standards or regulations relevant to the Critical Information Infrastructure (CII) being audited, ensuring comprehensive coverage of sector-specific requirements.
- 12.3.3 The defined scope shall encompass all critical assets, systems, processes, and information assets within the CII, ensuring a thorough assessment of cybersecurity risks and controls specific to the organization's operations and objectives.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | RDSO | Jung |
| Date | 11-02-2025 | 11/2/25 | 11/2/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 44 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

12.4. Audit should check the compliance on ground and not be based on just submitted documents or assurance of the auditee.

- 12.4.1 Auditors should conduct thorough on-site inspections and observations to verify compliance with applicable standards, regulations, and internal policies.
- 12.4.2 Auditors should physically inspecting facilities, processes, and practices to ensure alignment with documented procedures and requirements.

12.5. VAPT should be done as part of the internal / external audit.

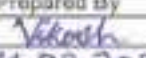
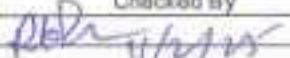
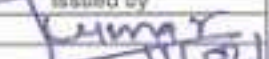
- 12.5.1 VAPT should be done as part of the external audit which is to be conducted annually by the CERT-In Empanelled agency.
- 12.5.2 Audit plans should include specific provisions for conducting VAPT exercises in conjunction with traditional audit activities to provide a comprehensive evaluation of cybersecurity controls.
- 12.5.3 Findings from VAPT exercises should be documented and reported alongside other audit observations, ensuring that security-related issues are appropriately addressed and remediated as part of the overall audit compliance process.

12.6. Internal audit should be conducted annually.

- 12.6.1 The internal audit department or designated personnel (Sr. DEE/TRD or Dy. CEE/TRD, TPC & RCC Engineer) shall establish an annual internal audit schedule outlining the timing and scope of audits to be conducted.
- 12.6.2 The internal Audit shall include compliance of this SOP (Instruction No. TI/IN/0052) and Cyber Security Guidelines for protection of CII of Indian Railways.
- 12.6.3 The planning of the internal audit shall involve identifying key areas and processes to be audited, considering risk assessments, regulatory requirements, and organizational priorities in case of Cyber attacks.
- 12.6.4 The key areas shall include Remote Control Centre (RCC), Backup Control Centre & TSS RTUs. Various processes such as Proper inventory management, patch management, periodic mock drills from backup Control Centre, trainings etc and other processes mentioned in this SOP, shall be included in Internal Audit Report.
- 12.6.5 Upon completion of audits, detailed audit reports, documenting findings, observations, and recommendations for improvement, shall be prepared and presented to Zonal Headquarter.

12.7. Establish a PT program and perform external penetration tests annually.

- 12.7.1 Perform external penetration tests as part of the External Audit which is to be conducted annually by CERT-In Empanelled Agency
- 12.7.2 Formulate a comprehensive plan outlining the objectives, scope, and frequency of penetration testing activities (annual).
- 12.7.3 Define the roles and responsibilities of individuals or teams responsible for managing and executing the PT program, ensuring clear accountability.
- 12.7.4 Ensure that the penetration tests cover external-facing systems, networks, applications, and infrastructure to identify potential vulnerabilities and security weaknesses.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued By |
| Signature |  |  |  |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 45 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

13. Security Operations:

13.1. The centralized SOC should be established for continuous monitoring and analysing cyber threats to CIIs. It must play an active role in protecting Critical Information Infrastructures in real time.

- 13.1.1 Develop a detailed plan for the establishment of the centralized Security Operations Centre (SOC), outlining the objectives, scope, and functions of the SOC.
- 13.1.2 Implement robust monitoring systems and tools within the SOC to continuously monitor critical information infrastructures (CIIs) for potential cyber threats.
- 13.1.3 Utilize advanced threat intelligence capabilities and analytics to analyse incoming data in real-time, enabling proactive identification, assessment, and response to cyber threats to CIIs.

13.2. Selection of SOC should be based on the risk assessment of the organization.

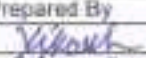

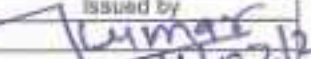
- 13.2.1 Determine selection criteria for the SOC based on the findings of the risk assessment, considering factors such as the organization's risk tolerance, criticality of assets, regulatory requirements, and budget constraints.

13.3. Dedicated trained team formed from employees with in the CII is strongly recommended to be deployed for operational and analysis activities of the SOC. Complete outsourcing is not recommended at all.

- 13.3.1 Identify skilled and experienced employees within the Critical Information Infrastructure (CII) organization to form a dedicated team for operational and analysis activities of the Security Operations Centre (SOC).
- 13.3.2 Provide specialized training and ongoing skill development programs to ensure that the team members are equipped with the necessary knowledge and expertise to effectively perform their roles within the SOC.
- 13.3.3 Maintain control and oversight over SOC operations by deploying an internal team, ensuring alignment with organizational goals, policies, and security requirements while mitigating potential risks associated with complete outsourcing.

13.4. All collected logs and artifacts should be stored carefully with timestamp and retained as per the period specified by NCIIPC / CERT-In.

- 13.4.1 Ensure all collected logs and artifacts are carefully stored in a secure and centralized repository.
- 13.4.2 Each log and artifact should be tagged with a timestamp indicating the date and time of collection to maintain chronological order and facilitate traceability.
- 13.4.3 Adherence to the retention periods specified by the National Critical Information Infrastructure Protection Centre (NCIIPC) or CERT-In for storing logs and artifacts.
- 13.4.4 Regularly review and update the storage infrastructure and procedures to ensure compliance with the specified retention periods and prevent inadvertent data loss or deletion.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 46 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

13.5. SOC should have the right combination of people, process and technology to carry out necessary analysis for early detection of anomalies / threats.

13.5.1 Ensure the SOC is staffed with a diverse team possessing the necessary skills and expertise in cybersecurity analysis, incident response, and threat intelligence.

13.5.2 Formulate clear roles and responsibilities for SOC personnel.

13.5.3 Deploy appropriate technologies, including SIEM (Security Information and Event Management) systems, threat intelligence platforms, and advanced analytics tools, to augment human capabilities and enhance the SOC's ability to detect and respond to anomalies and threats in real-time.

13.6. Clock synchronization of all the devices/assets of the CIIs need to be completed before operationalization of the SOC. Synchronize the time using Network Time Protocol Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL).

13.6.1 Prior to the operationalization of the Security Operations Centre (SOC), ensure that clock synchronization of all devices and assets within the Critical Information Infrastructures (CIIs) is completed.

13.6.2 Configure devices to synchronize their time with the designated NTP server, ensuring consistency and accuracy of timestamps for logs, events, and other time-sensitive data within the CII infrastructure.

13.6.3 Utilize the Network Time Protocol (NTP) server provided by National Informatics Centre (NIC) or the National Physical Laboratory (NPL) or any standard time source other than NPL or NIC for time synchronization across CII devices.

13.6.4 Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however, it is to be ensured that their time source shall not deviate from NPL or NIC (Para (i) of CERT-In directive issued vide No. 20(3)/2022-CERT-In dated 28.04.2022 may be referred for the same).

13.7. SOC should be capable of querying vast volumes of fast-changing data in real time across multiple vectors such as geography, network partitions and databases to facilitate quick analysis & detection.

13.7.1 Develop standardized procedures and protocols for querying data in real-time across various vectors within the SOC.

13.7.2 Implement distributed computing and storage architectures to efficiently process and query data across multiple vectors such as geography, network partitions, and databases.

13.7.3 SOC analysts to be trained on advanced querying techniques and tools to facilitate quick analysis and detection of anomalies or threats, leveraging the SOC's capabilities to effectively respond to security incidents in real-time.

13.8. SOC should allow collating the information from different sources in different formats to be captured, indexed, normalized, analysed and shared.

13.8.1 Implement a comprehensive data collection framework within the SOC to capture information from various sources, including logs, events, alerts, and threat intelligence feeds.

| | | | |
|-------------|-------------|--------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | RDSO-11/2/25 | J. Kumar |
| Date | 11-02-2025 | | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 47 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 13.8.2 Develop procedures for normalizing data collected from different sources, ensuring consistent formatting, and standardizing data structures to facilitate effective analysis.
- 13.8.3 Establish protocols and workflows for analysing collated information within the SOC, using advanced analytics tools and techniques to identify patterns, trends, and anomalies.
- 13.8.4 Implement mechanisms for sharing analysed information with relevant stakeholders, including incident responders, management, and external partners, to facilitate timely response and decision-making in response to emerging threats or security incidents.
- 13.9. SOC operations required to be automated so that analytics engines can ingest and work with highly diverse data types with minimal human intervention.**
- 13.9.1 Conduct a comprehensive assessment of SOC operations to identify tasks and processes suitable for automation, focusing on data ingestion, correlation, and analysis.
- 13.9.2 Prioritize automation initiatives based on their potential to improve operational efficiency, reduce response times, and enhance threat detection capabilities.
- 13.9.3 Deploy advanced analytics engines and machine learning algorithms within the SOC infrastructure to automate the ingestion and processing of highly diverse data types.
- 13.9.4 Configure analytics engines to intelligently ingest, correlate, and analyse data from various sources with minimal human intervention, enabling SOC analysts to focus on strategic decision-making and response efforts.
- 13.10. SOC should continuously examine high-value systems and information assets to identify threats based on behaviour, risk models along with threat signatures as per latest cyber kill chain methodologies.**
- 13.10.1 Define a list of high-value systems and information assets within the organization, considering factors such as criticality to operations, sensitivity of data, and potential impact of compromise.
- 13.10.2 Establish procedures for continuous examination of these high-value systems and assets within the SOC, utilizing a combination of behaviour analysis, risk modelling, and threat signatures to identify potential threats.
- 13.10.3 Implement cyber kill chain methodologies within the SOC framework to systematically analyse and respond to cyber threats.
- 13.11. Aggregate information from many trustworthy, relevant sources and present them in machine-readable forms that can be correlated with and analysed alongside internal data for pointing, highlighting and linking the possible IOC (Indicator of Compromise) across the networks in a CII with minimal human intervention.**
- 13.11.1 Establish protocols for aggregating information from a variety of trustworthy and relevant sources, including threat intelligence feeds, industry reports, and security advisories.
- 13.11.2 Implement automated mechanisms to collect and ingest this information in machine-readable formats, ensuring compatibility with internal data analysis tools and platforms.
- 13.11.3 Develop automated processes and workflows within the Security Operations Centre (SOC) to correlate external IOCs with internal data sources across the networks in a Critical Information Infrastructure (CII).

| | | | |
|-------------|----------------|-----------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vidhush</i> | <i>R. S. R.</i> | <i>J. Kumar</i> |
| Date | 11.02.2025 | 11/2/25 | 11/2/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 48 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

13.11.4 Utilize advanced analytics and machine learning algorithms to analyse correlated data and identify potential indicators of compromise, minimizing the need for manual intervention while enhancing the SOC's ability to detect and respond to cyber threats.

13.12. Effectiveness of SOC should be tested periodically through SOC maturity models and by simulating real world attacks by hiring ethical hackers.

13.12.1 Schedule regular assessments of SOC effectiveness using established SOC maturity models.

13.12.2 Conduct comprehensive evaluations of SOC capabilities, processes, and technologies to identify areas for improvement and measure progress towards maturity goals.

13.12.3 Collaborate with ethical hackers to simulate various attack scenarios, including advanced persistent threats (APTs), ransomware attacks, and insider threats, to validate SOC effectiveness and readiness to handle evolving cyber threats.

13.13. Threat models of SOC should be continuously refined and configured keeping in view the latest threat scenarios of the organisation.

Data Gathering Strategies – All logs pertaining to CII assets and their dependencies should be collected at central server (e.g. syslog) and analysed in the security operation centre (SOC) in real time. Retain logs of all these assets (in standard analysis formats) as per NCIIPC / CERT-In guidelines (minimum 06 months as of now).

13.13.1 Establish a process for continuously refining SOC threat models to stay aligned with the latest threat scenarios relevant to the organization.

13.13.2 Regularly review threat intelligence feeds, industry reports, and incident data to identify emerging threats and update threat models accordingly.

13.13.3 Configure SOC threat models based on the latest threat scenarios identified, ensuring alignment with the organization's risk profile and business objectives.

13.13.4 Implement automated mechanisms to adjust threat model configurations in real-time as new threat intelligence becomes available, enabling proactive detection and response to evolving cyber threats.

13.13.5 Establish a centralized log collection mechanism, such as syslog, to gather logs from all Critical Information Infrastructure (CII) assets and their dependencies.

13.13.6 Ensure that logs are transmitted securely to the Security Operations Centre (SOC) in real-time for analysis, enabling timely detection and response to security incidents.

13.13.7 Retain logs of all CII assets in standard analysis formats as per guidelines provided by the National Critical Information Infrastructure Protection Centre (NCIIPC) or CERT-In.

13.14. Cyber Threat Intelligence feeds from best available sources should be integrated in the SOC.

13.14.1 Identify and select cyber threat intelligence feeds from the best available sources, including reputable vendors, government agencies, industry consortiums, and open-source threat intelligence platforms.

13.14.2 Evaluate potential feeds based on factors such as relevance to the organization's industry sector, comprehensiveness, timeliness, accuracy, and reliability of threat information.

13.14.3 Develop procedures for integrating selected cyber threat intelligence feeds into the Security Operations Centre (SOC) infrastructure.

| | | | |
|-------------|---------------|-------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>R.R.</i> | <i>J. Kumar</i> |
| Date | 11.07.2025 | 11/7/25 | 11/07/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 49 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

14. Service Provider Management:

14.1. Establish and Maintain a Service Provider Management Policy. Review and update the policy annually or when significant changes occur that could impact the organization.

- 14.1.1 Zonal Railways shall frame a comprehensive Service Provider Management Policy outlining procedures for selecting, contracting, and managing third-party service providers.
- 14.1.2 Define criteria for assessing service provider capabilities, performance, security posture, and adherence to regulatory requirements and industry standards.
- 14.1.3 Conduct an annual review of the Service Provider Management Policy to ensure alignment with organizational objectives, changes in regulatory requirements, and emerging best practices.

14.2. Establish and maintain inventory of service providers. Review and update the inventory annually or when significant changes occur that could impact the organization.

- 14.2.1 Develop procedures for systematically identifying and documenting all service providers engaged by the organization, including vendors, contractors, and partners.
- 14.2.2 Create a centralized inventory database containing information such as provider name, contact details, services provided, contract terms, and criticality to business operations.
- 14.2.3 Conduct an annual review of the service provider inventory to ensure accuracy, completeness, and relevance.
- 14.2.4 Update the inventory whenever significant changes occur that could impact the organization, such as on boarding new service providers, terminating contracts, or changes in service offerings or terms of engagement.

14.3. Review service providers periodically and a risk rating associated with their potential impact to the business in case of an incident must be maintained. There should also be language in the contracts to hold them accountable if there is an incident that impacts the organization.

- 14.3.1 Establish a schedule for periodic review of service providers based on factors such as criticality to business operations, contractual obligations, and risk assessment.
- 14.3.2 Conduct comprehensive reviews of service providers, including assessments of their performance, security practices, compliance with contractual requirements, and potential impact on the organization in case of an incident.
- 14.3.3 Assign risk ratings to each service provider based on the potential impact they could have on the business in the event of an incident.
- 14.3.4 Include language in contracts with service providers to hold them accountable for any incidents that impact the organization, specifying terms for compensation, liability, breach notification, and incident response obligations.


14.4. Service provider contracts should include cyber security related SLAs. These includes minimum security program requirements, security incident or data breach notification

| | | | |
|-------------|-------------|-------------------|-------------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | R. K. S. 11/02/25 | J. Kumar 11/02/25 |
| Date | 11.02.2025 | | |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 50 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

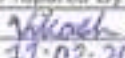
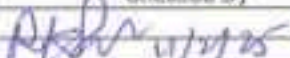
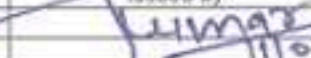
and response, signing of OSA / NDA, data encryption and data disposal. Review service provider contracts annually to ensure contracts are not missing security requirements.

- 14.4.1 Develop standardized cybersecurity-related Service Level Agreements (SLAs) to be included in contracts with service providers.
- 14.4.2 These SLAs should cover minimum security program requirements, protocols for security incident or data breach notification and response, signing of Operational Service Agreements (OSAs) or Non-Disclosure Agreements (NDAs), and provisions for data encryption and secure data disposal.
- 14.4.3 Establish a process for annually reviewing service provider contracts to ensure that cybersecurity-related SLAs are included and meet organizational security requirements.
- 14.5. Any breach in MSP & MSSP must be notified by them to CIIs.**
- 14.5.1 Develop a clear breach notification protocol outlining the procedures for Managed Service Providers (MSP) and Managed Security Service Providers (MSSP) to notify Critical Information Infrastructures (CIIs) in the event of a security breach.
- 14.5.2 Define specific timeframes and methods for reporting breaches, ensuring timely communication and collaboration between the service providers and CIIs.
- 14.6. Service dependent cyber security certification of these vendors be asked for before engagement.**
- 14.6.1 Prior to engaging with vendors, establish a requirement for service-dependent cybersecurity certification.
- 14.6.2 Develop a checklist or set of criteria outlining the specific cybersecurity certifications or standards that vendors must meet to qualify for engagement.
- 14.6.3 Verify the validity and authenticity of certifications through independent validation or verification processes before finalizing engagement with the vendors.
- 14.7. Liability be fixed if breach because of non-compliance of cyber security norms by the vendor.**
- 14.7.1 Incorporate a liability clause in contracts with vendors, specifying that they are liable for any breaches resulting from non-compliance with cybersecurity norms or requirements.
- 14.7.2 Clearly outline the extent of liability, including financial penalties or legal consequences, to be incurred by the vendor in the event of a breach caused by their non-compliance.
- 14.7.3 If a breach occurs due to vendor non-compliance, enforce the liability provision by holding the vendor accountable for damages incurred by the organization, including costs associated with breach remediation, data loss, and reputational damage.
- 14.8. Have penal provisions to enforce cyber security clauses of the SLAs.**
- 14.8.1 Ensure that Service Level Agreements (SLAs) include penal provisions specifically related to cybersecurity clauses.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 51 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 14.8.2 Define penalties or consequences for service providers in case of non-compliance with cybersecurity requirements, such as financial penalties, service credits, or termination of contract.
- 14.9. Securely decommission service providers on contract completion or termination. Decommission activities may include user and service account deactivation, termination of data flows, and secure disposal of organization's data within service provider systems.**
- 14.9.1 Develop a comprehensive plan outlining the steps and procedures for securely decommissioning service providers upon contract completion or termination.
- 14.9.2 Include activities such as deactivating user and service accounts associated with the service provider, terminating data flows between the organization and the service provider, and ensuring the secure disposal of the organization's data within the service provider's systems.
- 14.9.3 Execute the decommissioning plan in a systematic and controlled manner, following established procedures and protocols to minimize security risks and data exposure.
- 14.9.4 Coordinate closely with the service provider to ensure that all necessary decommissioning activities are completed satisfactorily and that any residual data or access rights are effectively removed or revoked to mitigate potential security threats.
- 14.10. Monitor service provider's consistency through periodic assessment of service provider compliance, monitoring service provider release notes and dark web monitoring.**
- 14.10.1 Establish a schedule for conducting periodic assessments of service provider compliance with contractual obligations and cybersecurity requirements.
- 14.10.2 Define assessment criteria and methodologies to evaluate the service provider's adherence to agreed-upon service levels, security protocols, and regulatory standards.
- 14.10.3 Utilize dark web monitoring tools or services to proactively identify any potential exposure of sensitive information or security threats related to the service provider's operations.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11-02-2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 52 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

15. Physical and Environmental Security:

15.1. Proper plan with clear policies of how to implement physical and environmental security should be devised.

- 15.1.1 Zonal Railways shall establish a comprehensive plan detailing the implementation of physical and environmental security measures within the organization.
- 15.1.2 Develop clear policies outlining the requirements, guidelines, and procedures for safeguarding physical assets, facilities, and the surrounding environment against unauthorized access, theft, vandalism, natural disasters, and other potential threats.
- 15.1.3 Implement the devised plan and policies by deploying appropriate security controls and countermeasures, such as access controls, surveillance systems, environmental monitoring, and emergency response protocols.

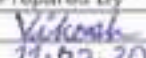

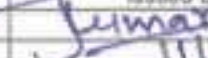
15.2. For human threats security, checks like CCTV cameras, swipe badges, access control policies, and secure work area should be in place.

- 15.2.1 Install CCTV cameras in strategic locations throughout the premises to monitor and record activities, providing surveillance coverage of critical areas and potential points of entry.
- 15.2.2 Implement swipe badge access systems and access control policies to restrict entry to authorized personnel only, ensuring that individuals without proper credentials are prevented from accessing sensitive areas.
- 15.2.3 Designate secure work areas within the organization's facilities where sensitive information, assets, or operations are located.
- 15.2.4 Implement additional security measures such as physical barriers, biometric authentication, or security personnel to further safeguard these areas against unauthorized access or intrusion attempts.

15.3. All equipment should be protected from power failures and other disruptions, including those caused by failures in supporting utilities, by using online UPS and generator.

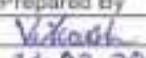

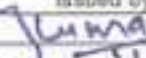
- 15.3.1 Install and maintain online UPS systems to provide continuous and clean power to critical equipment.
- 15.3.2 Ensure that UPS systems are properly sized and configured to support the load requirements of the equipment and are capable of seamlessly switching to battery power in the event of a power failure.
- 15.3.3 Install backup generators capable of providing emergency power during prolonged outages or disruptions in utility services.
- 15.3.4 Conduct regular testing and maintenance of UPS & generators to verify their operational readiness and reliability in supplying power to essential equipment during emergencies.

15.4. Proper security controls should be implemented for Data centre, signalling room, server room, SP, TSS, and SSP.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI/3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 53 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 15.4.1 Identify critical areas such as the data centre, signalling room, server room, Service Provider (SP) facilities, Telecommunications Service Supplier (TSS) sites, and Security Service Provider (SSP) locations.
- 15.4.2 Conduct risk assessments to determine the potential threats and vulnerabilities associated with each critical area.
- 15.4.3 Deploy appropriate security controls tailored to the specific requirements and risks of each critical area, including access controls, surveillance systems, intrusion detection systems, and environmental monitoring.
- 15.5. Periodic audits and mock drills by the employees for addressing the issue of physical threats is must to deal with the situation.**
- 15.5.1 Schedule regular audits of physical security measures to evaluate their effectiveness in mitigating potential threats.
- 15.5.2 Assign trained personnel or designated teams to conduct comprehensive assessments of security controls, including access controls, surveillance systems, and perimeter barriers, to identify vulnerabilities and areas for improvement.
- 15.5.3 Organize mock drills and exercises involving employees to simulate various physical threat scenarios, such as intrusions, thefts, or emergencies.
- 15.6. Biometric access, card swipes, CCTV footages log should be protected, stored, retained and destroyed as per the IS policy of the organisation.**
- 15.6.1 Establish secure storage mechanisms for biometric access records, card swipe data, and CCTV footage logs in accordance with the Information Security (IS) policy of the organization.
- 15.6.2 Implement encryption and access controls to protect the confidentiality and integrity of the stored data, ensuring that only authorized personnel have access to sensitive information.
- 15.6.3 Adhere to the retention periods specified in the IS policy for retaining biometric access records, card swipe data, and CCTV footage logs.
- 15.6.4 Develop procedures for the systematic and secure destruction of data once it reaches the end of its retention period, ensuring compliance with data protection regulations and minimizing the risk of unauthorized access or misuse.
- 15.7. All the devices/servers/systems storing access log information needs to be physically protected with proper backup policy for legal obligations.**
- 15.7.1 Ensure that all devices, servers, and systems storing access log information are physically protected in secure locations, such as access-controlled server rooms or data centres.
- 15.7.2 Implement measures such as locked cabinets, biometric access controls, and surveillance systems to prevent unauthorized physical access to these devices and mitigate the risk of tampering or theft.
- 15.7.3 Establish a comprehensive backup policy for access log information to fulfill legal obligations and ensure data integrity and availability.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|--|
| Page 54 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System. |
|---------------|---|--|

15.7.4 Regularly backup access logs to secure and reliable storage mediums, such as encrypted drives or cloud-based storage solutions, following predefined schedules and procedures to facilitate data recovery in the event of system failures, data loss, or legal requirements.

15.8. Only persons authorized by department shall be allowed to enter the CII facilities by showing valid identification with prior intimation/authorization of officer in charge.

15.8.1 Ensure that only individuals authorized by the department are permitted entry into Critical Information Infrastructure (CII) facilities.

15.8.2 Mandate that individuals seeking entry to CII facilities provide prior intimation or authorization from the officer in charge of the facility.

15.8.3 Establish clear procedures for obtaining authorization, including submitting requests through designated channels and obtaining approval from authorized personnel before accessing CII facilities.

15.9. The department must maintain visitor records at Control offices.

15.9.1 Implement a visitor record system at control offices to accurately document and track all individuals entering the premises.

15.9.2 Utilize electronic or manual record-keeping methods to capture visitor details, including name, affiliation, purpose of visit, date and time of entry and exit, and any accompanying personnel.

15.9.3 Designate responsible personnel for maintaining visitor records and ensuring their accuracy and completeness.

| | | | |
|-------------|---------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>R.D.</i> | <i>Sumit</i> |
| Date | 11-02-2025 | 11/2/25 | 11/2/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 55 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

16. Cyber Crisis Management:

16.1. Following should be formalized for cyber crisis readiness:

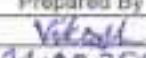


- Setting up of quarterly meetings of Information Security Steering Committee (ISSC).
- Promulgation and implementation of Information Security Policy.
- Comprehensive Risk Assessment and Risk Management.
- Allocation of adequate Budget and deployment of suitable Contingency Plan.
- Cyber crisis simulation exercises should be conducted on latest cyber threat scenarios.

- 16.1.1 Formally establish an Information Security Steering Committee (ISSC) responsible for overseeing cyber crisis readiness efforts.
- 16.1.2 Schedule quarterly meetings of the ISSC to review and assess the organization's cybersecurity posture, discuss emerging threats, and evaluate the effectiveness of cyber crisis preparedness measures.
- 16.1.3 Zonal Railways shall develop a comprehensive Information Security Policy outlining the organization's approach to cybersecurity and crisis management.
- 16.1.4 Ensure the policy is effectively communicated to all stakeholders and consistently implemented across the organization, with regular reviews and updates to reflect changes in technology, regulations, and threat landscape.

16.2. Ensure harmonious Institutional Response with following:

- Creation of full time CISO & his team.
- Constitution of Incident monitoring team.
- Constitution of Crisis Management Group.
- Identification of Critical Business Processes.
- Priority List among the Critical Business Processes.
- Identification of associated ICT Assets & KMP (Key Management Personal) dealing with ICT assets.

- 16.2.1 Establish a dedicated CISO position along with a competent team responsible for overseeing and implementing cybersecurity measures.
- 16.2.2 Define roles, responsibilities, and reporting structures within the CISO team to ensure effective coordination and execution of cybersecurity initiatives.
- 16.2.3 Formulate an Incident Monitoring Team tasked with proactively monitoring for security incidents, analysing threats, and coordinating incident response efforts.
- 16.2.4 Establish a Crisis Management Group comprising key stakeholders from various departments to provide strategic direction and decision-making during cybersecurity crises or emergencies, ensuring swift and coordinated response efforts.
- 16.2.5 Conduct a thorough assessment to identify critical business processes essential for the organization's operations and objectives.
- 16.2.6 Map associated ICT assets and key management personnel (KMP) responsible for managing these assets, ensuring clear accountability and ownership.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 56 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 16.2.7 Establish a priority list among the identified critical business processes based on their impact on organizational objectives, revenue generation, regulatory compliance, and stakeholder expectations.
- 16.3. Ensure following Internal Measures & Controls:**
- Compliance of ISO 27001 and sector specific standards.**
 - Latest NCIIPC Guidelines Compliance.**
 - Availability of a well-trained and experienced Forensics Team.**
 - Operational, properly configured and well-staffed Security Operations Centre (SOC) and Network Operation Centre (NOC).**
- 16.3.1 Establish procedures to ensure ongoing compliance with ISO 27001 and relevant sector-specific standards by conducting regular audits and assessments.
- 16.3.2 Implement corrective actions to address any identified non-conformities or deficiencies, ensuring alignment with best practices and regulatory requirements.
- 16.3.3 Stay updated with the latest guidelines issued by the National Critical Information Infrastructure Protection Centre (NCIIPC) and other relevant regulatory bodies.
- 16.3.4 Develop processes to review and implement necessary changes or enhancements to align with updated guidelines, ensuring continuous improvement in cybersecurity posture and resilience.
- 16.4. Communication: Maintain Continuous Communication with Govt. & LEAs regarding reporting of incidents and monitoring advisories / newsletters / threat reports.**
- 16.4.1 Set up dedicated communication channels for regular interaction with government agencies and Law Enforcement Agencies (LEAs) regarding incident reporting and monitoring advisories, newsletters, and threat reports.
- 16.4.2 Designate responsible personnel or a dedicated team to manage communication with government and LEAs, ensuring timely dissemination of information and coordination of response efforts.
- 16.4.3 Promptly report any security incidents, suspicious activities, or emerging threats to the appropriate government agencies and LEAs, following established reporting procedures and protocols to facilitate collaboration and response coordination.
- 16.5. Cyber Crisis Mitigation: Responses for attacks in case of crisis should include but not limited to the following:**
- Crisis Situations**
 - Symptoms/Indications**
 - Source of information**
 - Response Actions (Forensic, Customer Notification, Mitigation)**
 - Responsible Team and its contact information.**
 - Learning from the past crisis situations**
- 16.5.1 Develop a comprehensive response plan outlining specific actions to be taken in various cyber crisis situations, including but not limited to data breaches, malware outbreaks, or denial-of-service attacks.

| | | | |
|-------------|---------------|-------------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>R.P. Singh</i> | <i>Sumit</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 57 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

- 16.5.2 Define clear roles and responsibilities for each phase of the response process, detailing the actions to be taken by the responsible team members and their contact information.
- 16.5.3 Conduct post-incident reviews and analyses to identify lessons learned and areas for improvement following each crisis situation.
- 16.5.4 Use insights gained from past crises to enhance response strategies, update response plans, and improve overall cyber resilience, ensuring the organization is better prepared to mitigate future cyber threats effectively.
- 16.6. Testing of CCMP: It should be undertaken regularly by conducting mock drills on latest threat scenarios and the lessons learnt in these tests should be incorporated in the CCMP to achieve higher maturity and resilience.**
- 16.6.1 Schedule regular testing of the Cyber Crisis Management Plan (CCMP) by conducting mock drills simulating various threat scenarios, including the latest cyber threats and attack vectors.
- 16.6.2 Conduct thorough debriefings and post-exercise evaluations following each mock drill to identify lessons learned, areas for improvement, and best practices.
- 16.7. Post Crisis: Learning Cycle is critical to extract lessons based on previous disruptions. This should involve Root Cause Analysis (RCA) and forensics of the cyber security incidents to identify the weaknesses in the peoples, processes & technology which led to the incident (crisis) and find out what needs to be done to prevent recurrence. The learnings be implemented for improvement in the cyber security posture.**
- 16.7.1 Conduct thorough Root Cause Analysis (RCA) and forensic investigations of cyber security incidents to identify underlying weaknesses in people, processes, and technology that contributed to the crisis.
- 16.7.2 Utilize forensic techniques and tools to analyse digital evidence, identify attack vectors, and determine the extent of impact, helping to uncover vulnerabilities and gaps in existing security measures.
- 16.7.3 Compile findings from RCA and forensic investigations into actionable insights and recommendations for improving the organization's cyber security posture.
- 16.7.4 Implement corrective actions and remediation measures based on the identified weaknesses and lessons learned to prevent recurrence of similar incidents and enhance overall cyber resilience.
- 16.8. Other Triggers for Reviewing of Cyber Crisis Management Plan are:**
- a. Information Security Audit & Vulnerability/Threat/Risk (V/T/R) Analysis of Internal Team.**
- 16.8.1 Conduct periodic information security audits to assess the effectiveness of existing cybersecurity measures and controls.
- 16.8.2 Perform regular vulnerability, threat, and risk assessments to identify potential security threats and vulnerabilities within the organization's infrastructure, systems, and operations.

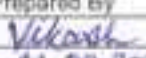

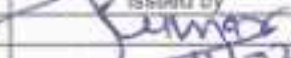
| | | | |
|-------------|-------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | [Signature] | [Signature] |
| Date | 11.07.2025 | 11/07/25 | 11/07/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 58 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

16.8.3 Initiate a review of the CCMP based on the findings of V/T/R analysis, particularly if new or heightened risks are identified that may require adjustments to response strategies, incident handling procedures, or risk mitigation measures.

16.9. Periodical VAPT assessment by the Third-Party Audit (CERT-In empanelled).

- 16.9.1 Establish a schedule (annually) for conducting periodic Vulnerability Assessment and Penetration Testing (VAPT) assessments by a Third-Party Audit firm certified by CERT-In.
- 16.9.2 Determine the frequency of assessments based on organizational risk tolerance, regulatory requirements.
- 16.9.3 Select a CERT-In empanelled Third-Party Audit firm with expertise in VAPT services and a proven track record of delivering thorough and effective assessments.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 21.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|--|
| Page 59 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System. |
|---------------|---|--|

17. Cybersecurity Awareness and Skill training

17.1. Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- 17.1.1 Develop a comprehensive training program focused on raising awareness and educating workforce members about various social engineering attacks, including phishing, pre-texting, and tailgating.
- 17.1.2 Design training modules that cover the tactics, techniques, and indicators of social engineering attacks, as well as best practices for identifying and mitigating such threats.
- 17.1.3 Conduct regular training sessions or workshops to provide workforce members with the knowledge and skills needed to recognize and respond effectively to social engineering attacks.
- 17.1.4 Utilize a variety of training methods, such as presentations, interactive exercises, simulated phishing campaigns, and scenario-based simulations, to engage participants and reinforce learning objectives.

17.2. Train workforce members on authentication as a best practice. Example topics include MFA, password composition and credential management.

- 17.2.1 Create a structured training curriculum that covers authentication best practices, including topics such as Multi-Factor Authentication (MFA), password composition, and credential management.
- 17.2.2 Design training materials that provide clear explanations of each concept, along with practical examples and demonstrations to illustrate their importance and application in securing digital assets.

17.3. Train workforce on how to identify and properly store, transfer, archive, destroy sensitive data. Clear screen and clear desk best practices including erasing of physical and virtual whiteboards at the end of meetings.

- 17.3.1 Develop a comprehensive training program focusing on educating the workforce on identifying, handling, storing, transferring, archiving, and securely disposing of sensitive data.
- 17.3.2 Create training materials that cover best practices for data handling, including guidelines for classifying data, encryption methods, secure file transfer protocols, and procedures for data archival and destruction.
- 17.3.3 Conduct regular training sessions or workshops to provide workforce members with the knowledge and skills necessary to effectively manage sensitive data.
- 17.3.4 Incorporate practical exercises and simulations into the training program to reinforce learning and allow employees to practice proper data handling techniques in realistic scenarios.
- 17.3.5 Emphasize the importance of clear screen and clear desk policies, including the erasure of physical and virtual whiteboards at the conclusion of meetings, as part of data security best practices.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | Rishi | Sumit |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 60 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

17.4. Train workforce to understand how to verify any failures in automated processes and tools.

- 17.4.1 Develop a comprehensive training curriculum that covers the principles and techniques for verifying failures in automated processes and tools.
- 17.4.2 Include topics such as understanding common failure modes in automated systems, interpreting error messages and alerts, troubleshooting techniques, and best practices for verifying the integrity and reliability of automated processes.
- 17.4.3 Provide guidance on documenting and reporting failures, including escalation procedures and communication protocols for notifying relevant stakeholders and seeking assistance when necessary.

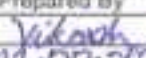
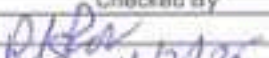
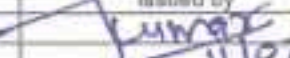
17.5. Train workforce members to be aware of causes for unintentional data exposure, e.g. mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

- 17.5.1 Create comprehensive training material focusing on raising awareness among workforce members about the causes of unintentional data exposure.
- 17.5.2 Include topics such as mis-delivery of sensitive data, loss of portable end-user devices, accidental publication of data to unintended audiences, and common scenarios leading to unintentional data exposure.
- 17.5.3 Provide practical guidance and best practices for preventing unintentional data exposure, including secure data handling practices, encryption techniques, proper device management, and verification procedures before sharing or publishing sensitive information.

17.6. Train workforce members to be able to recognize a potential incident and be able to report such an incident.

- 17.6.1 Develop a structured training program to educate workforce members on how to recognize potential incidents and effectively report them.
- 17.6.2 Design training materials that provide clear examples of common indicators of security incidents, including suspicious activities, anomalies in system behaviour, unusual network traffic, and unauthorized access attempts.
- 17.6.3 Conduct regular training sessions or workshops to train workforce members on incident recognition and reporting procedures.
- 17.6.4 Provide clear instructions and guidelines for reporting incidents, including designated reporting channels, contact information for incident response teams, and procedures for documenting incident details and observations.

17.7. Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 21.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TF3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 61 of 76 | Instruction No. TIIN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

- 17.7.1 Develop comprehensive training materials to educate workforce members on the dangers associated with connecting to and transmitting data over insecure networks for enterprise activities.
- 17.7.2 Cover topics such as the risks of using public Wi-Fi networks, unsecured hotspots, or untrusted networks, potential threats such as man-in-the-middle attacks or eavesdropping, and the importance of encrypting data transmissions.
- 17.7.3 Provide practical guidance on how to identify secure networks, use Virtual Private Networks (VPNs) for secure remote access, enable encryption for data transmissions, and adhere to company policies and procedures for network security.
- 17.8. Conduct role-specific security awareness and skills training, including secure system administration courses for IT professionals and courses for top management to keep them updated on latest technologies and threat landscape.**
- 17.8.1 Develop role-specific security awareness and skills training programs tailored to the needs of different groups within the organization, including IT professionals and top management.
- 17.8.2 Design training materials and courses that cover relevant topics such as secure system administration practices, cybersecurity fundamentals, emerging technologies, and the evolving threat landscape.
- 17.8.3 Conduct regular training sessions or workshops targeting specific roles within the organization, ensuring that each group receives training relevant to their responsibilities and level of expertise.
- 17.8.4 Monitor participation and track progress to ensure that all relevant personnel receive the necessary training and stay updated on the latest technologies and cybersecurity developments.
- 17.9. The background verification needs to be undertaken by the Railways for all personnel employed in CII domain. This may include all vendors, consultants and O&M firms and service providers appointed by the department.**
- 17.9.1 Develop a standardized background verification process to be implemented by the Railways for all personnel employed in Critical Information Infrastructure (CII) domain, including vendors, consultants, O&M firms, and service providers.
- 17.9.2 Define clear criteria and requirements for background checks, such as verifying employment history, educational qualifications, criminal records, and references, to ensure the integrity and reliability of individuals working in sensitive roles within the CII domain.
- 17.9.3 Make sure that all vendors, consultants, O&M firms, and service providers appointed by the department to undergo background verification as per the established process before engaging in CII-related activities.
- 17.10. Train workforce member for compliance process on termination / transfer / superannuation. A termination/transfer/superannuation process shall include return of all**

| | | | |
|-------------|-------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vishakh | P. K. G. V. | Suma S. |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 62 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

issued assets that are the property of the department. User ID, credentials and access rights shall be revoked/ deactivated at the end of the last working day.

- 17.10.1 Develop a comprehensive training program to educate workforce members on the compliance process for termination, transfer, or superannuation.
- 17.10.2 Cover topics such as the return of department-issued assets, revocation or deactivation of user IDs, credentials, and access rights, and the importance of adhering to established procedures and timelines.
- 17.10.3 Conduct regular training sessions or workshops to train workforce members on the compliance process for termination, transfer, or superannuation.
- 17.10.4 Emphasize the importance of timely revocation or deactivation of user IDs, credentials, and access rights at the end of the last working day, and provide clear instructions on the steps to be followed to ensure compliance with departmental policies and procedures.

17.11. Periodic assessment of skill level should be done through regular periodic assessments and accordingly formulate / improve the training & awareness programs for different level of employees.

- 17.11.1 Develop a standardized framework for conducting periodic assessments of skill levels among employees at different levels within the organization.
- 17.11.2 Define clear assessment criteria, objectives, and performance indicators aligned with organizational goals, job roles, and competency requirements.
- 17.11.3 Conduct regular periodic assessments of employee skill levels using the established framework to identify areas of strengths and weaknesses.
- 17.11.4 Based on assessment results, formulate or improve training and awareness programs tailored to the specific needs of different levels of employees, ensuring targeted skill development and continuous improvement.

| | | | |
|-------------|-------------|------------|---------------|
| | Prepared By | Checked By | Issued by |
| Signature | | | |
| Date | 12.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR TI-3 |

| | | |
|---------------|--|---|
| Page 63 of 76 | Instruction No. TI/N/0052 (Version 1.0) | Technical instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

CATEGORY: ASSET IDENTIFICATION/ INVENTORY**ANNEXURE-1****FORMAT FOR HARDWARE INVENTORY MANAGEMENT**

| S.No. | Item | Make/ Vendor information | Model No. | Serial No. | Software version installed | IP Address configuration details (if any) | AMC Partner Details | Location of Asset | Installation Date | License/ Subscription information (with expiry date) | End of life information |
|-------|-----------------------------|--------------------------------|--------------|---------------|----------------------------------|--|---------------------------|----------------------|----------------------|--|----------------------------|
| 1. | Workstation/ PCs | | | | | | | | | | |
| 2. | Servers | | | | | | | | | | |
| 3. | RTU | | | | | | | | | | |
| 4. | Laptop | | | | | | | | | | |
| 5. | Printer | | | | | | | | | | |
| 6. | Display Wall | | | | | | | | | | |
| 7. | Network Switches | | | | | | | | | | |
| 8. | Routers | | | | | | | | | | |
| 9. | Firewall | | | | | | | | | | |
| 10. | Storage devices (NAS) | | | | | | | | | | |
| 11. | Battery | | | | | | | | | | |
| 12. | UPS | | | | | | | | | | |
| 13. | Other devices | | | | | | | | | | |

| | | | |
|-------------|-----------------------|-----------------|----------------|
| Signature | Prepared By | Checked By | Issued by |
| Date | Vishakh 19-02-2025 | Rishabh 11/4/25 | Jumafoz |
| Designation | JIE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 64 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 2**FORMAT FOR SOFTWARE INVENTORY MANAGEMENT**

| S.N. | Software Name | Item | Make/ Vendor information | Model No. | Serial No. | Software version installed | Device in which software is installed | Location of Asset | Installation Date/ Deployment date | License/ Subscription information (with expiry date) | End of life information /Decommis sion date (if any) |
|------|--|------|--------------------------------|--------------|---------------|----------------------------------|--|----------------------|---|--|--|
| 1. | Software Name | | | | | | | | | | |
| 2. | URL name, app store(s), version(s) | | | | | | | | | | |
| | | | | | | | | | | | |

NOTE: The information maintained on the above lists can be expanded to whatever level is most useful to the organization (Indian Railways).
The field which does not apply may be scored out.

| | | | |
|-------------|----------------------|------------|----------------|
| Signature | Prepared By | Checked By | Issued by |
| Date | Vatsoh 11.09.2025 | 11.09.2025 | 11.09.2025 |
| Designation | Jr/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|--|---|
| Page 65 of 76 | Instruction No. TEIN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|--|---|

ANNEXURE- 3**EQUIPMENT ASSETS**

| S.N. | No. assigned | Description/ requirement | Qty. | Manufacturer serial no./ model | Inventory No. | Building ID | Room or area |
|------|--------------|--------------------------|------|--------------------------------|---------------|-------------|--------------|
| 1. | EQ-001 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of all vital equipment and/or systems, to the server or major component level. This list itself should be treated as an essential document and reviewed and updated quarterly or whenever major equipment is added or removed. The Zonal Railways must make determination in regard to what types of equipment are considered as sufficiently important to be placed on this list and to what level of granularity the equipment should be identified. Equipment whose loss or failure will affect the ability of the Indian Railways to meet its operational requirements, or which will potentially endanger personnel or facilities by its loss, should be included on this list. A major reason for having and maintaining this list is to ensure that equipment on the list is appropriately considered when making decisions about necessary operational spare parts, service contracts, maintenance planning, and system redundancy. The information maintained on this list can be expanded to whatever level is most useful to the organization. Contacts and telephone numbers for service and support, storage location of replacement components, and other such information can be added to this list if such data are not already maintained in other databases. Linkages to other such databases can be added to this list as well. The field which does not apply may be scored out.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | Rishi | Juma |
| Date | 11-02-2025 | 11/2/25 | 11/5/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 66 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 4**COMMUNICATION ASSETS**

| S.N. | No. assigned | Description/ usage | Qty. | Vendor and reference ID | Type function | Building ID | Room or area |
|------|--------------|-----------------------|------|----------------------------------|------------------|----------------|-----------------|
| 1. | COM-001 | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of all vital communication equipment such as routers, LAN switches, firewalls, modems, converters etc. This is the electronic equipment necessary for the communication links between the SCADA system and the field devices, other systems, and external and internal networks. This list should be treated as an essential document and reviewed and updated quarterly or whenever major equipment is added or removed. The Zonal Railways must make a determination in regard to what level of granularity the equipment should be identified. Equipment whose loss or failure will affect the ability of the organization to meet its operational requirements, or which will potentially endanger personnel or facilities by its loss, should be included on this list. A major reason for having and maintaining this list is to ensure that equipment on the list is appropriately considered when making decisions about necessary operational spare parts, service contracts, maintenance planning, and system redundancy. The information maintained in this list can be expanded to whatever level is most useful to the Indian Railways. Contacts and telephone numbers for service and support, storage location of replacement components, and other such information can be added to this list if such data are not already maintained in other databases. Linkages to other such databases can be added to this list as well. It may be useful to include cross-references to the respective communication circuit (listed subsequently as "Electronic Access Points"). The field which does not apply may be scored out.

| | | | |
|-------------|---------------|--------------------|--------------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>R. K. Singh</i> | <i>K. S. Singh</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 67 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 5**INFORMATION ASSETS**

| S.N. | No. assigned | Description/ Title | Qty. | Responsible manager and title | Media | Building ID | Room or area |
|------|--------------|--------------------|------|-------------------------------|-------|-------------|--------------|
| 1. | INF-001 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of all vital information and documentation, regardless of its medium. This is the information necessary for the support, operation, and maintenance of the SCADA system and related critical subsystems. This list itself should be treated as an essential document and reviewed and updated annually or whenever changes are made that affect this list. Information that would normally be on this list would include user's guides, operating and maintenance instructions, configuration settings, system databases, backup copies of all system software, and so forth. Any information, data, file, or document that would be needed to restore the system (or a critical subsystem) after a failure should be included on this list. Any such items necessary for the execution of a procedure (see the previous list entitled "Documented Procedures") should be included on this list. If materials are in secure storage or require additional levels of authority for access, this information should be added to the list. The purpose of this list is to identify and locate all critical information assets, so that they can be located when needed and so that suitable precautions can be taken for their storage and preservation. Any critical information that is normally maintained in a file or database table on a computer ought to have a corresponding documented procedure for its periodic backup and storage. The field which does not apply may be scored out.

| | | | |
|-------------|---------------|-------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>RDSO</i> | <i>Sumit</i> |
| Date | 11-02-2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 68 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

CATEGORY: PERSONNEL MANAGEMENT**ANNEXURE- 6****AREA ACCESS RIGHTS**

| S.N. | Employee name | Department | Supervisor | SCADA Room | Server Room | Control Room | Telecom Room |
|------|---------------|------------|------------|------------|-------------|--------------|--------------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of employees who have been granted access rights to sensitive areas, and review this list regularly (on a biannual basis) and whenever an employee is added or job responsibilities are changed. Use different indicators to differentiate personal access rights and the right to bring others, who do not have access rights, into each area. The list of secured areas will be specific to Indian Railways and may encompass multiple facilities. This list should be customized to match the specific requirements of different Zonal Railways. The field which does not apply may be scored out.

| | | | |
|-------------|-------------|------------|----------------|
| | Prepared By | Checked By | Issued by |
| Signature | Vikash | 11/02/25 | 11/02/25 |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/TI | ADE/TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 69 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 7**ELECTRONIC ACCESS RIGHTS**

| S.N. | Employee ID | Employee name and account IDs per System | Department | Supervisor | Office PC | Remote telecom | IT Servers | E-mail/ Web Server | SCADA System |
|------|-------------|--|------------|------------|-----------|----------------|------------|--------------------|--------------|
| 1. | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Instruction: Create and maintain an accurate list of employees who have been granted access rights to both business and operational computer systems, and review this list regularly (on a biannual basis) and whenever an employee is added or terminated or job responsibilities are changed. All user IDs granted to an employee (or contractor) should be listed, including those for company-provided PCs. The account designation should indicate the authorization level for the account, if multiple levels are defined. This list should be customized to match the specific requirements of Indian Railways. If electronic credentials, such as ID cards and password tokens, are issued to employees, these should be noted on this list, and sufficient information should be provided to support the revocation procedure for those items. If temporary access rights are granted to contractors, the list ought to include a place to record the date when those rights are to be revoked. The field which does not apply may be scored out.

| | | | |
|-------------|---------------|--------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>Rishi</i> | <i>J. Kumar</i> |
| Date | 11.02.2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 70 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 8**SECURITY TRAINING & BACKGROUND CHECKS**

| | | | | | Basic security | Cybersecurity | |
|------|-------------|---------------|------------|------------|-----------------------|-----------------------|-------------------------------|
| S.N. | Employee ID | Employee name | Department | Supervisor | Date of last training | Date of last training | Date of last background check |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of employees who have received training in cybersecurity, basic security, and social engineering techniques, and review this list regularly (on an annual basis) and whenever an employee is added or job responsibilities are changed. Additional security training may be required for selected job positions and when new threats are identified that require training augmentation. Also, track the performance and review of employment background checks (and rechecks) to ensure that personnel in critical positions maintain proof of suitability and trustworthiness. This list should be restructured to address the specific needs of the individual Zonal Railways. The field which does not apply may be scored out.



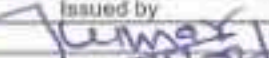
| | | | |
|-------------|---------------|------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vikash</i> | <i>AK</i> | <i>J. Kumar</i> |
| Date | 11/02/2025 | 11/21/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 71 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

CATEGORY: COMPUTER VIRUS SCAN/ CONFIGURATION CHECK**ANNEXURE- 9****SERVERS & PCs REQUIRING PERIODIC SCANNING**

| S.N. | No. assigned | User/ responsible employee name | Equipment identification (Inventory no.) | IP address or host ID | Building ID | Room or area | Port or circuit | Date of last virus scan and update |
|------|--------------|---------------------------------|--|-----------------------|-------------|--------------|-----------------|------------------------------------|
| 1. | VIR-001 | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Instruction: Create and maintain an accurate list of the various PCs and servers that are part of the SCADA system or that share a LAN connection (even through a firewall) with the SCADA system, for the purpose of scheduling and verification of completion of periodic virus scanning and configuration checks on those computers. It is important to verify that all such computers have suitable virus-scanning software and that it is enabled for the specified checks. It is also important to verify that specified configuration settings (including digital certificates, disabling of Wi-Fi or Bluetooth, etc.) are properly established. In many organizations, the ability to have automatic virus-scanning updates (on computers within the electronic security perimeter) will not be possible, owing to firewall settings; therefore, someone will need to be responsible for periodically updating the virus profiles of these computers. If VPN technologies are used for remote access, it will be necessary to ensure periodic updating of digital certificates. The purpose of this list is to aid in organizing and scheduling these activities and in making sure that all relevant computers are identified. This list should be reviewed quarterly, whenever new equipment is added or existing equipment is removed, or whenever software upgrades (e.g., updating the operating system version) are installed. The field which does not apply may be scored out.

| | | | |
|-------------|---|---|---|
| | Prepared By | Checked By | Issued by |
| Signature |  |  |  |
| Date | 13.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 72 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

CATEGORY: ELECTRONIC ACCESS POINTS**ANNEXURE- 10****LOCAL AREA NETWORK CONNECTIONS**

| S.N. | No. assigned | VLAN segment description / usage | Protective measures implemented | LAN equipment ID | Building ID | Room or area | Port or circuit |
|------|--------------|----------------------------------|---------------------------------|------------------|-------------|--------------|-----------------|
| 1. | LAN-001 | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of actual communication connections (LAN) between the SCADA system and any other systems or equipment outside the defined electronic perimeter. This could include a LAN connection to the Engineering Department or to a GIS system or other such connections. If desired, this list can also be used to document the LAN connections of the actual SCADA equipment to the SCADA LAN, if no other document already exists for that purpose. The purpose of this list is primarily to document LAN-based electronic access points through which an external attacker could attempt to gain access to the SCADA system. The actual connection points (in the form of switch equipment, hubs, and ports used) should be defined to the level necessary to enable an authorized person to physically disconnect (or reconnect) and isolate the SCADA LAN from external systems. This information will also be useful in the configuration of a NIDS (Network Intrusion Detection System) that monitors for unexpected traffic on the SCADA LAN and for ensuring proper configuration of Ethernet switches. Another key component of this list is the documentation of protective measures (or verification of the existence of suitable protective measures) being applied to secure this access point. The structure and content of this list should be modified, as needed, to incorporate sufficient information to permit management review of the protective measures in place. This does not have to include the details concerning the programming of rules in a firewall, but it should indicate that such provisions are in place, identify the document where those details are recorded, and document that the provisions are reviewed on a regular basis. With firewalls, there is a need for regular updating of virus profiles, and some mechanism needs to be in place to ensure that such updates are being made; that need not be part of this list, but this list should indicate the person responsible. This list should be reviewed on a biannual basis or whenever the equipment or network configuration of the SCADA system is modified. This list should be considered as a critical information asset and handled with the requisite security and confidentiality. The field which does not apply may be scored out.

| | | | |
|-------------|--------------------|--------------------|--------------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>V. K. Singh</i> | <i>R. K. Singh</i> | <i>J. K. Singh</i> |
| Date | 11-02-2025 | 11/2/25 | 11/2/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 73 of 76 | Instruction No. TIVIN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 11**WIRELESS ACCESS POINTS**

| S.N. | No. assigned | WLAN segment description / usage | Protective measures implemented | AP equipment ID | Building ID | Room or area | SSID |
|------|--------------|----------------------------------|---------------------------------|-----------------|-------------|--------------|------|
| 1. | WAP-001 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of any Wi-Fi access points (APs) implemented on the SCADA LAN. The purpose of this list is primarily to document wireless electronic APs through which an external attacker could attempt to gain access to the SCADA system. The actual AP information should be defined to the level necessary to enable an authorized person to physically disconnect (or reconnect) and isolate the SCADA LAN from wireless access. This information will also be useful in the configuration of a NIDS (Network Intrusion Detection System) that monitors for unexpected traffic on the SCADA LAN. Another key component of this list is the documentation of the protective measures (or verification of the existence of suitable protective measures) being applied to secure this AP. The structure and content of this list should be modified, as needed, to incorporate sufficient information to permit management review of the protective measures in place. This does not have to include the details concerning the disabling of beacons, enabling of WEP (Wired Equivalent Privacy), and so on, but it should indicate that such provisions are in place, identify the document where those details are recorded, and document that the provisions are reviewed on a regular basis. This list should indicate the person responsible for maintaining the security configuration of the Aps (Access Points). This same list can also be used to track any PCs that are constantly or periodically connected to the SCADA LAN and that have integral Wi-Fi and/or Bluetooth capabilities. The user(s) of these computer(s) should be identified, and there should be a record indicating that suitable configuration settings have been implemented on these PCs. This list should be reviewed on a biannual basis or whenever the equipment or network configuration of the SCADA system is modified. This list should be considered as a critical information asset and handled with the requisite security and confidentiality. The field which does not apply may be scored out.

| | | | |
|-------------|------------------------------|---------------------------------|---------------------------|
| Signature | Prepared By <i>Vikash</i> | Checked By <i>R.B. Singh</i> | Issued by <i>Singh</i> |
| Date | 11.02.2025 | 11/2/25 | 11/5/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 74 of 76 | Instruction No. TUN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 12**WIDE AREA NETWORK CONNECTIONS**

| S.N. | No. assigned | WAN description / purpose | Router serial no./ model | Protective measures implemented | Circuit ID number/ type | Building ID | Room or area |
|------|--------------|---------------------------|--------------------------|---------------------------------|-------------------------|-------------|--------------|
| 1. | WAN-001 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Instruction: Create and maintain an accurate list of actual communication connections (WAN) between the SCADA system and any other systems or equipment outside the defined electronic perimeter. This could include a WAN connection to the regional EMS or ISO SCADA system or other such connections. The purpose of this list is primarily to document WAN-based electronic access points (APs) through which an external attacker could attempt to gain access to the SCADA system. This list should include connections to the Internet via an ISP, leased telephone lines used for point-to-point network connections, frame-relay circuits, X.25 circuits, and T1/T3 circuits. The actual connection points (in the form of communications equipment and the ports used) should be defined to the level necessary to enable an authorized person to physically disconnect (or reconnect) and isolate the SCADA system from external systems. This information will also be useful in the configuration of a NIDS (Network Intrusion Detection System) that monitors for unexpected traffic on the SCADA LAN. Another key component of this list is the documentation of the protective measures (or verification of the existence of suitable protective measures) being applied to secure this AP. The structure and content of this list should be modified, as needed, to incorporate sufficient information to permit management review of the protective measures in place. This does not have to include the details concerning the programming of rules in a firewall, but it should indicate that such provisions are in place, identify the document where those details are recorded, and document that the provisions are reviewed on a regular basis. With firewalls, there is a need for regular updating of virus profiles, and some mechanism needs to be in place to ensure that such updates are performed. That need not be part of this list, but this list should indicate the person responsible. This list should be reviewed on a biannual basis or whenever the equipment or network configuration of the SCADA system is modified. This list should be considered as a critical information asset and handled with the requisite security and confidentiality. The field which does not apply may be scored out.

| | | | |
|-------------|------------------------------|------------------------------|---------------------------|
| Signature | Prepared By <i>Vikash</i> | Checked By <i>Rishabh</i> | Issued by <i>Sumit</i> |
| Date | 11.02.2025 | 11/2/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 75 of 76 | Instruction No. TI/IN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

ANNEXURE- 13**TELEPHONE CONNECTIONS (MODEMS)**

| S.N. | No. assigned | Description / purpose | Telephone no. | Telecom Circuit ID | Modem ID | Protective measures implemented | Building ID | Room or area |
|------|--------------|-----------------------|---------------|--------------------|----------|---------------------------------|-------------|--------------|
| 1. | TEL-001 | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Instruction: Create and maintain an accurate list of authorized telephone circuits that provide dial-out and/or dial-in connectivity to the SCADA system, as well as leased lines used for remote, dedicated, serial communications to other systems. This is not specifically a list of the leased telephone circuits used for RTU polling, although it may be used for that purpose if that information is not documented elsewhere. This list should not include any leased telephone line used to create a WAN linkage to another site/facility (e.g., a field site), because that would be a WAN connection (and thus should be listed in the previous table entitled "Wide Area Network Connections"). This list is intended to document primarily dial-in/dial-out telephone circuits that could enable an external attacker to communicate with the SCADA system, one of the computers that compose the SCADA system, or to be routed onto the SCADA LAN. Of primary concern are any such telephone lines that are permanently connected to a modem set up for auto-answering of an incoming call. Making and maintaining an accurate inventory of all such telephone circuits is an essential component of cybersecurity. The list should document the measures (dial-back, encrypting modems, VPN, manual connection of modem, etc.) used to secure this connection. Management should review the list and make decisions about the need for each, as well as about the suitability of the protection used to secure each. This list should be coordinated with accounting information related to any conventional telephone circuits (circuits not derived from a bulk T1/T3 circuit), so that all such independent circuits are identified. If any circuit has multiple extensions, each should be identified. The employees authorized to use each circuit should be identified, as should the manager responsible for authorizing the usage. This list should be reviewed on a biannual basis or whenever the equipment or communications configuration of the SCADA system is modified. This list should be considered as a critical information asset and handled with the requisite security and confidentiality. The field which does not apply may be scored out.

| | | | |
|-------------|----------------|-----------------|-----------------|
| | Prepared By | Checked By | Issued by |
| Signature | <i>Vishakh</i> | <i>11/02/21</i> | <i>11/02/21</i> |
| Date | 11-02-2025 | | |
| Designation | JE/ TI | AOE/ TI-3 | DIRECTOR/ TI-3 |

| | | |
|---------------|---|---|
| Page 76 of 76 | Instruction No. TI/TN/0052 (Version 1.0) | Technical Instruction regarding Standard Operating Procedure for implementing Cyber Security Guidelines for protection of Critical Information Infrastructure (CII) of Indian Railways with respect to SCADA System |
|---------------|---|---|

CATEGORY: PHYSICAL ACCESS MONITORING & CONTROL**ANNEXURE- 14****ENTRY POINTS INTO SENSITIVE AREAS**

| S.N. | No. assigned | Area/ Section | Building ID | Floor/ room | Entrance/ egress | Type | Access level | Control mechanisms | Last tested on | Alarms |
|------|--------------|---------------|-------------|-------------|------------------|------|--------------|--------------------|----------------|--------|
| 1. | ACC-001 | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Instruction: Create and maintain an accurate list of authorized physical entrances into facilities and areas containing critical systems and information. All non-authorized entrances (windows, loading docks, suspended ceilings, etc.) are assumed to be monitored and/or alarmed or sealed in an acceptable manner. The purpose of this list is to account for all allowable means of entrance and/or egress (e.g., a fire door) and to enumerate the control (and monitoring) mechanisms that will be used to secure these access points. Not all areas require the same level of access control or monitoring. This will be a decision that will be made by the Zonal Railways. This list is intended as an aid in formulating a strategy for access control and monitoring. Access controls may range from simple keyed locks to snares with biometric authentication, depending on the critical nature and contents of the area being protected. This will be up to the management of the particular Zonal Railway. If monitoring is performed, the mechanisms can range from a simple log book to full-time video surveillance or even an armed guard. Again, the appropriate mechanisms must be determined by the respective Zonal Railways. If entry requires that special authorizations be given and possibly the use of a reserved item (e.g., a special key), then this should be indicated in the list above. There should be written procedures for the testing of security mechanisms and for the upgrading and replacement of existing mechanisms. The mechanisms used for access control and monitoring shall be reviewed and tested on a periodic basis, and this information should be added to the table. This list should be reviewed at least annually and whenever a change is made to the facility or an access security mechanism is replaced or serviced. This list should be considered as a critical information asset and handled with the requisite security and confidentiality. The field which does not apply may be scored out.

| | | | |
|-------------|-------------|------------|----------------|
| Signature | Prepared By | Checked By | Issued by |
| Date | 11-02-2025 | 11/02/25 | 11/02/25 |
| Designation | JE/ TI | ADE/ TI-3 | DIRECTOR/ TI-3 |