**<<Name of Organisation>>**

**Standard Operating Procedure (SoP)**

**for Cyber-Security**

CONFIDENTIALITY CLAUSE

This document is the property of **<<Organisation Name>>**. All ideas and information contained within the document is the intellectual property of **<<Organisation Name>>**. These documents are not for general distribution and are meant for use solely by the person/persons to whom it is specifically issued to or shared with. **<<Organisation Name>>** does not share this document with any third party or vendor unless specifically exempted by the competent authority. Copying or unauthorized distribution of these documents, in any form or means including electronic, mechanical, photocopying or otherwise is illegal.

**CONTACT INFORMATION**

For any question regarding this policy, please contact -

Email:

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| **Document Version Control Note** | |
| Name of the Document | SoP for Cyber Security |
| Document Version Number | XX |
| Effective Date | XX.XX.XXXX |
| Approved By | XXXX |
| Document Classification | Restricted |
| Distribution List | CISO, ISMs, Nominated Members of <<Organization Name>>, Vendors / third parties and Service providers |
| Access Level | Read Only |

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Release Date** | **Prepared By** | **Reviewed/**  **Approved By** |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 5](#_Toc104395599)

[2 Purpose 5](#_Toc104395600)

[3 Scope and Applicability 5](#_Toc104395601)

[4 Standard Operating Procedures (SoP) for Cyber-Security 6](#_Toc104395602)

[5 Change, Review and Update 13](#_Toc104395603)

[6 Standard Operating Procedure Templates 14](#_Toc104395604)

# Introduction

**<<Organisation Name>>** handles critical IT and OT infrastructure which includes assets, applications, important data, information systems and processes for electricity transmission. **<<Organisation Name>>** infrastructure is classified as critical infrastructure by the Government and there are many periodic advisories issued by various government agencies. It is important to follow cyber security standard operating procedures in **<<Organisation Name>>** to protect critical infrastructure. It is important and mandatory for employees and associated vendors/ third-parties or any interested party to adhere to best industry practices and cyber security SOP to maintain standard operational method throughout **<<Organisation Name>>**.

# Purpose

The main purpose of this SOP is to ensure mandatory cyber security practices and best industry practices are followed. This SOP is should be implemented for **<<Organisation Name>>.**

# Scope and Applicability

The procedure written in this document is applicable to all **<<Organisation Name>>** employees, vendors/third parties/service provides and contractors as per applicability of cyber security procedures and recommendations by CISO. This SOP is applicable for **<<Organisation Name>>.**

# Standard Operating Procedures (SoP) for Cyber-Security

**Procedure for Organization is as follows**:

| **Sr. No.** | **Activity** | **Responsible** |
| --- | --- | --- |
| 1. | Define the security goals, objectives, scope, and boundaries of information security program ***(Refer Annexure 5)*** | Cyber Security Team |
| 2 | Define minimum baseline security standard applicable to all installed Cyber assets and evaluate the same periodically for any change/upgradation of base line.  Ensure all new procurements of Cyber asset are in compliance with minimum base line identified. The Minimum base lines should be part of the standard specifications of all such procurement made by the constituents. | CISO |
| 3. | Estimate budget and resources required to develop and maintain a resilient and robust cyber system | CISO |
| 4. | Define information security measurement metrics and other key performance indicators. ***(Refer Annexure 6)*** | Cyber Security Team |
| 5. | A formal process should be followed for creating, documenting, reviewing, updating, and implementing security policies, procedures, plans, guidelines and processes. | ISMs & Cyber Security Team |
| 6. | Disseminate information security policies, procedures and guidelines to all concerned personnel including management, employees, contractors, sub-contractors and other stakeholders | CISO |
| 7. | Define roles and responsibilities of the key personnel of the Organization for ensuring implementation of policies and guidelines of information security.  ***Please Refer Annexure-7 for Roles and Responsibilities of CISO*** | CISO |
| 8. | Enforce and oversee implementation of approved information security policies, procedures, plans, guidelines and ISMS as per ISO-27001. | CISO |
| 9. | Ensure that information security considerations are integrated with IT and OT system planning, development & acquisition life cycle. | ISMs, **<<Organisation>>** Nominated members |
| 10. | Identify Critical Information Infrastructure (CII) based on following parameters but not limited to:   1. Functionality: It may be viewed at two levels-Functional uniqueness and Functional Dependency. 2. Criticality Scale: It can involve factors such as the availability, delivery, access, and consummation of essential services. 3. Degree of Complementarities: It considers that how various systems in an organization are complementing each other. 4. Time duration: It is important because it may happen that not all systems are always critical and all circumstances and there may be time slots in which they are critical. | CISO, ISMs, **<<Organisation>>** Nominated members |
| 11. | Classify all documents as ‘Top Secret’, ‘Confidential’, ‘Restricted’ and ‘Public’. A document which has been classified as ‘Top Secret’ is to be treated as the most critical document in **<<Organisation>>**. Also, the appropriate documents must be stored in a secure manner. | CISO, ISMs, **<<Organisation>>** Nominated members |
| 12. | Implement Segregation of Duties (SoD) to reduce conflicts of duties and interests | ISMs, **<<Organisation>>** Nominated members |
| 13. | Identify and allocate a dedicated team for asset and inventory management, with clear roles and responsibilities. | CISO and ISMs |
| 14. | Periodically evaluate and review effectiveness of information security policies, procedures, standards, plans, guidelines and processes etc. | CISO |
| 15. | Issue alerts and advisories with respect to new vulnerabilities/threats to all concerned personnel, departments, and inform other related organizations | CISO |
| 16. | Perform Risk Assessment and based on analysis perform risk mitigation on regular basis. | CISO, ISMs and Cyber Security Team |
| 17. | Document any non-compliance within a stipulated time frame as deemed fit by **<<Organisation>>**. A valid reason in the documentation for not complying with cyber security policies, plans, procedures, guidelines, standards, processes etc. | ISMs and Cyber Security Team |
| 18. | Approve any exception and noncompliance with justification and submit to the senior management. | CISO |
| 19. | Share information related to critical information security incidents and breaches with associated reporting organizations. | CISO |
| 20 | Raise information security awareness among management, employees, contractors, subcontractors, and other stakeholders.  Provide Cyber Security Training to all persons engaged in O&M of IT and OT Systems as per Article 8 of CEA (Cyber Security in Power Sector) guidelines 2021. | CISO |
| 21. | Coordinate and ensure implementation of a Business Continuity Plan (BCP). Periodically conduct mock drills to evaluate the effectiveness of the Business Continuity Plan | CISO, ISMs, **<<Organisation>>** Nominated members |
| 22. | Ensure compliance of information security by contractors/suppliers/sub-contractors etc. | ISMs, **<<Organisation>>** Nominated members |
| 23. | Ensure all information systems with the Organization are adequately patched and updated. Evaluate compliance with respect to legal and regulatory requirements for information security. | ISMs, **<<Organisation>>** Nominated Members Nominated Members of Third parties, vendors or service providers |
| 24. | Perform Cyber security audit bi-annually from CERT-In empaneled auditor and prepare Cyber security audit report along with recommendations for improving Cyber security and present to senior management. | ISMs and Cyber Security Team |
| 25. | Ensure closure of reported audit observations | ISMs, **<<Organisation>>** Nominated members, Nominated Members of Third parties, vendors or service providers |
| 26. | Send a copy of the audit report periodically to regulatory bodies and senior management as required. | CISO |
| 27 | Ensure that CEA (Cyber Security in Power Sector) guidelines 2021 and amendments thereof, if any is being followed by the Organization.  ***Please Refer Annexure -8 for the CEA (Cyber Security in Power Sector) guidelines 2021*** | CISO |

**Procedure for Incident Response:**

| **Sr. No.** | **Activity** | **Responsible** |
| --- | --- | --- |
|  | Notify any suspicious event or incident to respective ISM or incident management team.  Incident information may be received from the following sources:   * Call * Email | All User/Employees/ Contract employees/ Vendors |
|  | Incident Logging Initiate Incident Management Process and log or record the incident when there is a disruption of any IT or OT services, or any suspicious incident reported by any user. | Incident Management Team |
|  | Classification Classify the incident based on probable Impact and Urgency of the incident. Decide Priority for incident repose as per Impact-Urgency matrix. | Incident Management Team |
| 4. | Assign Ownership Assign logical ownership to the Incident logged. The Assignment could be self or to any individual of team to have the incident resolved at the earliest. | Incident Management Team |
| 5. | a. Reporting to CERT-IN and Regulatory Authorities:  The incident to be reported to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents as per the directives of CERT-IN and CEA Guidelines.  The incident also to be reported to respective Sectoral CERT and Regulatory Authorities  ***Please Refer Annexure -9 for the directives of CERT-IN.***  ***Please Refer Annexure -10 for the CERT-IN incident report form.***  b. Communicate/Inform Stakeholders  Inform/Report users, interested parties, senior management and service providers about logged incident, its priority and assignee details. Periodically communicate status of incident with stakeholders-based on priority. | Incident Management Team |
| 6. | Matching the Incident Match the incident against below parameters once the incident is assigned to the appropriate team.  Parameters:   * Incident Records * Problem Records * Change Records * Known Error Database.   The incidents can be matched based on the symptoms of the incident recorded. | Incident Management Team |
| 7. | Check whether resolution available from KEDB The technical staff checks in the Knowledge database for any solution provided for similar Incidents.  If solution exist move to step 9 else step 8. | Incident Management Team |
| 8. | Investigation Analyse and investigate incident in detail and to take up suitable measures to limit the spread of the incident ensuring the spread is limited on to the affected system. Search for best possible resolution. Suitable checklist to be referred for incident which are known and mitigation measures identified earlier.  After determining that there is no resolution available, it is necessary to escalate functionally/hierarchically and transfer the incident from existing line of support (L1 to L2 and then to L3).  The relevant team to investigate and diagnose the issue and look for a work around. Evidences should be collected during investigation and preserved for future reference. | Incident Management Team and relevant IT and OT teams |
| 9. | Provide Resolution The objective of the Incident Management is to restore services as soon as possible, hence it is important to provide a resolution. The resolution provided could either be a workaround / temporary fix or a permanent change (New/Update) for resolving the Incident.  After resolution, status should be set to Resolved. | Incident Management Team and relevant IT and OT teams |
| 10. | Review  Based on the solution provided, it is necessary to know if the solution provided is effective or not. Based on the review of resolution and decisions taken, the following actions might be taken:   * Suspend an Incident Resolution * Cancel an Incident * Reopen an Incident * Close an Incident | Incident Management Team |
| 11. | Close Incident Ticket Close incident only after review. Ensure that the resolution details are recorded correctly, and the incident is resolved.  Before closure of ticket ensure sufficient monitoring time of the affected system and effectiveness of the deployed resolution. | Incident Management Team |
| 12. | Communicate Closure  Create a detailed RCA/Technical investigation report (TIR) for the incident and ensure the same is communicated to all relevant stake holders including Incident Management team members.  Inform all users, interested parties, senior management and service providers about resolution.  Track the resolution time and same to be taken up for improvement in future.  Ensure learnings from Incident are shared with all stakeholders  ***Refer Incident Report Form Annexure 2*** | Incident Management Team |

**Procedure for Threat Advisory Compliance:**

| **Sr. No.** | **Activity** | **Responsible** |
| --- | --- | --- |
| 1. | Receive Threat advisories, assessment reports and recommendations from nodal agencies such as Cert In, Sectoral Cert, NCIIPC and other third-party advisors. | CISO |
| 2. | E-Mail threat advisories, reports and recommendations to respective ISMs and internal nominated members of **<<Organisation>>**  ***Please refer Annexure-3 & 4 for Nominated members of* <<Organisation>> and Vendors/Third Parties.** | CISO |
| 3. | Receive and identify applicable threat advisories and record them in compliance tracker.  ***Please refer Annexure-1 for Threat Advisory Compliance Tracker*** | ISMs, **<<Organisation>>** Nominated members |
| 4. | Implement threat advisories and recommendations if applicable threat advisories to **<<Organisation Name>>** employees and record compliance in compliance tracker. | ISMs, **<<Organisation>>** Nominated members |
| 5. | In case of Vendor specific advisories or recommendations or third-party dependencies then forward threat advisories, recommendations and reports to relevant Nominated Members of vendors/ third parties or service providers and record details in compliance tracker. | ISMs, **<<Organisation>>** Nominated members |
| 6. | Implement received applicable threat advisories and recommendation received from ISM and **<<Organisation>>** Nominated Members within stipulated timeframe. | Nominated Members of Third parties, vendors or service providers |
| 7. | Share compliance and evidence against received threat advisories and recommendations with ISM and **<<Organisation>>** Nominated members within stipulated timeframe. | Nominated Members of Third parties or vendors or service providers |
| 8. | Forwarding compliance and evidences received from third parties or vendors or service providers to CISO and Record compliance in compliance tracker | ISMs, **<<Organisation>>** Nominated members |
| 9. | Sending Consolidated Compliance to respective government agencies such as Cert-IN, Sectoral Cert, NCIIPC and other third-party advisors. | CISO |
| 10. | Quarterly Review of status of compliance of threat advisories, compliance tracker and discuss issues and improvement opportunities with ISMs, nominated members of **<<Organisation>>**, Nominated Members of Vendors / Third parties / Service providers. | CISO |
| 11. | Quarterly Reporting of status of compliance of threat advisories and discuss issues, if any with Higher Authority of **<<Organisation>>** | CISO |

# Change, Review and Update

This procedure shall be reviewed once every year unless the **<<Organisation Name>>** considers an earlier review necessary to ensure that this procedure remains current. Changes to this procedure shall be approved by CISO and senior management of **<<Organisation Name>>.**

# Standard Operating Procedure Templates

|  |  |  |
| --- | --- | --- |
| S. No. | Document Name | Document |
| 1. | Threat Advisory Compliance Tracker |  |
| 2. | Incident Report |  |
| 3. | Nominated Members of <<Organisation Name>> |  |
| 4. | Nominated Members of vendors / Third parties |  |
| 5. | Scope, Objectives & Goals of Information Security Program |  |
| 6. | Security measurement metrics and other Key Performance Indicators |  |
| 7 | Roles and Responsibility of CISO (as per CERT-IN) |  |
| 8 | CEA (Cyber Security in Power Sector) guidelines 2021. |  |
| 9 | The directives of CERT-IN |  |
| 10 | The CERT-IN incident report form. |  |