

# Information Security Policy

## Version 5.0

### Document Statistics

Type of Information	Document Data
Document Title	Information Security Policy V5
Date of Release	21/12/23
Document Version No	5.0
Security Classification	Internal
Document Status	Official Release

### Document Revision History

Ver. No.	Date	Change Description	Signature	Approved By
1.0	01 July 2020	Change in formats and logo added information on digital certificates		Pankaj Shrivastava
2.0	4 <sup>th</sup> March 2023	Policy Updated in-line with recommendation by E&Y		Pankaj Shrivastava
3.0	07 December 2023	Updated in line with ISO 27001:2022		Jagannath Sahoo

### Approved by Leadership Team

Sl. No.	Name	Position	Signature	Date
1	Saurabh Gupta	Group CDIO		
2	Kallol Chakravarty	Group HR Head		
3	SK Mathu Sudana	CEO (IGSL)		
4.	Kailash Tarachandani	CEO (IWL)		

### Document Reference List

S. No.	Document Name
1	EDR Policy
2	IT Asset Management Policy
3	Secure SDLC Policy
4	IT Security Log Management Policy
5	Network Management Policy
6	Key Management and Encryption Policy
7	IT Acceptable Usage Policy
8	Backup and Restoration Policy
9	User Access Management Policy
10	Data Management Policy
11	IT Incident Management Policy
12	IT Internal Audit Policy
13	IT Physical Security Policy
14	Vulnerability Assessment and Penetration Testing Policy
15	Change Management Policy
16	IT Capacity Management Policy
17	Data Privacy Policy
18	IT Business Continuity and Management Policy
19	Third-Party Security Management Policy

## Contents

<b>1. Introduction</b>	8
<b>2. Scope</b>	8
<b>3. Objective</b>	8
<b>4. Policy Enforcement</b>	8
<b>5. Exception Management</b>	8
<b>6. Reference Laws and Documents</b>	9
<b>7. Terms and Definitions</b>	9
<b>8. Policy</b>	10
8.1 Information Security Framework	10
8.1.1 Information Security Domains	10
8.1.2 Information Security Themes and Attributes	10
8.2 Organizational Controls	11
8.2.1 Policies for Information Security	11
8.2.2 Information Security Roles and Responsibilities	11
8.2.3 Segregation of Duties	12
8.2.4 Management Responsibilities	12
8.2.5 Contact with Authorities	13
8.2.6 Contact with Special Interest Groups	13
8.2.7 Threat Intelligence	13
8.2.8 Information Security in Project Management	14
8.2.9 Inventory of information and other associated assets	14
8.2.10 Acceptable use of information and other associated assets	15
8.2.11 Return of assets	16
8.2.12 Classification of Information	16
8.2.13 Labelling of Information	17
8.2.14 Information Transfer	17
8.2.15 Access Control	18
8.2.16 Identity Management	19
8.2.17 Authentication Information	19
8.2.18 Access Rights	20
8.2.19 Information Security in Supplier Relationship	20
8.2.20 Addressing information within Supplier Relationship	20
8.2.21 Managing Information Security in the ICT supply chain	20

8.2.22	Monitoring, review and change management of supplier services .....	21
8.2.23	Information security for use of cloud services.....	21
8.2.24	Information security incident management planning and preparation .....	22
8.2.25	Information security incident management planning and preparation .....	22
8.2.26	Response to Information security incidents .....	22
8.2.27	Learning from Information security incidents .....	22
8.2.28	Collection of evidence.....	23
8.2.29	Information Security during disruption .....	23
8.2.30	ICT readiness for business continuity .....	23
8.2.31	Legal, statutory, regulatory, and contractual requirements .....	24
8.2.32	Intellectual Property Rights .....	24
8.2.33	Protection of Records .....	25
8.2.34	Privacy and Protection of PII.....	25
8.2.35	Independent Review of Information Security.....	25
8.2.36	Compliance with policies, rules, and standards for information security .....	26
8.2.37	Documented operating procedures.....	26
8.3	People Controls.....	27
8.4.1	Screening.....	27
8.4.2	Terms and Conditions of employment .....	27
8.4.3	Information security awareness, education, and training.....	27
8.4.4	Disciplinary Process.....	28
8.4.5	Responsibilities after termination or change of employment.....	28
8.4.6	Confidentiality or Non-Disclosure Agreements .....	28
8.4.7	Remote Working .....	29
8.4.8	Information security event reporting .....	29
8.4	Physical Controls .....	30
8.4.1	Physical Security Perimeters .....	30
8.4.2	Physical entry .....	30
8.4.3	Securing offices, rooms, and facilities.....	31
8.4.4	Physical Security Monitoring .....	31
8.4.5	Protecting against physical and environmental threats .....	31
8.4.6	Working in secure areas.....	32
8.4.7	Clear desk and clear screen .....	32
8.4.8	Equipment siting and protection .....	33
8.4.9	Security of assets off-premises .....	33

8.4.10	Storage Media .....	34
8.4.11	Supporting Utilities .....	34
8.4.12	Cabling Security.....	34
8.4.13	Equipment Maintenance .....	35
8.4.14	Secure disposal or re-use of equipment .....	35
8.5	Technological Controls.....	36
8.5.1	User endpoint devices .....	36
8.5.2	Privileged Access Rights .....	37
8.5.3	Information Access restrictions .....	37
8.5.4	Access to source code .....	38
8.5.5	Secure Authentication .....	38
8.5.6	Capacity Management .....	39
8.5.7	Protection against malware .....	40
8.5.8	Management of Technical Vulnerabilities .....	40
8.5.9	Configuration Management.....	41
8.5.10	Information Deletion .....	42
8.5.11	Data Masking .....	42
8.5.12	Data Leakage Prevention .....	42
8.5.13	Information Backup .....	43
8.5.14	Redundancy of information processing facilities.....	43
8.5.15	Logging .....	44
8.5.16	Monitoring activities .....	44
8.5.17	Clock Synchronisation .....	45
8.5.18	Use of privileged utility programs.....	45
8.5.19	Installation of software on operational systems .....	45
8.5.20	Network security.....	46
8.5.21	Security of Network services.....	47
8.5.22	Segregation of Networks .....	47
8.5.23	Web filtering .....	47
8.5.24	Use of cryptography.....	48
8.5.25	Secure Development Lifecycle.....	49
8.5.26	Application Security Requirements.....	49
8.5.27	Secure system architecture and engineering principles .....	50
8.5.28	Secure coding.....	51
8.5.29	Security testing in development and acceptance.....	51

8.5.30	Outsourced development .....	52
8.5.31	Separation of development, test, and production environments .....	52
8.5.32	Change Management.....	53
8.5.33	Test Information .....	53
8.5.34	Protection of Information Systems during audit testing .....	54

## 1. Introduction

The information security policy outlines commitment to the security of Renewable Energy Business comprises of Inox Wind Limited, Inox Green Energy Services Limited, Resco Global Wind Services Ltd., (hereafter referred to as “Renewable Energy”) its businesses, subsidiaries, associates, resources, employees, contractors, other stakeholders, and the actions they shall take to prevent any information security incidents. It also seeks to set responsibilities for functions/businesses to deliver against information security commitments as well as establish a management framework to initiate/control the implementation and operation of information security within RENEWABLE ENERGY.

The CEA (Central Electricity Authority) has formulated a guideline on cyber security in the power sector under the provision of Section 3(10) in the ‘Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019’. The guideline has been prepared after extensive consultations with stakeholders and inputs from CERT-In, the National Critical Information Infrastructure Protection Centre, NSCS (National Cyber Safety and Security Standards), IIT-Kanpur, and subsequent discussions with the Ministry of Power. All power sector utilities are mandated to follow the guidelines to ensure cyber security in the power sector. Refer to Annexure – 1 for detail guidelines and link.

[https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines\\_on\\_Cyber\\_Security\\_in\\_Power\\_Sector\\_2021-2.pdf](https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf)

## 2. Scope

This document applies to all the users in the organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. The policy includes business operational activities of all functional Renewable Energy locations as per Annexure - A

## 3. Objective

The overall objective of this policy shall be to provide guidance and direction for the protection of RENEWABLE ENERGY’s data, information, and information systems against any kind of accidental or deliberate damage, destruction, or misuse. It shall also seek to ensure that the information systems comply with relevant standards, laws, and regulations.

## 4. Policy Enforcement

Any violation of this policy by a RENEWABLE ENERGY employee shall be subjected to corrective actions and or/disciplinary actions as per HR Policies.

***(For more details, please refer to RENEWABLE ENERGY HR Policy)***

Any violation of this policy by a RENEWABLE ENERGY partner/vendor shall be reported to their respective organizations to take appropriate action. The partner/vendor organization may be subjected to penalties and/or legal action as per the contractual agreement between both parties.

***(For more details, please refer to Third Party Security Management Policy\_V5)***

## 5. Exception Management

Exceptions may be granted in cases where security risks are mitigated by compensating controls and in cases where security risks are at a low, acceptable level and compliance with minimum security requirements, not



interfering with legitimate business needs. To request a security exception, approval from the respective Unit head/Business head, Group CDIO, Group Head HR & CEO.

## 6. Reference Laws and Documents

Reference Laws:

- ISO27001:2022
- IT Act 2000
- CERT-In Guidelines
- PDPA (Personal Data Protection Act 2023)
- GDPR (General data protection regulation)

Reference Documents:

1. EDR Policy
2. IT Asset Management Policy
3. Secure SDLC Policy
4. IT Security Log Management Policy
5. Network Management Policy
6. Key Management and Encryption Policy
7. IT Acceptable Usage Policy
8. Backup and Restoration Policy
9. User Access Management Policy
10. Data Management Policy
11. IT Incident Management Policy
12. IT Internal Audit Policy
13. IT Physical Security Policy
14. Vulnerability Assessment and Penetration Testing Policy
15. IT Change Management Policy
16. IT Capacity Management Policy
17. Data Privacy Policy
18. IT Business Continuity and Management Policy
19. Third-Party Security Management Policy

## 7. Terms and Definitions

- **Information Asset:** A piece of information which has business value. Types of Information assets include software, hardware, electronic & paper documents, services, facilities, and people.
- **Information Processing Facility:** Any information processing system, service or infrastructure, or the physical locations housing them.
- **Information Security:** All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, authenticity, and reliability, of information or Information Processing Facilities.
- **Third Party:** All vendors who enter a direct contract (including their employees/sub-contractors) providing services/products to RENEWABLE ENERGY.
- **Data Subject:** The person to whom personal data belongs.

- **Security Event:** A security event is an identified occurrence of a system, service or network state indicating a possible breach of Information Security policy or failure of safeguards, or a situation that may be security relevant.
- **Information Security Incident:** An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- **Infrastructure Elements:** Generic term used for network devices, security devices, telecom devices, servers etc.
- **Malware:** Malware is a generic term used for viruses, worms, Trojans, spywares, and other types of malicious codes.
- **Control:** Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.
- **Asset Owner:** An asset owner refers to an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets.
- **Storage Media:** Information recorded/stored on paper and hard copy files/folders and information stored in portable hard disks, USB, CD/DVD, memory cards, tape drives, phones, mobile devices.
- **Cloud Storage:** Cloud storage allows to save data and files in an off-site location that can be accessed either through public network or a dedicated private network connection.
- **Business Continuity:** Continuity of RENEWABLE ENERGY's activities irrespective of the occurrence of natural disasters, terrorist strikes, man-made disasters etc. Refer to Cyber Crisis Management Plan.
- **Risk Assessment:** To understand what actions should be taken to minimize future damage to carrier and what risks are inevitable.

## 8. Policy

### 8.1 Information Security Framework

#### 8.1.1 Information Security Domains

- This policy addresses the domains and controls mentioned in the ISO 27001:2022 standard under the following:
  - a. Organizational Controls
  - b. People Controls
  - c. Physical Controls
  - d. Technological Controls

#### 8.1.2 Information Security Themes and Attributes

- **Control Type** – This attribute views the control from the perspective of when and how the control modifies the risk about occurrence of an Information Security Incident. *Attribute Values comprise of Preventive, Detective, and Corrective.*
- **Information Security Properties** – This attribute views the control from the perspective of which characteristic of the information the control will contribute to preserving. *Attribute values comprise of Confidentiality, Integrity, and Availability.*

- **Cybersecurity Concepts** – This attribute views the control from the perspective of the association of controls to cybersecurity concepts as defined in ISO 27110. *Attribute values comprise of Identify, Protect, Detect, Respond, and Recover.*
- **Operational Capabilities** – This attribute views the control from the perspective of information security capabilities. *Attribute comprises of Governance, Asset management, Information Protection, Human Resource Security, Physical Security, System and Network Security, Application Security, Secure Configuration, Identity and Access Management, Threat and Vulnerability Management, Continuity, Supplier Relationship Security, Legal and Compliance, Security Event Management, and Security Assurance.*
- **Security Domains** – This attribute views the control from the perspective of four Information Security Domains as identified in ISO 27001:2022. *The attributes comprise of Governance and Ecosystem, Protection, Defence and Resilience.*

## 8.2 Organizational Controls

### 8.2.1 Policies for Information Security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Governance	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Resilience</li> </ul>

- This policy highlights the senior management’s intention to identify and secure organization’s valuable assets in a manner which complies with legislations, meets leading practices and business needs, protecting it from unauthorized use, disclosure, or destruction. To ensure continuing suitability, adequacy, and effectiveness, the information security policy and supporting documents shall be reviewed annually or earlier if a significant change occurs (e.g., technology level changes in the organization, business level changes in the organization and regulations that impact information security).
- The input to the review should include but not be limited to:
  - Change in the business.
  - Change in the IT environment.
  - Trends related to threat and vulnerabilities; and
  - Reported security incidents and audit findings.
- Records for the management review and approval shall be maintained.
- Recommendations provided by relevant authorities and/or other associated entities, both within and outside the organization, shall be part of the security policy review agenda.

### 8.2.2 Information Security Roles and Responsibilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Governance	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Resilience</li> </ul>

- All Information Security responsibilities, with regards to the protection of RENEWABLE ENERGY’s sensitive information, Information Systems and information processing facilities shall be clearly defined through job descriptions, work allocation and delegation of tasks.
- The Information security policy shall be approved by CDIO.
- The standards, procedures, templates, and guidelines shall be approved by CDIO.

- The defined Information Security responsibilities shall be formally allocated and accepted across the organization. Such responsibilities shall include but are not limited to: -
  - Identifying the information assets and the security processes associated with each individual asset.
  - Defining and documenting the asset ownership, the level of responsibility and authorization levels; and
  - Classification, labelling and handling of information assets in accordance with the RENEWABLE ENERGY Data Classification, Labelling and Handling Policy.
- Conduct risk assessment for all the identified critical assets at the time of any major change in the business/operational environment or once in every year, whichever is earlier.
- Identification and implementation of controls that shall be termed necessary to adequately protect assets.
- Reviewing and approving user access privileges in accordance with the User Access Management Policy; and
- Conduct of internal audit, and fire drill and other audit activities, to ensure that the above mentioned are being followed.

***(For further details please refer to Data Management Policy\_V5 and IT Asset Management Policy\_V5)***

### 8.2.3 Segregation of Duties

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Governance</li> <li>• Identity and Access Management</li> </ul>	Governance and Ecosystem

- Roles defined to carry out business activities must consider segregation of duties to reduce opportunities for deliberate or accidental misuse of infrastructure elements and/or software. E.g., ability to initiate, authorize, execute, and verify requests should be split so that no one person completes the entire request.
- Wherever segregation of duties is not possible, appropriate compensatory controls such as activity monitoring, audit trails and management supervision shall be developed to detect misuse of access rights.
- When primary personnel are not available (e.g., vacations, illness and leave of absence) and the role is filled in by another person with a different role, appropriate segregation and/or compensatory controls shall be considered; and
- Conflicting functions (e.g., functions with ability to initiate, authorize, execute, and verify transactions) shall be identified and formally documented.

### 8.2.4 Management Responsibilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Identify	Governance	Governance and Ecosystem

- RENEWABLE ENERGY Management shall enforce all personnel to adhere Information Security Policy and other relevant documents.
- All the RENEWABLE ENERGY personnel shall be properly briefed on their Information Security Roles and Responsibilities.

### 8.2.5 Contact with Authorities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li><b>Preventive</b></li> <li><b>Corrective</b></li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Identify</li> <li>Protect</li> <li>Respond</li> <li>Recover</li> </ul>	Governance	<ul style="list-style-type: none"> <li>Defence</li> <li>Resilience</li> </ul>

- Appropriate contacts shall be established with law enforcement authorities, regulatory bodies, third party vendors such as hardware vendors, software vendors, and office security providers.
- The responsibilities to maintain those contacts shall be jointly fulfilled by the legal, Information Security team and IT team.

### 8.2.6 Contact with Special Interest Groups

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li><b>Preventive</b></li> <li><b>Corrective</b></li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Protect</li> <li>Respond</li> <li>Recover</li> </ul>	Governance	Defence

- The IT Head shall maintain appropriate contacts with special interest groups, forums, and professional associations related to Information Security to:
  - Improve knowledge about best practices and keep up to date with latest developments; and
  - Gain access to specialist Information Security advice.
- Such information security related interest groups are ISACA (Information Systems Audit and Control Association), CERT-IN (Computer Emergency Response Team) agency for respective country, and likewise.

### 8.2.7 Threat Intelligence

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li><b>Preventive</b></li> <li><b>Detective</b></li> <li><b>Corrective</b></li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Identify</li> <li>Detect</li> <li>Respond</li> </ul>	Threat and Vulnerability Management	<ul style="list-style-type: none"> <li>Defence</li> <li>Resilience</li> </ul>

- The IT Head shall gather threat intelligence feeds or alerts from various external sources such as Vendor (OEM) Reports, Government Agencies (CERT-IN), Subscription to publicly available Threat Intel web sources and analyse the feeds as per the existing threat vector or landscape and maintaining the feeds in a centralized manner to take appropriate mitigation actions.
- The IT Team shall update the appropriate IOCs in their respective security devices such as Firewalls, IDS, IPS, Anti-Malware, SIEM tool to prevent the RENEWABLE ENERGY environment from any potential cyber-attack.

### 8.2.8 Information Security in Project Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	Governance	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> </ul>

- Information security shall be integrated into organizations project management methods to ensure that information security risks are identified and addressed as part of projects. The project management methods in use shall require that:
  - Information security objectives are included in project objectives.
  - A project risk assessment is conducted at an early stage of the project to identify project risks.
  - Information security is part of all phases of the applied project methodology.
- Information security implications shall be addressed and reviewed regularly in all projects.

### 8.2.9 Inventory of information and other associated assets

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Asset management	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> </ul>

- All Information Assets (Physical, Software, Information, Paper, People, Site and Services) shall be clearly identified along with owners and an inventory of all assets shall be drawn and maintained; and
- Each function shall be responsible for identification of Information Assets and Information Systems used for processing and storing information; they shall maintain an inventory of such assets.
- Asset Owner shall be identified for each asset within the asset inventory.
- The asset owner or his delegates shall be responsible for:
  - Ensuring that assets are appropriately classified.
  - Defining and periodically reviewing access restrictions and classifications, considering applicable access control policies.
  - Approving information-oriented access control privileges.
  - Selecting special controls needed to protect information, such as additional input validation checks or more frequent backup procedures.
  - Approving all new or substantially enhanced application systems that use their information before these systems are moved into production operational status.
  - Reviewing reports about system intrusions and other events that are relevant to their information; and

- Select a security classification category relevant to their information and review this classification for possible downgrading or upgrading.
- Information owners shall not delegate ownership responsibilities to contractors /external consultants, or to any individual who is not a full-time employee of the company.
- Software asset management: Software asset management includes maintaining software license compliance; tracking the inventory and usage of software assets; and maintaining control over the deployment and use of software assets. These include:
  - Procurement details, such as number of licenses granted, expiry date of licenses, etc., of software purchased shall be recorded by the IT team.
  - Software usage and deployment shall be tracked and reconciled against purchase data on a periodic basis. Any discrepancies, if observed, shall be reported to the asset owner, fixed asset team and IT team.
  - In case software license agreements are found to be violated, the fixed asset team & IT team shall initiate immediate corrective actions to be taken as applicable.
  - Software purchases and related data shall be tracked and regularly monitored. IT team along with respective business owner of the applications, shall be responsible for conducting annual reviews on this data to determine, but not limited to, the following:
    - If more licenses are being used than purchased; and
    - If new software or a greater number of licenses need to be procured to meet future business requirements.
  - IT team shall conduct a review at least once a year, of servers, desktops & laptops to determine if any unauthorized and unlicensed software are installed.
- The asset owner shall be responsible for the conducting a risk assessment as described in IT Asset Management Policy.

***(For further details please refer to IT Asset Management Policy\_V5)***

#### 8.2.10 Acceptable use of information and other associated assets

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>● Confidentiality</li> <li>● Integrity</li> <li>● Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>● Asset management</li> <li>● Information Protection</li> </ul>	<ul style="list-style-type: none"> <li>● Governance and Ecosystem</li> <li>● Protection</li> </ul>

- Acceptable use of assets associated with information processing facilities shall be clearly defined.
- All users (employees) who use or interface with assets associated with information processing facilities shall acknowledge their awareness of acceptable use of assets.
- Employees and vendors using or having access to RENEWABLE ENERGY’s assets shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility; and
- RENEWABLE ENERGY shall ensure control against unauthorized copying of relevant information (e.g., intellectual property) by employees and vendors.
- RENEWABLE ENERGY shall ensure that adequate security controls are put in place to secure the information on the employee-owned devices.

***(For further details please refer to IT Acceptable Usage Policy\_V5)***

### 8.2.11 Return of assets

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	Asset management	Protection

- Upon termination of employment or services, the employees or third-party vendors shall return/ hand-over all RENEWABLE ENERGY's assets that were issued to them or are under their purview.

*(For further details please refer to IT Asset Management Policy\_V5)*

### 8.2.12 Classification of Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Identify	Information Protection	<ul style="list-style-type: none"> <li>Protection</li> <li>Defence</li> </ul>

- Information Assets and information processing systems shall be classified based on their business value, legal requirements, sensitivity, and criticality to the organization.
- Information Assets shall be classified as per established standard in the following parameters:

**Confidential** – This classification applies to data that must be available for RENEWABLE ENERGY to effectively perform its mission and meet legally assigned responsibilities, and for which special precautions are taken to ensure its accuracy, relevance, timeliness, and completeness. This data, if lost, could cause significant financial loss, inconvenience, or delay in performance of the RENEWABLE ENERGY mission.

*Examples: Third Party/Vendor Contracts, Internal Audit Reports, System Design Documents, Financial Records etc.*

**Internal** – This classification applies to data that is specifically meant for employees of RENEWABLE ENERGY. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact. The distribution of such documents shall remain with the business, employees, customers, stockholders and/or business partners.

*Examples: Intranet web site content, Process documentation like policies and procedures etc.*

**Public** – This classification applies to data, which has been explicitly approved by the management for open/public access.

*Example: Sales brochures, Web Site Content, Advertisements, Statutory Audit reports etc.*

- Following guidelines shall be considered for reclassification of data assets:
  - Classification of data assets should be reviewed periodically (at least once every year) to ensure adequate classification as per the business requirements.
  - Whenever there is a need to reclassify the data, the data custodian should seek approval from the data owner, in consultation with Business head, prior to changing the data classification.



- In case the data owner and Business head are same individual, the approval (over email) shall be taken accordingly.
- Reclassification date for “confidential data” should be mentioned on the document statistics section of any document; and
- After reclassification, the data custodian should ensure that all the necessary changes are incorporated in the asset register.

### 8.2.13 Labelling of Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Information Protection	<ul style="list-style-type: none"> <li>• Protection</li> <li>• Defence</li> </ul>

- Data owners shall ensure that data either in paper form or stored in removable media like tape, USB etc. shall be externally labelled (marked) with the appropriate classification.
- Data owners shall ensure that the labelling will be maintained until the paper / removable media is destroyed or data is declassified. Data owners shall ensure that in case of electronic documents, the appropriate data classification is mentioned in the footers of the document. Alternatively, the electronic documents residing on the systems shall be kept in folders marked according to the pre-defined data classification; and
- Users shall ensure that the naming of RENEWABLE ENERGY data files will be meaningful and capable of being recognized by its intended users. Every document should follow a specific naming convention for ease of understanding and to maintain the integrity of the document. **Example: IT Asset Management Policy**

### 8.2.14 Information Transfer

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Asset Management</li> <li>• Information Protection</li> </ul>	Protection

- RENEWABLE ENERGY shall ensure that security is maintained at all aspects of Confidentiality, Integrity, and Availability while transferring the information within and outside the organization.
- Adequate legal controls like signing of NDAs and other Information Security Controls shall be put in place while sharing the information with any third party.
- RENEWABLE ENERGY official emails shall not be forwarded to personal email account(s).
- RENEWABLE ENERGY emails shall not be forwarded to unauthorized personnel within or outside of RENEWABLE ENERGY network.
- All information stored, transmitted, received, or contained in RENEWABLE ENERGY's e-mail systems is RENEWABLE ENERGY's sole property and may be accessed by the company at any time; and
- Wherever possible, business functions shall use only officially appointed courier service providers for transmitting physical information.

### 8.2.15 Access Control

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	Identify and Access Management	Protection

- An access control policy shall be established, documented, and reviewed regularly considering the requirements of the business for the assets in scope. The policy should consider below mentioned points:
  - Access to different business applications.
  - Management of assigned level of access; and
  - Formal procedures/policies for defined roles and responsibilities.
- As per the principle of least access, every RENEWABLE ENERGY employee should only get access to RENEWABLE ENERGY network and network services as per their designated job's roles and responsibilities. The following points should be taken into consideration:
  - The networks and network services in scope for access.
  - RENEWABLE ENERGY employees shall only have direct access to the network services that they have been specifically authorized to use.
  - Users should not establish any external network connections that could permit third party users to gain access to RENEWABLE ENERGY systems and information; and
  - When using RENEWABLE ENERGY systems, users shall not deliberately conceal or misrepresent their network identity.
- A formal user registration and de-registration process shall be implemented to enable assignment of required access rights. The below mentioned points should be taken into consideration
  - All user IDs on RENEWABLE ENERGY systems shall be assigned according to the RENEWABLE ENERGY standard user ID creation.
  - Every user shall have a unique user ID and password for access to RENEWABLE ENERGY systems and networks.
  - There shall be a formal process for user id creation and deletion process.
  - User id creation/ modification/deactivation request shall be required to be authorized by respective Business head and submitted to application owner/IT team before user access is created; and
  - IT team should follow formal de-registration process for revocation of access to all RENEWABLE ENERGY systems and network services.
- A formal user access provisioning process shall be implemented to assign or revoke rights for all user types to all systems and services. The provisioning and revoking process should include the following points:
  - The respective Business head of the user shall be authorised to approve the access to RENEWABLE ENERGY domain, applications, and infrastructure components.
  - Post obtaining the required approval from Business head, access shall be provisioned/ granted to the user by the IT team; and
  - For any privileged access to RENEWABLE ENERGY systems/networks/applications the approval shall be obtained from CDIO in consultation with Business head.

- Process shall be defined to ensure that access rights associated with the employees, and third-party personnel are revoked upon termination of their employment, contract, or agreement.
  - The defined processes must also outline steps to be taken in case of management-initiated terminations based on disciplinary grounds.
  - If there is a change of role, necessary changes/adjustments shall be made so that the user does not have more rights than required to carry out the new job function and
  - The removal or modification of access rights for terminated RENEWABLE ENERGY employees or contract employee shall be carried out by the IT team.

### 8.2.16 Identity Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Identify and Access Management	Protection

- A formal user registration and de-registration process shall be implemented to enable assignment of required access rights. The below mentioned points should be taken into consideration
  - All user IDs on RENEWABLE ENERGY systems shall be assigned according to the RENEWABLE ENERGY standard user ID creation.
  - Every user shall have a unique user ID and password for access to RENEWABLE ENERGY systems and networks.
  - There shall be a formal process for user id creation and deletion process.
  - User id creation/ modification/deactivation request shall be required to be authorized by respective Business head and submitted to application owner/IT team before user access is created; and
  - IT team should follow formal de-registration process for revocation of access to all RENEWABLE ENERGY systems and network services.

### 8.2.17 Authentication Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Identify and Access Management	Protection

- Secret authentication information is a gateway to access valuable assets. It typically includes passwords, encryption keys etc. the allocation of secret authentication information shall be controlled through a formal management process.
  - Passwords used by the RENEWABLE ENERGY employees and those set/provisioned on systems, network devices shall meet complexity requirements.
  - Users shall be educated to keep the passwords allocated to them confidential.
  - When granting access to infrastructure or software(s), users shall be provided with a temporary or one-time password that meets the password complexity requirements. Users need to change this password at first login and shall be unique for each user; and
  - Temporary passwords should be given to users in a secure manner such as through restricted emails to intended user.

### 8.2.18 Access Rights

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	Identify and Access Management	Protection

- Asset owners in coordination with Business heads must review users' access rights at regular intervals. The below mentioned points should be taken into considerations:
  - The user's access level, access logs shall be reconciled on a monthly frequency or as agreed by IT team.
  - Redundant and unused user accounts shall be removed within 90 days: and
  - Authorisation for privileged access rights should be reviewed at frequent intervals (as per IT guidelines) by IT team.

### 8.2.19 Information Security in Supplier Relationship

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	Supplier Relationships Security	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> <li>Protection</li> </ul>

- Information security requirements for mitigating the risks associated with supplier's access to RENEWABLE ENERGY's assets shall be agreed with the supplier and documented in the form of agreements or contracts.
- RENEWABLE ENERGY shall identify the critical vendors based on confidential, integrity and availability of the services associated with the vendor.

### 8.2.20 Addressing information within Supplier Relationship

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Identify	Supplier Relationships Security	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> <li>Protection</li> </ul>

- All agreements with suppliers that access, process, communicate or manage organizations information or information processing facilities, or provide products or services shall have relevant security requirements embedded in them.
- The information security clauses in the supplier agreements shall be followed in adherence to the RENEWABLE ENERGY Third Party Management Security Policy

### 8.2.21 Managing Information Security in the ICT supply chain

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Identify	Supplier Relationships Security	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> <li>Protection</li> </ul>

- RENEWABLE ENERGY shall maintain security in line with Confidentiality, Integrity, and Availability for its ICT systems.
- Agreement with suppliers shall include requirements to address the information security risks associated with information and information processing facilities and product supply chain.
- A Business Continuity strategy shall be developed for all ICT systems.
- Periodic risk assessments or security assessments shall be performed to ensure the assurance of the security.

### 8.2.22 Monitoring, review and change management of supplier services

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Supplier Relationships Security	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> <li>• Defence</li> <li>• Information Security Assurance</li> </ul>

- Significant changes to supplier services (e.g., enhancement to networks, new technologies, new products, or newer versions, change of vendors, change of physical location etc.) shall be informed to the Information Security team.
- Such changes shall:
  - Consider criticality of business systems and processes involved; and
  - Be accompanied by re-assessment of risks.
- All the changes in the supplier services shall be performed in line with RENEWABLE ENERGY Change Management Policy.

### 8.2.23 Information security for use of cloud services

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Supplier Relationships Security	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> </ul>

- RENEWABLE ENERGY shall define Information Security requirements associated with the use of Cloud Services for all SaaS, IaaS, and PaaS platforms.
  - All the cloud infrastructure shall be hardened
  - There shall be adequate security controls to manage the access to the cloud infrastructure
  - The cloud infrastructure shall be integrated with the SIEM solution
  - A Vulnerability Assessment and Penetration Testing of the cloud infrastructure shall be performed, and the findings shall be mitigated. In case of SaaS platforms, the vendor shall be asked to share the VAPT reports.
  - RENEWABLE ENERGY shall follow secure coding guidelines for the applications which are going to be deployed on cloud.

### 8.2.24 Information security incident management planning and preparation

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Corrective</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Respond</li> <li>Recover</li> </ul>	<ul style="list-style-type: none"> <li>Governance</li> <li>Information Security Event Management</li> </ul>	Defence

- An incident management approach should document how RENEWABLE ENERGY shall establish responsibilities and procedures to ensure timely, effective, and orderly response to address weaknesses, events, and security incidents.
- The procedures for incident, event and weakness response planning shall need to be clearly defined in advance of an incident occurring and been approved by RENEWABLE ENERGY.
- Information Security weaknesses, both actual and suspected, shall be reported through different channels such as email, phone line, and intranet. In addition, users shall not test the existence of vulnerability in any information facility, system, or application.
- Centralized tracker shall be maintained of all reported Information Security weakness.

### 8.2.25 Information security incident management planning and preparation

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Detective</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Detect</li> <li>Respond</li> </ul>	Information Security Event Management	Defence

- The reported events shall be analyzed and classified as information security incidents, as per the defined criteria, on basis of their potential impact.
- If required, the Information Security team shall have the necessary rights to access the systems and applications for forensic purposes.

### 8.2.26 Response to Information security incidents

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Corrective</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Respond</li> <li>Recover</li> </ul>	Information Security Event Management	Defence

- The overall response to reported incidents shall include identification of corrective action(s).
- Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

### 8.2.27 Learning from Information security incidents

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Identify</li> <li>Protect</li> </ul>	Information Security Event Management	Defence

- Incident Response Team (IRT) in consultation with IT Team shall establish a Known Error Database (KEDB) for the information gained from the evaluation of all incidents. The KEDB shall be referred to for incident handling and as a learning source of incidents.

#### 8.2.28 Collection of evidence

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Corrective</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Detect</li> <li>• Respond</li> </ul>	Information Security Event Management	Defence

- As per the legal/contractual requirements, the evidence shall be collected during incident analysis, retained, and presented for relevant authorities for the high and medium incidents for which Root Cause Analysis (RCA) shall be conducted. The evidence shall be collected in a manner that does not destroy its evidentiary value. While collecting the evidence, the following shall be considered but not limited to:
  - Applicability of evidence: Whether the evidence can be used in a court of law; and
  - Weight of evidence: The quality and completeness of the evidence.

#### 8.2.29 Information Security during disruption

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>• <b>Preventive</b></li> <li>• <b>Corrective</b></li> </ul>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Protect</li> <li>• Respond</li> </ul>	Continuity	<ul style="list-style-type: none"> <li>• Protection</li> <li>• Resilience</li> </ul>

- The organization-wide Information security processes shall include Information Security requirements to help ensure that confidentiality, integrity, and availability of critical information assets shall be preserved even in the event of a business disruption or disaster.
- RENEWABLE ENERGY shall identify recovery guidelines that can be taken as baseline reference to classify critical systems and develop recovery and restoration plans.
- A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to information security; and
- In the absence of formal business continuity and disaster recovery planning, information security management shall assume that information security requirements remain the same in adverse situations, compared to normal operational conditions.

#### 8.2.30 ICT readiness for business continuity

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Corrective</b>	Availability	Respond	Continuity	Resilience

- RENEWABLE ENERGY shall ensure that an adequate framework is in place to prepare for, mitigate and respond to a disruptive event using personnel with necessary authority, experience, and competence.
- RENEWABLE ENERGY shall identify personnel with necessary responsibility, authority, and competence to manage an incident and maintain information security.
- RENEWABLE ENERGY shall ensure that documented plans, response, and recovery procedures are developed and approved, describing how RENEWABLE ENERGY will manage a disruptive event and maintain its information security at a predetermined management approved information security continuity objective.
- Information security controls for all systems shall be reviewed and verified. Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.
- Each calendar quarter, emergency contact information shall be validated and revised.
- The roles and responsibilities for both information systems contingency planning and information systems recovery shall be reviewed and updated annually.

### 8.2.31 Legal, statutory, regulatory, and contractual requirements

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Legal and Compliance	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> </ul>

- CDIO at RENEWABLE ENERGY shall be responsible for communicating changes to any of the above areas and additional security requirements.
- Necessary measures shall be taken to prevent the following types of content from being carried over the RENEWABLE ENERGY network in any form:
  - Objectionable, obscene, unauthorized content.
  - Content, messages, or communications infringing copyright, intellectual property etc.; and
  - If instances of such infringement are reported by the enforcement agencies, it shall be ensured that carriage of such material on the network is prevented immediately.
- Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

### 8.2.32 Intellectual Property Rights

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Identify	Legal and Compliance	Governance and Ecosystem

- Software used must be acquired from legitimate (known and reputable sources) to ensure copyright is not violated.
- Proof and evidence of ownership of licenses, master disks, manuals etc. shall be maintained.



- Controls shall be implemented to ensure maximum number of users permitted to use the software is not exceeded.
- Only authorized software and licensed products shall be installed; and
- Copying, storage, duplicating, converting to another format, extracting of electronic content (eBooks, media files, articles, reports etc.) must not violate copyright laws.

### 8.2.33 Protection of Records

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	<ul style="list-style-type: none"> <li>• Legal and Compliance</li> <li>• Asset Management</li> <li>• Information Protection</li> </ul>	Defence

- Important records required for meeting statutory and regulatory requirements shall be identified and their retention periods defined; and
- Each department having ownership of such records shall ensure that these records are protected from loss, destruction, unauthorized disclosure, and falsification.

### 8.2.34 Privacy and Protection of PII

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	<ul style="list-style-type: none"> <li>• Information and Protection</li> <li>• Legal and Compliance</li> </ul>	Protection

- RENEWABLE ENERGY shall ensure Privacy and protection of personally identifiable information as required by the relevant legislation and regulations.
- The customer data shall be masked on SAP application and a unique identifier shall be assigned to each customer.
- Access to customer database shall be restricted and shall only be accessed from intranet.

### 8.2.35 Independent Review of Information Security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>• <b>Preventive</b></li> <li>• <b>Corrective</b></li> </ul>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	Information Security Assurance	Governance and Ecosystem

- Audits of operational Information Systems shall be planned and performed at periodic intervals with the agreement of the Information Systems’ owner to minimize the risk of disruption to business processes.
- Independent audits of information security management system shall be performed as per the planned intervals or when significant changes occur.

### 8.2.36 Compliance with policies, rules, and standards for information security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	<ul style="list-style-type: none"> <li>• Legal and Compliance</li> <li>• Information Security Assurance</li> </ul>	Governance and Ecosystem

- Continued compliance with RENEWABLE ENERGY’s information security policies and procedures shall be maintained.
- Any detected non-compliances with the information security policies shall be investigated and corrective action shall be taken and reviewed.
- Such non-compliances as well as their preventive actions shall be further reported at the time of independent reviews.

### 8.2.37 Documented operating procedures

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>• <b>Preventive</b></li> <li>• <b>Corrective</b></li> </ul>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Protect</li> <li>• Recover</li> </ul>	<ul style="list-style-type: none"> <li>• Asset Management</li> <li>• Physical Security</li> <li>• System And Network Security</li> <li>• Application Security</li> <li>• Secure Configuration</li> <li>• Identity And Access Management</li> <li>• Threat And Vulnerability Management</li> <li>• Continuity</li> <li>• Information Security Event Management</li> </ul>	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> <li>• Defence</li> </ul>

- Operations shall ensure that all relevant documentation including software details is obtained from manufacturer/vendor/supplier.
- Following documents will be made available to the relevant people manning the operations:
  - Operations and Maintenance procedure or standard operating procedure (SOP) for all operational activities including security requirements.
  - Network diagrams to be maintained; and
  - Product and user manuals.

### 8.3 People Controls

#### 8.4.1 Screening

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Human Resource Security	Governance and Ecosystem

- Background verification checks shall be performed on all candidates considered for employment, in accordance with relevant laws, regulations and ethics.
  - The background verification checks process should ensure that all personal information is kept confidential, and the privacy of the prospective employees’ data is maintained in line with the Section [8.2.34](#) “Privacy and Protection of PII”
  - The organisation shall ensure that competent personnel are employed for performing duties assigned to them.

#### 8.4.2 Terms and Conditions of employment

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Human Resource Security	Governance and Ecosystem

- The terms and conditions of employment, signed by RENEWABLE ENERGY’s employees shall include the employee’s responsibilities for information security and related obligations, both during and after employment.
- All employees handling or accessing organizations information assets shall be liable for protecting the asset against unauthorized disclosure, modification and/ or destruction of information.

#### 8.4.3 Information security awareness, education, and training

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Human Resource Security	Governance and Ecosystem

- All employees shall be provided appropriate awareness training and regular updates in organizational policies and procedures.
- The initial security training and awareness program shall be conducted as part of the induction process; and

- The learning and development function shall conduct information security sessions for all the employees joining RENEWABLE ENERGY. Further, a refresher training shall be conducted for all employees.

#### 8.4.4 Disciplinary Process

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>Preventive</li> <li>Corrective</li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Protect</li> <li>Respond</li> </ul>	<ul style="list-style-type: none"> <li>Human Resource Security</li> </ul>	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> </ul>

- The organization shall ensure that a comprehensive disciplinary process is in place to handle all kind of security breaches and cases of misconduct. The disciplinary procedure shall be applicable to all employees and be enforced in event of an information security breach.

#### 8.4.5 Responsibilities after termination or change of employment

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Human Resource Security</li> <li>Asset Management</li> </ul>	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> </ul>

- The responsibilities for performing employment termination and/or change of employment shall be defined, documented, and clearly communicated. The respective Function Head shall sign off the exit letter for the employee exiting the organization.
- Employment agreement shall include the duties and responsibilities that shall be valid after the termination of such contract or agreement.
- Upon termination, all assets issued by RENEWABLE ENERGY to the employee shall be taken back and access rights on RENEWABLE ENERGY's information assets be removed.
- In the case of change of employment, the access rights and/or privileges granted to employees shall be formally reviewed and accordingly adjusted; and
- The academic or professional qualification certificates/records from the employee will be retained for a period of three years post the last working date.

#### 8.4.6 Confidentiality or Non-Disclosure Agreements

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	Confidentiality	Protect	<ul style="list-style-type: none"> <li>Human Resource Security</li> <li>Information Protection</li> <li>Supplier Relationship</li> </ul>	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> </ul>

- Non-disclosure agreements shall be defined, implemented, and maintained to address organization's information confidentiality/ non-disclosure requirements.

- All employees shall sign and comply with the non-disclosure agreement maintained by the Human Resource Team.
- All external consultants or the entity providing these services shall sign and comply with a non-disclosure agreement prior to any access to critical assets; and

#### 8.4.7 Remote Working

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Asset Management</li> <li>• Information Protection</li> <li>• Physical Security</li> <li>• System and Network Security</li> </ul>	Protection

- Employees shall be allowed to remotely connect to the organisation’s network/application using mobile devices (such as organisation issued laptops) to access the business information, only after successful identification and authentication.
- A secure communication channel between the remote user and the networks/Application of the organisation shall be provided.

#### 8.4.8 Information security event reporting

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Detective</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Detect	<ul style="list-style-type: none"> <li>• Information Security Event Management</li> </ul>	Defence

- Information Security events shall be reported through appropriate management channels as quickly as possible.
- Different channels such as email and phone line shall be implemented to facilitate reporting of Information Security event. All information security events will be logged in an information security incident tracker.
- Facility for monitoring (like Security Operations Centre) shall be setup for proactive monitoring of intrusions, attacks, and frauds.
- Users/Employees shall be educated on how to identify and report Information Security events.

## 8.4 Physical Controls

### 8.4.1 Physical Security Perimeters

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	Physical Security	Protection

- Security controls, such as perimeter fencing, entry control and manned reception desk, shall be used to protect areas that contain information and information processing facilities. The facility department should carry out the following activities to ensure physical security of the facility:
  - Identify and define perimeter of the facility.
  - Ensure that doors to public zones are equipped with the locking devices.
  - Deploy security personnel on round-the-clock basis.
- Combustible materials should be stored safely at a safe distance from secure areas.
- The RENEWABLE ENERGY offices shall be logically divided into different zones. Each zone shall have appropriate level of access restrictions and access authorization requirements. Areas containing critical IT equipment (such as the network room and the data centres) shall be designated as high security zones.

### 8.4.2 Physical entry

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Physical Security</li> <li>Identity and Access Management</li> </ul>	Protection

- Offices, buildings, and facilities should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Following controls should be implemented to ensure access to authorized personnel:
  - The facility department should issue badges for employees of RENEWABLE ENERGY and visitors. The badges issued should help in clear identification and differentiation between employee and visitor.
  - Deploying security guards round the clock.
  - Maintenance of entry / exit register for visitors.
  - Requirement for personnel to wear visible identification badge.
  - Declaration of belongings such as Laptop, personal devices like pen drive, hard disk, etc. at entry gate.
- All floor and office premises shall be accessed by using valid electronic card/access card which is issued by security team/IT team.
- Visitor or other third-party access to RENEWABLE ENERGY facility containing sensitive information shall be controlled by proper access controls, guards, receptionists, or other front office staff.
- Inventory of all types of visitor passes / badges should be maintained at security gate and all visitor passes / badges shall be verified on the daily basis against the inventory issued and received. Any discrepancy needs to be communicated to respective Business head.

### 8.4.3 Securing offices, rooms, and facilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Physical Security</li> <li>Asset Management</li> </ul>	Protection

- Security personnel should check all RENEWABLE ENERGY required rooms and facilities are locked after office hours.
- Facility department should ensure that photocopiers, printers, fax machines are located outside the secure area.
- Employees should ensure that they lock their cabins before they leave office.
- IT team shall ensure that any network switches and cabling racks/ distribution points in the office area are not physically accessible to people other than IT team.
- CCTV surveillance system shall store 180 days of recordings in secure areas entry and exit points.
- Fire drill / earthquake drills and training shall be provided to employees on periodic intervals.
- Fire drill record shall be maintained with the respective business departments. The records shall include time taken in evacuations of the building, learnings, etc. from the drill.

### 8.4.4 Physical Security Monitoring

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li><b>Preventive</b></li> <li><b>Detective</b></li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Protect</li> <li>Detect</li> </ul>	Physical Security	<ul style="list-style-type: none"> <li>Protection</li> <li>Defence</li> </ul>

- CCTV Cameras shall be installed to view and record access to the sensitive areas within and outside RENEWABLE ENERGY premises.
- Monitoring systems should be protected from unauthorized access to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.
- Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.

### 8.4.5 Protecting against physical and environmental threats

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> </ul>	Protect	Physical Security	Protection

	<ul style="list-style-type: none"> <li>• Availability</li> </ul>			
--	--	--	--	--

- RENEWABLE ENERGY shall ensure that critical information processing facilities are appropriately equipped and maintained with security controls to safeguard against external and environmental threats.
- Data center/ Hub room/ server room shall have proper/enough illumination to restrict any unauthorized access.
- Doors/ windows of server room/hub room/data center shall not be transparent.
- No water line/pipeline shall be through adjoining server room/ hub room/ data center.

#### 8.4.6 Working in secure areas

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Physical Security	Protection

RENEWABLE ENERGY shall ensure that:

- Employees and third-party resources shall be aware of the existence of, or activities within a secure area on a need to- know basis.
- All areas within its facilities shall be supervised to avoid safety breaches and to prevent opportunities for malicious activities.
- Vacant secure areas shall be physically locked and periodically reviewed.

#### 8.4.7 Clear desk and clear screen

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	Confidentiality	Protect	Physical Security	Protection

- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
- All confidential information shall be kept in a secure office or other location e.g., storage in a locked drawer, file cabinet etc.
- All incoming and outgoing mail points and unattended facsimile machines shall be protected from unauthorized physical and logical access.
- Personal computers, laptops and printers shall be left logged off or protected by a password, token, or similar user authentication mechanism when unattended.



- Application sessions shall be locked after 30 minutes of inactivity until a user’s password is re-entered.
- Users shall log off or lock their systems when leaving it unattended for any period.

#### 8.4.8 Equipment siting and protection

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Physical Security</li> <li>• Asset Management</li> </ul>	Protection

Equipment needs to be sited and protected to reduce the risks from environmental threats and hazards, and against unauthorized access. The siting of equipment will be determined by several factors including the size and nature of the equipment, it’s proposed use and accessibility and environmental requirements.

- All elements of systems including but not limited to servers, firewalls, hubs, routers etc. shall be physically located within a secure area.
- All equipment shall be sited to reduce the risk and opportunities for unnecessary and unauthorized access into work areas.
- Information processing facilities (laptops, desktops etc.) handling sensitive data should be protected using screen protectors to reduce the risk of information being viewed by unauthorized persons during their use.
- Information processing facilities like laptops are sited so they are securely stored when not in use and easily accessed when required.

#### 8.4.9 Security of assets off-premises

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Physical Security</li> <li>• Asset Management</li> </ul>	Protection

Security controls need to be applied to off-site assets, considering the different risks involved while working outside the RENEWABLE ENERGY’s premises.

RENEWABLE ENERGY shall ensure that:

- Any use of equipment or assets for information processing outside RENEWABLE ENERGY premises shall require authorization by Business head in consultation with IT head. Authorization for issue of mobile computing devices (includes laptops & smart phones) shall be considered as an authorization for use of equipment and assets for information processing outside RENEWABLE ENERGY premises.

- Employees shall store mobile and other hardware devices sensibly and securely when storing outside RENEWABLE ENERGY’s premises e.g., hotels, airports, etc. Equipment shall not be left unlocked, logged in or powered up without the employee being with the equipment.
- While traveling on road via taxi/ own car the employees are requested to secure office belongings, laptop etc. in car boot space.

#### 8.4.10 Storage Media

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Physical Security</li> <li>• Asset Management</li> </ul>	Protection

- RENEWABLE ENERGY shall ensure authorized disclosure, modification, removal, or destruction of information on storage media.
- Procedures for the secure reuse or disposal of storage media shall be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information.
- When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered.

#### 8.4.11 Supporting Utilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>• <b>Preventive</b></li> <li>• <b>Detective</b></li> </ul>	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Protect</li> <li>• Detect</li> </ul>	Physical Security	Protection

Equipment needs to be protected from power failures and other disruptions caused by failures in supporting utilities. For example, risks related to failing or faulty power supplies should be assessed and considered. This might include dual power supplies from different sub-stations; backup power generation facilities; regular testing of power provision and management, etc.

RENEWABLE ENERGY shall ensure that:

- All servers and network equipment shall be fitted with uninterruptible power supply systems, electrical power filters or surge suppressors that have been approved.
- All RENEWABLE ENERGY multi-user systems and communications facilities shall have alternative source of power, such a generator sets etc., so that normal business operations are sustainable even during extended period of unavailability of main power supply.

#### 8.4.12 Cabling Security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Availability</li> </ul>	Protect	Physical Security	Protection

RENEWABLE ENERGY shall ensure that:

- Power and telecommunications cabling carrying data supporting information services shall be protected from interception or damage.
- Cabling shall be physically protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas.
- Power cables should be segregated from communications cables to prevent interference.
- Cables should be protected using electromagnetic shield.
- Clearly identifiable cable and equipment markings should be used to minimize handling errors, such as accidental patching of wrong network cables.
- Installation of cables should be in such a way that it is not easily accessible.
- Shielded twisted pair (STP) cables should be used instead of unshielded twisted pair (UTP).

#### 8.4.13 Equipment Maintenance

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Physical Security</li> <li>Asset Management</li> </ul>	<ul style="list-style-type: none"> <li>Protection</li> <li>Resilience</li> </ul>

RENEWABLE ENERGY shall ensure that:

- All information systems equipment used for production processing shall be maintained in accordance with the supplier’s recommended service intervals and specifications, with any repairs and servicing performed only by qualified and authorized maintenance personnel.
- All hardware and software products shall be registered with the appropriate vendors for maintenance after RENEWABLE ENERGY staff takes delivery of new or upgraded information systems products.
- The annual maintenance contracts for all hardware and software products, if applicable, shall be monitored and reviewed after every year.
- Preventive maintenance shall be done and reviewed by relevant Business heads or IT head on predefined periods.

#### 8.4.14 Secure disposal or re-use of equipment

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	Confidentiality	Protect	<ul style="list-style-type: none"> <li>Physical Security</li> </ul>	Protection

			<ul style="list-style-type: none"> <li>Asset Management</li> </ul>	
--	--	--	--	--

All items of equipment including storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

RENEWABLE ENERGY shall ensure that:

- Equipment shall be disposed (transferred or scrapped) if:
  - The equipment has reached end of life.
  - The equipment does not suit the computing environment requirement and cannot be upgraded further to meet the same.
  - Equipment has gone faulty and cannot be repaired.
- Critical infrastructure equipment which needs to be disposed, such as servers, network, security equipment etc. shall be approved with valid justification by IT head. Exceptions to the same can be implemented based on the management approval.
- Any information that resides in the asset shall be removed from the equipment before disposal/transfer/scrapping.
- The list of equipment, which are being disposed, shall be removed, or deleted from asset list as well as from register books, if any.
- List of equipment disposed/ transferred/ scrapped shall be maintained separately by the IT team.
- Controls implemented to wipe information shall be commensurate with the classification of information on the storage media / systems.

***(For more details, please refer to Data Management Policy\_V5)***

- Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:
  - Hard disks: physical destroy, disk sanitization or shred platter.
  - Floppy disks: disintegrate, shred or melt, etc.
  - Tape media: demagnetize, shred, melt, etc.
  - USB drives and digital media: crush, melt, shred, etc.
  - Optical disks (CDs and DVDs): destroy optical surface, crush, shred, or melt, etc.

***(For more details, please refer to Media Management section in Backup and Restoration Policy\_V5)***

- Information or data shall be erased from equipment prior to disposal or re-use.
- Equipment shall be disposed in an environmentally sensitive manner, taking account of any recycling facilities provided by manufacturers, local authorities, or commercial organizations.

### 8.5.1 User endpoint devices

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Asset Management</li> <li>Information Protection</li> </ul>	Protection

- RENEWABLE ENERGY shall establish secure configuration and handling of user endpoint devices.
- All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures.
- A specific procedure considering legal, statutory, regulatory, contractual (including insurance) and other security requirements of RENEWABLE ENERGY should be established for cases of theft or loss of user endpoint devices.
- For the use of personal devices (BYOD) the personal usage and business use of the devices shall be segregated using end point device management tools to protect RENEWABLE ENERGY data on a private device

### 8.5.2 Privileged Access Rights

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Identity and Access Management</li> <li>• Information Protection</li> </ul>	Protection

The allocation and use of privileged access rights shall be restricted and controlled over RENEWABLE ENERGY systems and networks. The below mentioned points should be taken into considerations:

- Respective Business head shall approve privilege access rights for RENEWABLE ENERGY employees and notify the same to IT team.
- The RENEWABLE ENERGY system privileges of all users, systems, etc will be restricted based on the need to know.
- By default, all users shall be granted basic information systems services such as electronic mail, etc.
- All other system capabilities shall be provided through job profiles or by special request approved by the IT team in consultation with Business head; and
- The privileges for non RENEWABLE ENERGY employees shall be revoked immediately by the IT team when the requirement or the contract is over.

### 8.5.3 Information Access restrictions

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Identity and Access Management</li> <li>• Information Protection</li> </ul>	Protection

Access to RENEWABLE ENERGY information shall be tied to access control policy. Key considerations should include:

- Role-based access control.
- Levels of access.
- Read, write, delete, and execute permissions.
- Limiting output of information; and
- Physical and/or logical access controls to sensitive applications, data, and systems.

#### 8.5.4 Access to source code

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Identity and Access Management</li> <li>• Application Security</li> <li>• Secure Configuration</li> </ul>	Protection

- Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be controlled, to prevent the introduction of unauthorized functionality and to avoid unintentional changes.
- Where possible, program source libraries should not be kept in production systems.
- Support personnel should not have unrestricted access to program source libraries; and
- Relevant audit trails shall be maintained for accesses and changes to program source libraries.

#### 8.5.5 Secure Authentication

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Identity and Access Management	Protection

Secret authentication information is a gateway to access valuable assets. It typically includes passwords, encryption keys etc. the allocation of secret authentication information shall be controlled through a formal management process.

- Passwords used by the RENEWABLE ENERGY employees and those set/provisioned on systems, network devices shall meet complexity requirements.
- Users shall be educated to keep the passwords allocated to them confidential.

- When granting access to infrastructure or software(s), users shall be provided with a temporary or one-time password that meets the password complexity requirements. Users need to change this password at first login and shall be unique for each user; and
- Temporary passwords should be given to users in a secure manner such as through restricted emails to intended user.

### 8.5.6 Capacity Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>• <b>Preventive</b></li> <li>• <b>Detective</b></li> </ul>	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Availability</li> </ul>	<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> <li>• Detect</li> </ul>	<ul style="list-style-type: none"> <li>• Continuity</li> </ul>	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> </ul>

- Capacity management shall help identify and reduce inefficiencies associated with either under-utilized resources or customer demands not fulfilled and shall provide satisfactory service levels in a cost-efficient manner. This shall help ensure that all infrastructure components can perform all required functions, those components shall perform as efficiently as possible, and accommodate reasonable growth without being overly wasteful.
- Critical IT resources related to each of the business processes, which need to be provided with maximum availability, shall be identified by Management Committee. These can be:
  - Business Critical application(s).
  - Operating systems.
  - Databases.
  - Hardware (servers, PCs, storage devices).
  - Networking components (routers, switches, firewalls).
  - Data files; and
  - Network Connectivity.
- Critical parameters and their thresholds shall be monitored for all critical infrastructure elements and software(s) at periodic intervals to ensure required performance levels and availability.
- Capacity planning shall take account of new business and system requirements and current and projected trends in the organization’s information processing capabilities.
- The periodicity of capacity review shall be defined taking into consideration the criticality of the infrastructure element, lead time / costs to procure replacement, and the parameter being monitored.
- System tuning and monitoring shall be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time.
- Outcome of the monitoring activity shall:
  - Be used to take corrective actions (if required).
  - Help in root cause analysis (if required); and
  - Be used to make projections of future capacity requirements to reduce the risk of system overload.

### 8.5.7 Protection against malware

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>Preventive</li> <li>Detective</li> </ul>	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Identify</li> <li>Protect</li> <li>Detect</li> </ul>	Continuity	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> <li>Protection</li> </ul>

- Anti-malware tools shall be implemented to efficiently detect, prevent, and recover against Malwares.
- Appropriate protection shall be enforced so that the users cannot disable the Anti-virus check.
- Anti-virus software installed on gateway antivirus server and associated signature files and virus definitions shall be kept up to date.
- Use of unauthorized software shall be prohibited.
- E-mails, attachments, system files, download, and all removable media such as USB drives, or CD-ROMs shall be scanned and quarantined for malicious code before use.
- The auto run feature of CD, DVD or any other removable media shall be disabled on all systems.
- Updated and approved versions of anti-virus on windows systems, system firewalls, host Intrusion Prevention system/ intrusion detection system, scanning engines and other software shall be deployed. Signatures and virus-definitions of all such deployments shall be kept appropriately current.
- Controls shall be implemented to prevent malware files from being introduced into the organization’s infrastructure from external networks like Internet.
- Appropriate incident management process shall be put in place to recover from malicious code attacks.
- Malicious code incidents shall be reported and be dealt as per the Incident Management Procedure.
- Users shall report the results of virus scanning and removal activity to the system administrators.
- Any machine discovered to be infected by a virus shall immediately be disconnected from all networks. The machine shall not be reconnected to the network until IT system administration staff can verify that the virus has been removed; and
- Users and staff shall be educated and made aware of the dangers of malicious code and protection measures to be adhered.

### 8.5.8 Management of Technical Vulnerabilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Identify</li> <li>Protect</li> </ul>	Threat and Vulnerability Management	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> <li>Protection</li> <li>Defence</li> </ul>

- There shall be documented procedure for technical vulnerability management.



- Timely information about technical vulnerabilities in infrastructure elements and software(s) being used shall be obtained from trusted sources (e.g., through subscription to vendor security advisories).
- Timelines shall be defined for responding to identified / reported technical vulnerabilities.
- Information obtained regarding vulnerability shall be evaluated to assess risk to RENEWABLE ENERGY's/ infrastructure. The evaluation shall take into consideration:
  - Vendor reported criticality (e.g., high, medium, and low).
  - Likelihood of the vulnerability being exploited (e.g., existence of a known exploit or other malicious code that uses the vulnerability as an attack vector).
  - System criticality (e.g., the relative importance of the applications and data the system supports at RENEWABLE ENERGY); and
  - System exposure (e.g., proxy server vs. internal file server vs. application servers).
- The identified risk shall be categorized as per the severity of the risk (e.g., High, Medium, and Low).
- Appropriate measures shall be taken to address the associated risks. If the vulnerability cannot be addressed, controls shall be considered to reduce the impact of risk.
- If the vulnerability closure requires patch deployment, the patch must be tested in a test environment before deployment to production environment. The test environment should closely simulate the production environment and if possible, the test should verify the patch does not conflict with other software(s). The patch deployment must go through change management process with a rollback plan.
- The system should be checked to verify if the patch has not affected any of the existing functionality.
- For high-risk vulnerabilities, after applying the patch/solution, a check shall be performed to ensure that the vulnerability has been closed; and
- To assist with technical vulnerability management, inventory of Infrastructure elements and software assets shall be maintained.

### 8.5.9 Configuration Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Secure Configuration	Protection

- RENEWABLE ENERGY shall define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g., cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.
- Roles, responsibilities, and procedures should be in place to ensure satisfactory control of all configuration changes.
- Established configurations of hardware, software, services, and networks should be recorded and a log should be maintained of all configuration changes.
- Changes to configurations should follow the change management process.

### 8.5.10 Information Deletion

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	Confidentiality	Protect	<ul style="list-style-type: none"> <li>Information Protection</li> <li>Legal and Compliance</li> </ul>	Protection

- Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.
- A secure deletion method like degaussing or physical destruction shall be selected in accordance with the business requirements and taking into consideration relevant laws and regulations.
- Where cloud services are used, IT Head should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, RENEWABLE ENERGY should use it, or request that the cloud service provider delete the information.

### 8.5.11 Data Masking

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	Confidentiality	Protect	Information Protection	Protection

- While dealing with sensitive data or Personally Identifiable Data RENEWABLE ENERGY shall hide such data by using techniques such as data masking, pseudonymization or anonymization.
- Hash functions can be used to anonymize PII. To prevent enumeration attacks, they should always be combined with a salt function.

### 8.5.12 Data Leakage Prevention

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li><b>Preventive</b></li> <li><b>Detective</b></li> </ul>	Confidentiality	<ul style="list-style-type: none"> <li>Protect</li> <li>Detect</li> </ul>	Information Protection	<ul style="list-style-type: none"> <li>Protection</li> <li>Defence</li> </ul>

- RENEWABLE ENERGY shall
  - identify and classify information to protect against leakage (e.g., personal information, pricing models).
  - monitor channels of data leakage (e.g., email, file transfers, mobile devices, and portable storage devices).
  - act to prevent information from leaking (e.g., quarantine emails containing sensitive information).

- Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup.

### 8.5.13 Information Backup

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Corrective</b>	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Availability</li> </ul>	Recover	Continuity	Protection

- Backup solution shall be used to meet the business requirements and ensure availability of business-critical information, software(s), device configurations in case of emergencies.
- Relevant processes / procedures shall be created and followed to meet the business requirements. The process / procedures will cover:
  - Frequency for taking backup and testing of backup through a restoration process.
  - Data to be backed up.
  - Type of backup (incremental, differential, full).
  - Root Cause Analysis for such failure would be carried out as per the incident management procedure.
  - Instructions to restore in case of an actual disaster; and
  - Retention period for backup.
- Adequate controls shall be put in place to ensure protection of backup media. The environmental conditions for storing the backup media shall be in line with the specifications on environmental conditions for the backup media.
- The backup media shall be labelled to a consistent standard.
- Adequate controls shall be put in place to protect the information contained on back up media.
- Restoration testing shall be performed on regular basis to ensure effectiveness of backup tools; and
- The restored contents shall be verified against the tape for an exact match.

### 8.5.14 Redundancy of information processing facilities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	Availability	Protect	<ul style="list-style-type: none"> <li>• Continuity</li> <li>• Asset Management</li> </ul>	<ul style="list-style-type: none"> <li>• Protection</li> <li>• Resilience</li> </ul>

- RENEWABLE ENERGY shall identify business requirements for availability of information systems.
- Redundant components or architectures shall be considered wherever availability cannot be guaranteed using the existing systems architecture.
- Redundant information systems shall be tested to ensure the successful failover from one component to another: and
- Adequate redundancy has been provided for network links and network devices.

### 8.5.15 Logging

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Detective</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Detect	<ul style="list-style-type: none"> <li>Information Security Event Management</li> </ul>	<ul style="list-style-type: none"> <li>Protection</li> <li>Defence</li> </ul>

- Event logging activity affects information system performance, therefore, decision shall be made upon a risk assessment, to, which events require logging on a continuous basis and which events require logging in response to specific situations. Following minimum events shall be considered but not limited to:
  - Logins and logouts to systems and applications
  - Unsuccessful usage of user identification or authentication mechanisms.
  - Access violation and unsuccessful logon attempts.
  - Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing high impact file permissions, changing database object permissions and user password changes.
  - All system or application administrator actions.
  - Application process start-up, shutdown, or restart.
  - Application process abort, failure, or abnormal end, faults, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, disk space, or other resources) or hardware fault for critical applications.
  - Use of privileged accounts.
  - Administrator logons, changes to the administrator group, and account lockouts; and
  - System faults shall be logged in near real-time and corrective action shall be taken immediately by the IT Administrator/IT Team.
- IT Team shall ensure that systems are configured in such a way that the system administrator and system operator activities are logged. Event logs shall be captured and stored for administrator activities. It shall also be ensured that system administrator and operator do not edit /delete their logs. Logs shall include but not limited to:
  - The time at which an event (success or failure) occurred.
  - Information about the event or failure.
  - The user/service account involved.

### 8.5.16 Monitoring activities

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Detective</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Detect	<ul style="list-style-type: none"> <li>Information Security Event Management</li> </ul>	<ul style="list-style-type: none"> <li>Protection</li> <li>Defence</li> </ul>

- The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods.
- The monitoring system should be configured against the established baseline to identify anomalous behavior.

### 8.5.17 Clock Synchronisation

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Detective</b>	Integrity	<ul style="list-style-type: none"> <li>• Protect</li> <li>• Detect</li> </ul>	<ul style="list-style-type: none"> <li>• Information Security Event Management</li> </ul>	<ul style="list-style-type: none"> <li>• Protection</li> <li>• Defence</li> </ul>

- All systems, application and database servers shall have appropriate time and clock synchronization, wherever feasible. This shall be achieved by configuring a Network Time Protocol (NTP) environment to which all critical component like servers, network etc., shall synchronize time. To secure logs following shall be followed:
  - Access to logs shall be limited to authorized people, for review and analysis.
  - Backup of logs shall be taken on periodic basis; for critical system, database, and application the backup shall be taken at least on daily/weekly basis; and
  - Backup tapes or drives on which logs are getting backed up shall be secured against any unauthorized access.

### 8.5.18 Use of privileged utility programs

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• System and network security</li> <li>• Secure configuration</li> <li>• Application security</li> </ul>	Protection

- Access to RENEWABLE ENERGY’s local system control utilities shall be restricted and controlled.
- These system utilities shall be installed on local systems and shall be intended for use by IT to assist in resolving problems; and
- Remote control utilities for IT team personnel shall only be used after the IT team has informed the user of this capability and has received permission from the user to use them.

### 8.5.19 Installation of software on operational systems

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
--------------	---------------------------------	------------------------	--------------------------	------------------

<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Secure configuration</li> <li>Application security</li> </ul>	Protection
-------------------	--	---------	--	------------

- Installation of new software and changes to existing software on production systems shall be in line with change management policy to ensure:
  - Changes are authorized and made by authorized personnel only.
  - Production systems hold only approved code and not development code.
  - Implementation happens only after required level of testing.
  - System documentation is updated; and
  - Roll back plan is available.
- The risks of relying on unsupported software (software for which support has been ceased by the vendor) for business-critical applications shall be considered.

### 8.5.20 Network security

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li><b>Preventive</b></li> <li><b>Detective</b></li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Protect</li> <li>Detect</li> </ul>	System and network security	Protection

- Networks shall be adequately managed and controlled, to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
- Network based intrusion prevention/detection system shall be deployed to cover critical network segments within IT infrastructure as per the risks identified.
- Infrastructure elements and software(s) exposed to un-trusted or semi trusted networks/users (e.g., Internet facing systems, distributors, call centers, s etc.) shall be adequately protected by firewalls, intrusion prevention systems (IPSs), and limited connectivity.
- All internet facing systems shall be treated as semi-trusted systems.
- Any system deployed on the Internet must go through a thorough vulnerability check. All identified vulnerabilities must be closed or mitigated before the system is deployed on the Internet.
- All end user systems connecting to the RENEWABLE ENERGY's infrastructure must be hardened, patched, and installed with updated anti-malware software.
- Every connection to an external network terminated at a firewall.
- Firewalls do not have any rules that permit 'any' network, sub network, host, protocol, or port on any of the firewall.
- The firewall rule base treated as a sensitive information and is knowledge of the same restricted only to authorized officials in the IT team.

### 8.5.21 Security of Network services

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	System and network security	Protection

- The servers shall be implemented for a single primary function, wherever possible. This shall simplify configuration, thereby reducing the risk of configuration errors. In some cases, however, it may be appropriate to offer more than one service on a single host computer (e.g., database, DNS (Domain Name System), FTP (File Transfer Protocol) and HTTP (Hyper Text Transfer Protocol) services).
- All network servers shall be protected using strong passwords, and the passwords shall be managed as defined in the password policy of RENEWABLE ENERGY.
- The appropriate authority shall assess the security risks associated with enabling a network service to arrive at the security requirements.
- Any unused or unwanted network services shall be removed or disabled as per the relevant hardening documents.
- A documented list of services and ports required for the business purpose shall be maintained and updated regularly.
- If the business requires any services or ports to be enabled, they shall be enabled only after authorization and testing and implementation of mitigating controls to avoid misuse.

### 8.5.22 Segregation of Networks

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	System and network security	Protection

- Group of users, systems, applications shall be adequately segregated through creation of Virtual LANs, Zones based to prevent unauthorized access; and
- Appropriate logical segregation shall be done and Physical Security infrastructures through creation of zones. Traffic flows between different zones shall be documented.

### 8.5.23 Web filtering

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	System and network security	Protection

- RENEWABLE ENERGY shall reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material.

- RENEWABLE ENERGY shall identify the types of websites to which personnel should or should not have access. RENEWABLE ENERGY shall block access to the following types of websites:
  - websites that have an information upload function unless permitted for valid business reasons.
  - known or suspected malicious websites (e.g., those distributing malware or phishing contents).
  - command and control servers.
  - malicious website acquired from threat intelligence.
  - websites sharing illegal content.
- The IP addresses or domains of such malicious websites shall be blocked by the anti-malware.

#### 8.5.24 Use of cryptography

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	Secure configuration	Protection

- Encryption shall be adopted for information assets based on the criticality of information. Standard encryption technology would be deployed for encryption unless required by regulatory requirements.
- Users shall not employ encryption, digital signatures, or digital certificates for any business activity or business information without the written authorization of their department manager in consultation with IT head, the completion of proper training and having their systems configured by authorized personnel.
- Cryptographic algorithms shall be patched against any known technical vulnerabilities.
- Encryption shall be used for transportation of information by mobile devices and removable media devices or across communication lines.
- Key strength used shall be enough to prevent attacks targeted to breaking the cryptographic key (e.g., brute force attack on the cryptographic key).
- Roles and responsibilities shall be defined for key management and implementation of policy.

Key management that involves the generation, creation, protection, storage, exchange, replacement, and use of keys deals with many types of security liabilities beyond encryption, such as people and flawed policies. To mitigate such scenarios, the following standards need to be kept in mind when working with keys (wherever applicable):

- The secret key shall be secured by logically and physically securing the device on which the key is stored. Wherever possible, a Hardware Security Module (HSM) should be used to store the key.
- The shared secret key shall be accessible only by authorized personnel on a need-to-know basis.
- Keys shall be revoked and generated afresh in case of suspected compromise.



- Audit trails of key management activities shall be stored and protected.
- Internal Certification Authority systems shall be managed securely with appropriate physical and logical controls.
- Backed up keys shall be protected from physical and environmental threats.
- Cryptographic keys shall be destroyed in a secure manner when they are no longer required for both hardware and software keys.

### 8.5.25 Secure Development Lifecycle

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Application Security</li> <li>• System and Network Security</li> </ul>	Protection

- Secure development Policy shall be documented.
- Secure development environment for development of software and systems.
- Access to this environment shall be restricted and monitored.
- The devices shall be hardened to protect against exploitation.
- A secure development environment consists of people, process, and technology associated with system development and integration efforts that cover the entire secure development lifecycle. RENEWABLE ENERGY shall assess the risk considering the following but not limited to:
  - The sensitivity of the data to be processed, stored, and transmitted by the system.
  - Applicable external and internal requirements.
  - Security policies already implemented by RENEWABLE ENERGY that support system development.
  - The trustworthiness of the personnel working in the environment.
  - The degree of outsourcing associated with system development.
  - The need for segregation between different development environments.
  - Control of access to the development environment.
  - Monitoring of the change to the environment and the code stored within.
  - Backups are stored at secure offsite locations; and
  - Control over the movement of data from development to the production environment.

### 8.5.26 Application Security Requirements

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Application Security</li> <li>• System and Network Security</li> </ul>	Protection

- RENEWABLE ENERGY shall ensure all information security requirements are identified and addressed when developing or acquiring applications.
- Application security requirements should be identified and specified.
- These requirements shall be determined through a risk assessment.
- Application security requirements should include, as applicable:
  - level of trust in identity of entities [e.g., through authentication].
  - identifying the type of information and classification level to be processed by the application.
  - need for segregation of access and level of access to data and functions in the application.
  - resilience against malicious attacks or unintentional disruptions [e.g., protection against buffer overflow or structured query language (SQL) injections].
  - legal, statutory, and regulatory requirements in the jurisdiction where the transaction is generated, processed, completed, or stored.
  - need for privacy associated with all parties involved.
  - the protection requirements of any confidential information.
  - protection of data while being processed, in transit and at rest.
  - need to securely encrypt communications between all involved parties.
  - input controls, including integrity checks and input validation.
  - automated controls (e.g., approval limits or dual approvals).
  - output controls, also considering who can access outputs and its authorization.
  - restrictions around content of "free-text" fields, as these can lead to uncontrolled storage of confidential data (e.g., personal data).
  - requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements.
  - requirements mandated by other security controls (e.g., interfaces to logging and monitoring or data leakage detection systems).
  - error message handling.

#### 8.5.27 Secure system architecture and engineering principles

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• Application Security</li> <li>• System and Network Security</li> </ul>	Protection

- Secure information system engineering principles shall be designed into all architecture layers:
  - Business layer – e.g., based on user authentication level; only particular users can see personal data.
  - Data layer – e.g., only logging in with a strong database password for database maintenance activities is allowed.
  - Applications – e.g., application encryption is used for data export and import; and
  - Technology – e.g., open-source software and state-of-the-art hardware and network infrastructure provided by selected vendors are used.

### 8.5.28 Secure coding

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Application Security</li> <li>System and Network Security</li> </ul>	Protection

- RENEWABLE ENERGY shall establish organization-wide processes to provide good governance for secure coding. A minimum secure baseline should be established and applied.
- Such processes and governance should be extended to cover software components from third parties and open-source software.
- Secure coding principles should be used both for new developments and in reuse scenarios. These principles should be applied to development activities both within the organization and for products and services supplied by the organization to others.

### 8.5.29 Security testing in development and acceptance

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Identify	<ul style="list-style-type: none"> <li>Application Security</li> <li>Information Security Assurance</li> <li>System and Network Security</li> </ul>	Protection

- Acceptance criteria for new information systems and information processing facilities, upgrades and new versions shall be defined. Appropriate testing of the systems shall be carried out during development before moving to production; and
- Security clearance shall be obtained from the application owner and IT Team. IT head shall sign off before any new information systems, upgrades or new versions are accepted.

### 8.5.30 Outsourced development

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<ul style="list-style-type: none"> <li>Preventive</li> <li>Detective</li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	<ul style="list-style-type: none"> <li>Identify</li> <li>Protect</li> <li>Detect</li> </ul>	<ul style="list-style-type: none"> <li>Application Security</li> <li>Information Security Assurance</li> <li>System and Network Security</li> </ul>	<ul style="list-style-type: none"> <li>Governance and Ecosystem</li> <li>Protection</li> </ul>

- For the customized software developed by third parties, arrangements pertaining to licensing, legal and regulatory requirements, including data protection, ownership of the entire source code by RENEWABLE ENERGY, intellectual property rights and copyright, and compliances shall be documented in the contract between RENEWABLE ENERGY and the third parties.
- The contract shall include the right to audit the quality and accuracy of software development and testing. Such software code shall have arrangements in the event of failure of the third party not complying with information security requirements; and
- A Non-Disclosure Agreement (NDA) with RENEWABLE ENERGY shall be signed by all third-party employees (i.e., third parties, contractors, application developers, testers etc.) having access to RENEWABLE ENERGY’s resources. The NDA shall mandate that the third-party resources should not disclose any information related to RENEWABLE ENERGY. The third-party shall ensure that they read, accept, and sign the Non-Disclosure Agreement provided by RENEWABLE ENERGY.

### 8.5.31 Separation of development, test, and production environments

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
Preventive	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Application Security</li> <li>System and Network Security</li> </ul>	Protection

- Development, test and operational (production) environments shall be separated to reduce the risks of unauthorized access or changes to the operational system.
- Test environment should emulate the production environment wherever applicable or as closely as possible; and
- Development tools like compilers, editors shall not be available on production servers.

### 8.5.32 Change Management

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>Application Security</li> <li>System and Network Security</li> </ul>	Protection

- The scope of change shall be clearly articulated and documented. Changes shall be classified, recorded, validated, approved, and prioritized.
- All change requests shall include business benefits, risk assessment, impact analysis and roll back plan details. All accepted change requests shall be tested, verified, and approved before the release.
- The change request shall be analyzed by internal IT team or external agency and a detail timeline with cost will be projected for approval. Any major cash outflow for the change request must be approved by the Senior Management Team. Any scheduled change request may be deferred for an indefinite period for reasons of non-availability of adequate resources or if the change impacts any other business process.
- Depending upon the nature of the change request, periodic reviews shall be conducted to ensure that the impact of the change is adequately understood and addressed. This will also ensure successful completion of the change request.
- A change management log must be maintained for all changes. The log must contain, but is not limited to:
  - Date of submission and date of change.
  - Owner contact information.
  - Nature of the change.
  - Indication of success or failure; and
  - Fall Back Plan (If failure).
- All changes shall be planned, scheduled, and communicated to all respective stakeholders. A review board shall review the changes periodically to assess the trends and improvement areas. The findings of the review board meetings shall be documented and published.
- All procedures and activities will be planned and executed in accordance with the local and/or national regulatory requirements, with appropriate approvals wherever deemed necessary; and
- Wherever external agencies are involved, the relevant Change Request (CR) document shall be raised by the agency will be treated as the final CR document.

### 8.5.33 Test Information

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> </ul>	Protect	Information Protection	Protection

- Test data used shall be treated like the operational data. Operational data shall be sanitized before being used for test purposes. It shall be always ensured that ‘Confidential’ information is not utilized during testing (if possible).
- Operational information shall be erased from a test environment immediately after the testing is complete.
- Access to test environment shall be given to only those personnel who are involved in testing the entire application only.
- Segregation of duties shall be applied where the knowledge and/or privileges are needed to complete a process and divided among multiple users so that no single one can perform or controlling. The principles that shall be applicable to segregation of duties are but not limited to:
  - Sequential separation, when an activity is broken into steps performed by different persons e.g., development (by development team) and testing (by testers) of an application.
  - Individual separation, when at least two persons must approve an activity before it is done e.g., functional lead/ business module lead approval followed by development lead for the finalization of application development feasibility.
  - Spatial separation, when different activities are performed in different locations e.g., Teams at various locations working on a common application; and
  - Factorial separation, when several factors contribute to activity completion e.g., two-factor access authentication.
- System integration testing shall be carried out to verify the behavior of the complete system. It shall be tested to conduct on a complete, integrated system to evaluate the system's compliance with its specified requirement.
- System integration testing (SIT) shall be performed to verify the interactions between the modules of a software system. It shall deal with the verification of the high and low-level software requirements specified in the Software Requirements Specification/Data and the Software Design Document.
- User acceptance testing (UAT) shall be performed by the end user to verify/accept the software system before moving the software application to the production environment. UAT shall be done in the final phase of testing after functional, integration and system testing are done; and
- This testing shall play an important role in validating if all the business requirements are fulfilled before releasing the final software product. The use of live data and real use cases shall make this testing an important part of the release cycle.

#### 8.5.34 Protection of Information Systems during audit testing

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> </ul>	Protect	<ul style="list-style-type: none"> <li>• System and network security</li> <li>• Information Protection</li> </ul>	<ul style="list-style-type: none"> <li>• Governance and Ecosystem</li> <li>• Protection</li> </ul>

- Relevant precautions shall be taken to protect the Information Systems and data from damage or disruptions because of the audit. The following guidelines shall be observed:
  - agreeing audit requests for access to systems and data with appropriate management.
  - agreeing and controlling the scope of technical audit tests.
  - limiting audit tests to read-only access to software and data. If read-only access is not available to
  - obtain the necessary information, executing the test by an experienced administrator who has the necessary access rights on behalf of the auditor.
  - if access is granted, establishing, and verifying the security requirements (e.g., antivirus and patching) of the devices used for accessing the systems (e.g., laptops or tablets) before allowing the access.
  - only allowing access other than read-only for isolated copies of system files, deleting them when the audit is completed, or giving them appropriate protection if there is an obligation to keep such files under audit documentation requirements.
  - identifying and agreeing on requests for special or additional processing, such as running audit tools.
  - running audit tests that can affect system availability outside business hours.
  - monitoring and logging all access for audit and test purposes.

**Annexure -1 CEA Detail Guidelines**

**File No.CEA-CH-13-12/4/2021-IT Division**




**भारत सरकार  
Government of India  
विद्युत मंत्रालय  
Ministry of Power  
केन्द्रीय विद्युत प्राधिकरण  
Central Electricity Authority  
सूचना प्रौद्योगिकी एवं साइबर सुरक्षा प्रभाग  
Information Technology & Cyber Security Division**

: CEA (Cyber Security in Power Sector) Guidelines, 2021.

CEA is mandated to prepare 'Guidelines on Cyber Security' in Power Sector under the provision of regulation (10) of the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019. Guidelines on Cyber Security in Power Sector incorporating the cardinal principles has been prepared by CEA. In compliance to the provision of the above regulation, **CEA (Cyber Security in Power Sector) Guidelines, 2021** are issued for compliance by all entities listed in the clause 2.3 (Applicability of the Guidelines) of the guidelines.

**Encl:** Guidelines on Cyber Security



07/10/21  
(V.K. Mishra)  
Secretary CEA



## CEA (Cyber Security in Power Sector) Guidelines, 2021

### 1.0 Background

- 1.1 Cyber intrusion attempts and Cyber-attacks in any critical sector are carried out with a malicious intent. In Power Sector it's either to compromise the Power Supply System or to render the grid operation in-secure. Any such compromise, may result in mal-operations of equipments, equipment damages or even in a cascading grid brownout/blackout. The much hyped air gap myth between IT and OT Systems now stands shattered. The artificial air gap created by deploying firewalls between any IT and OT System can be jumped by any insider or an outsider through social engineering. Cyber-attacks are staged through tactics & techniques of Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Command and Control, Exfiltration. After gaining the entry inside the system through privilege escalation, the control of IT network and operations of OT systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/State sponsored or non-sponsored adversaries and cyber attackers to design more sinister and advanced cyber-attacks.
- 1.2 Government of India has set up the Indian Computer Emergency Response Team (CERT-In) for Early Warning and Response to cyber security incidents and to have collaboration at National and International level for information sharing on mitigation of cyber threats. CERT-In regularly issues advisories on safeguarding computer systems and publishes Security Guidelines which are widely circulated for compliances. All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct cyber security audit of their entire Cyber Infrastructure including websites at regular interval through CERT-In empanelled Auditors so as to identify gaps and appropriate corrective actions to be taken in cyber security practices. CERT-In extends supports to enable Responsible Entity in conducting cyber security mock drills and in assessment of their preparation to withstand cyber-attacks. The Responsible Entity must submit Reports of Cyber Audit of cyber security controls, architecture, vulnerability management, network security and periodic cyber security drills to sectoral CERT as well as CERT-In. Team of experts shall review these reports and shortcomings if any in the compliances shall be flagged by them. CERT-In on regular basis also conducts workshops and training programs to enhance Cyber awareness of all Stakeholders.
- 1.3 Ministry of Power has created 6(six) sectoral CERTs namely Thermal, Hydro, Transmission, Grid Operation, RE and Distribution for ensuring cyber security in Indian Power Sector. Each Sectoral CERT has prepared their sub-sector specific model Cyber Crisis Management Plan(C-CMP) for countering cyber-attacks and cyber terrorism. Each Sectoral CERT has circulated their model C-CMPs for preparation and implementation of organization specific C-CMP by each of their Constituent Utility.

All Responsible Entities, Service Providers, Equipment Suppliers/Vendors and Consultants engaged in Power Sector are equally responsible for ensuring cyber security

of the Indian Power Supply System. They are to act timely upon each threat intelligence, advisories and other inputs received from authenticated sources, for continuous improvement in their cyber security posture.

- 1.4 In the current Indian scenario though many cyber security directives and guidelines exists, but none of them are power sector specific. Ministry of Power has directed CEA to prepare Regulation on Cyber Security in Power Sector. And as an interim measures CEA has been directed to issue Guideline on Cyber Security in Power Sector, under the provision of Regulation 10 on Cyber Security in the “Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019”.
- 1.5 The Guidelines on Cyber Security, in the form of Articles written below, requires mandatory Compliance by all Responsible Entities. The Guidelines shall come into effect from the date of issue by Central Electricity Authority, New Delhi.
- 2.0 Hereby the Guidelines on Cyber Security are drawn in the form of Articles for compliance by the Requester as well as User under the following provision of Regulation 10 on Cyber Security, in the “Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019”.

***“The requester and the user shall comply with cyber security guidelines issued by the Central Government, from time to time, and the technical standards for communication system in Power Sector laid down by the Authority.”***

- 2.1 Objective of issuing Guideline:
  - a) Creating cyber security awareness
  - b) Creating a secure cyber ecosystem,
  - c) Creating a cyber-assurance framework,
  - d) Strengthening the regulatory framework,
  - e) Creating mechanisms for security threat early warning, vulnerability management and response to security threats,
  - f) Securing remote operations and services,
  - g) Protection and resilience of critical information infrastructure,
  - h) Reducing cyber supply chain risks,
  - i) Encouraging use of open standards,
  - j) Promotion of research and development in cyber security,
  - k) Human resource development in the domain of Cyber Security,
  - l) Developing effective public private partnerships, m) Information sharing and cooperation
  - n) Operationalization of the National Cyber Security Policy

2.2 Within the text of these Articles, '**Responsible Entity**' shall mean all:

- a) Transmission Utilities as well as Transmission Licensees,
- b) Load despatch centres (State, Regional and National),
- c) Generation utilities (Hydro, Thermal, Nuclear, RE),
- d) Distribution Utilities
- e) Generation Aggregators,
- f) Trading Exchanges,
- g) Regional Power Committees, and

2.3 Applicability:

All Responsible Entities as well as System Integrators, Equipment Manufacturers, Suppliers/Vendors, Service Providers, IT Hardware and Software OEMs engaged in the Indian Power Supply System.

2.4 **Scope:**

2.4.1 **Control Systems for System Operation and Operation Management.**

- a) Grid Control and Management Systems,
- b) Power Plant Control Systems,
- c) Central Systems used to monitor and control of distributed generation and loads e.g. virtual power plants, storage management, central control rooms for hydroelectric plants, photovoltaic/wind power installations,
- d) Systems for fault management and work force management,
- e) Metering and measurement management systems,
- f) Data archiving systems,
- g) Parameterisation, configuration and programming systems,
- h) Supporting systems required for operation of the above mentioned systems,

2.5 Communication System.

- a) Routers switches and firewalls,
- b) Communication technology-related network components,
- c) Wireless digital systems.
- d) Control Centre to Control Centre Communications for data exchange on ICCP.  
(IEC 61850/60850-5/TASE.2/)

2.6 Secondary, Automation and Tele control technologies

- a) Control and Automation components,
- b) Control and field devices,
- c) Tele control devices,

- d) Programmable logic controllers / Remote Terminal Units, including digital sensor and actuators elements,
- e) Protection devices,
- f) Safety components,
- g) Digital measurement and metering installations,
- h) Synchronisation devices,
- i) Excitation Systems,

### 3.0 Definition of Terms:

1. **Access Management:** shall mean set of policies and procedures of the Responsible Entity for allowing Personnel, devices and IoT to securely perform a broad range of operational, maintenance, and asset management tasks either on site or remotely as laid down in Clause 5.2.5 of IS 16335.
2. **Accreditation:** shall mean the process of verifying that an organisation is capable of conducting the tests and assessments against a product/process that are required to be certified.
3. **Accreditation Body:** shall mean an organisation that has been accredited to verify the credentials and capabilities of the organisations that wish to become a certification body.
4. **Act:** shall mean the Information Technology Act, 2000 (21 of 2000)
5. **Asset:** shall mean anything that has value to the organization.
6. **Certification:** shall mean the process of verifying that a product has been manufactured in conformance with a set of predefined standards and/or regulations by an organisation, that is accredited to conduct the certification process
7. **Certification Body:** shall mean an organisation that has been accredited by an accreditation body to certify products / process against a certification scheme.
8. **Certification Scheme:** shall mean the processes, paperwork, tools, and documentation that define how a product or manufacturer is certified
9. **Chief Information Security Officer:** shall means the designated employee of Senior management level directly reporting to Managing Director/Chief Executive Officer/Secretary of the Responsible Entity, having knowledge of Information Security and related issues, responsible for cyber security efforts and initiatives including planning, developing, maintaining, reviewing and implementation of Information Security Policies
10. **Critical Assets:** shall mean the facilities, systems and equipment which, if destroyed, degraded or otherwise declared unavailable, would affect the reliability or operability of the Power Supply System.
11. **Critical System:** shall mean cyber assets essential to the reliable operation of critical asset. Critical System consists of those cyber assets that have at least one of the following characteristics:
  - a) The cyber asset uses a routable protocol to communicate outside the electronic security perimeter.
  - b) The cyber asset uses a routable protocol within a control centre.
  - c) The cyber asset is dial-up accessible.
12. **Critical Information Infrastructure:** shall mean Critical Information Infrastructure as defined in explanation of sub-section (1) of Section 70 of the Act.

13. **Cyber Assets:** shall mean the programmable electronic devices, including the hardware, software and data in those devices that are connected over a network, such as LAN, WAN and HAN.
14. **Cyber Crisis Management Plan:** shall mean a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad-based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical processes.
15. **Cyber Security Breach:** shall mean any cyber incident or cyber security violation that results in unauthorized or illegitimate access or use by a person as well as an entity, of data, applications, services, networks and/or devices through bypass of the underlying cyber security protocols, policies and mechanisms resulting in the compromise of the confidentiality, integrity or availability of data/information maintained in a computer resource or cyber asset.
16. **Cyber Security Incident:** shall mean any real or suspected adverse cyber security event that violates, explicitly or implicitly, cyber security policy of Responsible Entity resulting in unauthorized access, denial of service or disruption, unauthorized use of computer resource for processing or storage of information or changes to data or information without authorization, leading to harm to the power grid or its critical sub-sectoral elements Generation, Transmission and Distribution.
17. **Cyber Security Policy:** shall mean documented set of business rules and processes for protecting information, computer resources, networks, devices, Industrial Control Systems and other OT resources.
18. **Electronic Security Perimeter:** shall mean the logical border surrounding a network to which the Cyber Systems of Power Supply System are connected using a routable protocol.
19. **Information Security Division:** shall mean a division accountable for cyber security and protection of the Critical System of the Responsible Entity.
20. **Protected System:** shall mean any computer, computer system or computer network of the Responsible Entity notified under section 70 of the Act, in the official gazette by appropriate Government.
21. **Security Architecture:** shall mean a framework and guidance to implement and operate a system using the appropriate security controls with the goal to maintain the system's quality attributes like confidentiality, integrity, availability, accountability and assurance.
22. **Vulnerability:** shall mean intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence
23. **Vulnerability Assessment:** shall mean a process of identifying and quantifying vulnerabilities

#### 4.0 Standards

Reference	Description
ISO/IEC 15408	Common Criteria Certification Standard
ISO/IEC 17011	General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
ISO/IEC 21827	Systems Security Engineering - Capability Maturity Model (SSE-CMM)
ISO/IEC 24748-1	Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management.
ISO 27001/2	Information Security Management
ISO/ IEC 27019	Information technology — Security techniques — Information Security controls for the energy utility industry
ISO/IEC 61508	Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
IEC	
	61850 Communication networks and systems for power utility automation
IEC 62351	Standards for Securing Power System Communications
IEC 62443	Cyber Security for Industrial Control Systems
IS 16335	Power Control Systems – Security Requirements.

## 5.0 Abbreviations

Abbreviations	Description
a) BES	Bulk Electric System
b) CDAC	Centre for Development of Advanced Computing
c) CEA	Central Electricity Authority
d) CERC	Central Electricity Regulatory Commission
e) CERT	Computer Emergency Response Team
f) CERT-In	Indian Computer Emergency Response Team
g) CII	Critical Information Infrastructure
h) CISO	Chief Information Security Officer
i) CSK	Cyber Swachhhta Kendra
j) COTS	Commercial off-the Shelf
k) ESP	Electronic Security perimeter
l) ICS	Industrial Control Systems
m) ICT	Information and Communications Technology
n) IEC	International Electro Technical Commission
o) ISAC	Information Sharing and Analysis Centre
p) ISD	Information Security Division
q) ISO	International Organization for Standardization
r) ISMS	Information Security Management System
s) IT	Information Technology
t) FAT	Factory Acceptance Test
u) NABL	National Accreditation Board for Testing and Calibration Laboratories
v) NCIIPC	National Critical Information Infrastructure Protection Centre
w) NLDC	National Load Dispatch Centre
x) NPTI	National Power Training Institute
y) NSCS	National Security Council Secretariat
z) OEM	Original Equipment Manufacturer
aa) OT	Operational Technology
bb) RLDC	Regional Load Dispatch Centres
cc) SAT	Site Acceptance Test
dd) SERC	State Electricity Regulatory Commission
ee) SCADA	Supervisory Control and Data Acquisition Systems
ff) SIEM	Security Information and Event Management
gg) SLA	Service Level Agreement
hh) SLDC	State Load Dispatch Centre
ii) QCI	Quality Council of India

## CEA (Cyber Security in Power Sector) Guidelines, 2021

### Article 1. Cyber Security Policy.

#### **a. Cardinal Principles: The Responsible entity will strictly adhere to following cardinal principles while framing cyber security policy:**

- i. There is hard isolation of their OT Systems from any internet facing IT system.
  - ii. May keep only one of their IT systems with internet facing at any of their site/location if required which is isolated from all OT zones and kept in a separate room under the security and control of CISO.
  - iii. Downloading/Uploading of any data/information from their internet facing IT system is done only through an identifiable whitelisted device followed by scanning of both for any vulnerability/malware as per the SOP laid down and for all such activities digital logs are maintained and retained under the custody of CISO for at least 6 months. The log shall be readily to carry out the forensic analysis if asked by investigation agency.
  - iv. List of whitelisted IP addresses for each firewall is maintained by CISO and each firewall is configured for allowing communication with the whitelisted IP addresses only.
  - v. Communication between OT equipment/systems is done through the secure channel preferably of POWERTEL through the fibre optic cable. Security configuration of the communication channel is also to be ensured.
  - vi. All ICT based equipment/system deployed in infrastructure/system mandatorily CII are sourced from the list of the "Trusted Sources" as and when drawn by MoP/CEA.
- b. The Responsible Entity shall be ISO/IEC 27001 certified (including sector specific controls as per ISO/IEC 27019).
  - c. The Responsible Entity shall have a Cyber Security Policy drawn upon the guidelines issued by NCIIPC.
  - d. The Responsible 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 Board of Directors.
  - e. The process of Access Management for all Cyber Assets owned or under control of the Responsible Entity shall be detailed in the Cyber Security Policy.
  - f. The Cyber Security Policy shall leverage state-of-art cyber security technologies and relevant processes at multiple layers to mitigate the cyber security risks.
  - g. The Responsible Entity shall be solely responsible to get Cyber Security Policy implemented through its Information Security Division (ISD).
  - h. 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 allowed only after an approval of provisions of compensatory control(s) to mitigate



residual cyber security risks.

- i. The CISO shall record the exemptions sought in statement of applicability controls, while getting the ISO 27001 certified. All exemptions and its justification need to be in conformance with Cyber Security Policy of the Responsible Entity.
- j. The Responsible Entity shall allocate sufficient Annual budget for enhancing cyber security posture, enhanced year over year.
- k. The Responsible Entity shall work in collaboration with other Industry Stakeholders as well as Academia to promote R&D activity in the domain of cyber security.
- l. The Responsible Entity shall ensure that cyber security issues are taken up as agenda items in their Board meetings once in every three months.

#### Article 2 Appointment of CISO.

- a) The Responsible Entity shall mandatorily appoint a CISO and shall confirm to qualification, if any, **laid** by Quality Council of India (QCI). In absence, the work of CISO shall be looked upon by Alternate CISO. In case qualification for appointment of Alternate CISO has been relaxed for reasons recorded thereof, Alternate CISO has to mandatorily acquire the minimum required cyber security skill sets within six months from the date of his appointment.
- b) The Responsible Entity shall regularly update details of CISO and Alternate CISO, with the Sectoral CERT, as well as on ISAC-Power Portal.
- c) Roles and Responsibility of CISOs shall be as laid by CERT-In and ring-fenced to ensure cyber security of the Cyber Assets of the Responsible Entity.

#### Article 3: Identification of Critical Information Infrastructure (CII).

- a) The Responsible Entity shall submit to NCIIPC through Sectoral CERT, details of Cyber Assets which uses a routable protocol to communicate outside the Electronic Security Perimeter drawn by the Responsible Entity or a routable protocol within a control centre and dial-up accessible Cyber Assets, within 30 days from the date of their commissioning in the System.
- b) The Responsible Entity shall submit details of Critical Business Processes and underlying information infrastructure along with mapped impact and Risk Profile to NCIIPC and shall get their CIIs identified in consultation with NCIIPC. The process of the notification/declaration by Appropriate Government shall follow thereafter.
- c) The Responsible Entity shall review their declared/notified CIIs at least once a year to examine changes if any in the functional dependencies, protocols and technologies or upon any change in security architecture. The Responsible Entity shall review their declared/notified CIIs once in every 6 months, in case if NCIIPC has directed them to constitute an Information Security Steering Committee.
- d) The Responsible Entity shall ensure that all cyber assets of their identified/notified

CII's are recorded in the asset register and considered for risk assessment as well as for finalization of controls in statement of applicability.

#### Article 4. Electronic Security Perimeter

- a) The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all Access Points to the perimeter(s).
- b) The Responsible Entity shall follow procedure of identifying "Electronic Security Perimeter" in case of distributed and/or hybrid information infrastructure, as per IEC 62443 / IS16335 (as amended from time to time).
- c) The Responsible Entity shall ensure that every Critical System resides within an Electronic Security Perimeter.
- d) The Responsible Entity shall perform a cyber-Vulnerability Assessment of each electronic Access Points to the Electronic Security Perimeter(s) at least once in every 6 (six) months and/or after any change in Security Architecture.
- e) The Responsible Entity shall ensure that all critical, high and medium vulnerabilities identified as a result of cyber Vulnerability Assessment shall be closed and verified for the effective closure.

#### Article 5. Cyber Security Requirements

- a) The Responsible Entity shall have an Information Security Division (ISD), headed by CISO.
- b) The Responsible Entity shall ensure that the ISD must be functional on 24x7x365 basis and is manned by sufficient numbers of Engineers having valid certificate of successful completion of course on cyber security of Power Sector from the Training Institutes designated by CEA.
- c) The Responsible Entity shall ensure that ISD
  - 1) has on-boarded Cyber Swachhta Kendra(CSK) of CERT-In, if they have public IPs.
  - 2) has timely acted upon the advisories, guidelines and directive of NCIIPC, CSK, CERT-In and Sectoral CERTs,
  - 3) has deployed an Intrusion Detection System and Intrusion Prevention System capable of identifying behavioural anomaly in both IT as well as OT Systems.
  - 4) shares reports on incident response and targeted malware samples with CERT-In,
  - 5) updates the firmware/software with the digitally signed OEM validated patches only.
  - 6) enables only those ports and services that are required for normal operations. In case of any emergency the procedure as laid in Access management be followed.
  - 7) maintains firewall logs for the last 6 months duration. Firewall logs shall be analysed and all critical and high severity comments shall be addressed for effective closure.
  - 8) retains document of FAT, SAT test results and report/ certificate of cyber tests carried out for compliance of Government Orders and Cyber Security Audit.\*

- 9) maintains all cyber logs and cyber forensic records of any incident for at least\*\* 90 days.
- \* FAT, SAT must include comprehensive cyber security tests of the component/equipment/system to be delivered/delivered at site.
- \*\* 90 days from date of the commissioning of the system/recovery from any incident, whichever is later.
- d) The Responsible Entity shall routinely audit and test security properties of the Critical System and must act upon, in case if any new vulnerabilities is identified through testing or by the equipment manufacturer.
- e) The Responsible Entity shall design a secure architecture for control system appropriate for their process control environment\*.
- f) All State Load Dispatch Centres(SLDCs) shall comply with the directions issued by the National Load Dispatch Centre(NLDC) as well as Regional Load Dispatch Centres(RLDCs) U/s 29 (1) of the Electricity Act, 2003 to ensure stability and cyber security of grid operation and achieve efficiency in the grid operation. In case of any non-compliance, the Head of SLDC shall be responsible and shall be liable for Penalty as per the provision of CERC/SERC.

\*There are so many different types of systems in existence and so many possible solutions, it is important that the selection process ensures that the level of protection is commensurate with the business risk and the Responsible Entity shall not rely on one single security measure for its defence. (*Reference IEC/TR62351-10 Edition1.0 2012-10 Power systems management and associated information exchange –Data and communications security – Part 10: Security architecture guidelines*).

#### Article 6 Cyber Risk Assessment and Mitigation Plan

- a) The Responsible Entity shall document in their Cyber Security Policy a Cyber Risk Assessment and Mitigation Plans drawn upon the best practises being followed in the Power Sector, and the same shall be approved by Board of Directors.
- b) The Cyber Risk Assessment and Mitigation Plans shall clearly define the matrix for assessing the cyber risk of both IT and OT environment and risk acceptance criteria.
- c) The Cyber Risk Assessment Plan shall be capable to demonstrate that repeated cyber security risk assessment delivers consistent, valid and comparable results.
- d) The review of cyber risk assessment shall be carried out at least once in a Quarter. The actionable of risk treatment and mitigation shall be tracked in this review for their effectiveness.
- e) The CISO shall be responsible for implementation and regular review, on the basis of internal and external feedbacks, of the Cyber Risk Assessment and Mitigation Plans.

#### Article 7 Phasing out of Legacy System

- a) As the life cycle of the Power System Equipment/System is longer than that of IT Systems deployed therein, the Responsible Entity shall ensure that all IT technologies in the Power System Equipment/System should have the ability to be upgraded.
- b) The Responsible Entity shall ensure that the Information Security Division shall draw the list of all communicable equipments/systems nearing end life or are left without support from OEM. Thereafter CISO shall identify equipment/systems to be phased out from the list drawn, firm up their replacement plan and put up the replacement plan for approval before the Board of Directors.
- c) The CISO shall ensure that till equipments/systems nearing end life or left without support from OEM are not replaced, their cyber security is hardened and ensured through additional controls provisioned in consultation with the OEM or alternate Supplier(s)\*.  
\*e.g. Use of CDAC developed AppSamvid and whitelisting of applications installed may be explored across all legacy systems.
- d) The Responsible Entity shall document in their Cyber Security Policy a Standard Operating Procedure for safe and secure disposal of outlived or legacy devices.

#### Article 8. Cyber Security Training.

- a) The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized physical access (unescorted or escorted) to their Critical Systems.
- b) The Responsible Entity shall review annually their cyber security training program and shall update it whenever necessary. Annual Review shall record evaluation of the effectiveness of the trainings held.
- c) The Responsible Entity shall ensure that Cyber Security training program designed for their IT as well as OT O&M Personnel must include following topics and as per their functional requirements and security concerns additional topics shall be added:
  - 1) User authentication and authorization.
  - 2) Cyber Security and Protection mechanisms of IT/OT/ICS Systems.
  - 3) Introduction to various standards i.e. ISO/IEC:15408, ISO/IEC:24748-1, ISO: 27001, ISO: 27002, ISO 27019, IS 16335, IEC/ISO:62443.
  - 4) Training on implementation of ISO/IEC 27001 and awareness on IEC 62443.
  - 5) Vulnerability Assessment in the Critical System.
  - 6) Monitoring and preserving of electronic logs of access of Critical Assets.
  - 7) Detecting cyber-attacks on SCADA and ICS systems
  - 8) The handling of Critical System during cyber crisis.
  - 9) Action plans and procedures to recover or re-establish normal functioning of Critical Assets and access thereto following a Cyber Security Incident.
  - 10) Hands on SCADA operation at any of the Regional Load Dispatch Centre.
  - 11) Handling of risks involved in the procurement of COTS Products.
- d) All Personnel engaged in O&M of IT & OT Systems shall mandatorily undergo

- courses on cyber security of Power Sector from any of the training institute designated by CEA, immediately within 90 days from the notification of CEA Guidelines on Cyber Security in Power Sector.
- e) The Responsible Entity shall ensure that none of their newly hired or the current Personnel have access to the Critical System, prior to the satisfactory completion of cyber security training programme from the Training Institutes designated in India, except in specified circumstances such as cyber crisis or an emergency.
  - f) NPTI in consultation with CEA shall identify and design domain specific courses on Cyber Security for different target groups. The “Governing Board for PSO Training and Certification” shall approve the content, duration etc of these courses and shall review it Annually. NPTI shall conduct these courses at all of their branches on regular basis and shall maintain the list of the Participants successfully completing the course.

#### Article 9 Cyber Supply Chain Risk Management

- a) The Responsible Entity shall ensure that, as and when Ministry of Power, Government of India notifies the Model Contractual Clauses on cyber security, these clauses are included in their every Bid invited for procurement of any ICT based components/equipments/System to be used for Power System.
- b) The Responsible Entity shall ensure that all the Communicable Intelligent Equipments and the Service Level Agreements (SLAs) for their Critical Systems shall be sourced from the list of the “Trusted Sources” as and when drawn by MoP/CEA.
- c) The Responsible Entity shall ensure that, in case, for the any Communicable Intelligent Devices, if no Trusted Source has been identified, then the successful bidder in compliance with the provisions made in MoP order dated 2.7.2020 and any other relevant MoP order has got the product cyber tested for any kind of embedded malware/Trojan/cyber threat and for adherence to Indian Standards at the designated lab.
- d) The Responsible Entity shall ensure that the essential cyber security tests are carried out successfully during FAT, SAT as detailed in **Annexure A**. The equipment/System besides for functionality shall also be tested in the factory for vulnerabilities, design flaws, parts being counterfeit or tainted, so as to minimize problems during on-site- testing and installation. Cyber Security Conformance Testing are to be carried out in the designated Lab as listed in **Annexure-I of MoP Order No. 12/13/2020-T&R dt. 8<sup>th</sup> June, 2021(Order at Annexure-B)**.
- e) The Responsible Entity shall ensure that the Equipment/System supplied by the successful bidder shall accompany with a certificate<sup>s, #</sup> obtained by OEM from a certification body accredited to assess devices and process for conformance to IEC 62443-4 standards during design and manufacture. The Responsible Entity shall accept the certificate submitted along with the supplied Equipment/System only if it’s in line with the Testing Protocol as notified by Ministry of Power, Government of India, from time to time.
- f) The Responsible Entity in compliance to the requirement of Article 9(e) shall also accept, till the setting up of an adequate certification facility in the India, a digitally signed self-declaration of conformance to the IEC 62443-4 standards during design

and manufacture of the equipment/system, if submitted by the OEM.

- g) The Responsible Entity shall dispose all unserviceable or obsolete Communicable Intelligent Devices as per the procedure laid in their Cyber Risk Assessment and Mitigation Plans which shall be in line with the prevailing best practices.

§ The National & International certification may be specified in the tender for critical systems/sub-systems being procured by the Responsible Entity.

# Certification Schemes:

**Embedded Device Security Assurance Certification** is for an individual product, **System Security Assurance Certification** is for a set of products in a system (possibly from different vendors)

**Security Development Lifecycle Assurance Certification** is for the development processes that a manufacturer uses for developing products.

#### Article 10 Cyber Security Incident Report and Response Plan

- a) The CISO of the Responsible Entity shall report in the formats prescribed by CERT-In, all Cyber Security Incidents, classified as reportable events.
- b) Root cause analysis for all reportable events shall be carried out and corrective action taken, so as to ensure that any re-occurrence of such event can be managed with ease.

The Responsible Entity shall mandatorily define in their Cyber Security Policy, criteria(s) identified on the basis of impact analysis, for declaring the occurrence of Cyber Security Incident(s) as a Cyber Crisis in the System owned or controlled by them.

- c) The Responsible Entity shall mandatorily designate an Officer along with his/her standby by name and designation and empower them to declare an occurrence of the incident(s) as “Cyber Crisis”. The contact details of these Officers shall be updated in the C-CMP within 15 days of changes if any due to transfer or superannuation etc.
- d) The CISO shall ensure that during any Cyber Security Incident, ISD monitors and minutely records every details of cyber security events and incidents in both IT as well as the OT System owned or controlled by the Responsible Entity.
- e) The CISO shall ensure that each cyber incident is handled strictly as per Cyber Security Incident Response Plan detailed in the latest C-CMP approved by the Board of Directors.
- f) The Responsible Entity shall ensure that the efficacy of the Cyber Security Incident Response Plan is tested annually through mock drill(s) carried out, if feasible, as simulation exercise(s) or as table top exercise(s) with wider participation of their employees, in consultation with CERT-In and sectoral CERT. In case if any shortcoming is observed in the Cyber Security Incident Response Plan suitable changes shall be made in it.

- g) The Responsible Entity shall ensure that the CISO compiles details of incident detection, incident handling, learnings from each incident and damage claims made if any and shall report to CERT-In as well as upload information on ISAC-Power Portal.

#### Article 11 Cyber Crisis Management Plan(C-CMP)

- a) The Responsible Entity shall prepare a Cyber Crisis Management Plan and submit to their sectoral-CERT for review with intimation to Ministry of Power/CISO-MoP. Responsible Entity shall update their C-CMP on the basis of comments made by sectoral-CERT and then submit for vetting to CERT-In. The C-CMP shall be updated once again to include the observations made by CERT-In before seeking approval of Board of Directors for implementation of C-CMP.
- b) The Responsible Entity shall ensure that the C-CMP is reviewed at least annually. The CISO shall ensure that all changes are made in C-CMP only with the due approval of Board of Directors and the changes made in C-CMP have been communicated through a verifiable means to all the concerned Personnel of the Responsible Entity.
- c) The CISOs shall be the custodian of all the cyber security related documents including Cyber Crisis Management Plan, Risk Treatment Plan, Statement of Applicability of controls, and compliance to regulator's requirement.
- d) The CISO shall be accountable for ensuring enforcement of C-CMP by Information Security Division of the Responsible Entity, during a cyber-crisis, as and when declared by the designated Officer. (refer Article 10(d))

#### Article 12: Sabotage Reporting%

- a) The Responsible Entity shall incorporate procedure for identifying and reporting of sabotage in their Cyber Security Policy within 30 days from issue of the Guidelines, or grant of licence under the appropriate legal provisions to the Responsible Entity.
- b) The CISO shall be held liable for non-reporting of identified sabotage(s) as per procedure laid for identifying and reporting of sabotage in the Cyber Security Policy of the Responsible Entity.
- c) The CISO shall prepare a detailed report on disturbances or unusual occurrences, identified, suspected or determined to be caused by sabotage in the Critical System of the Responsible Entity, and shall submit the report to the Sectoral CERT as well as to CERT-In within 24 hours of its occurrence.
- d) The CISO shall submit to NCIIPC within 24 hours of occurrence the report on every sabotage classified as cyber incidents(s) on "Protected System".
- e) The CISO upon occurrence on every sabotage shall take custody of all log records as well as digital forensic records of affected Cyber Assets, Intrusion Detection System, Intrusion Protection System, SIEM and shall preserve them for at least 90 days and shall make them available as and when called upon for investigation by the concerned Agencies.

*%Disturbances or unusual occurrences, suspected or determined to be caused by sabotage.*

*Sabotage e.g. can be a forced intrusion in un-manned/manned facility and taking control of operation of Critical System through a communicating device.*

#### Article 13 Security and Testing of Cyber Assets

- a) The Responsible Entity shall ensure security of all in-service phase as well as standby Cyber Assets through regular firmware/Software updates and patching, Vulnerability management, Penetration testing (of combined installations), securing configuration, supplementing security controls. CISO shall maintain details of update version of each firmware and software and their certification if received from OEMs.
- b) The Responsible Entity shall carry out regularly Vulnerability Assessment of all Cyber Assets owned or under their control. If a Cyber Asset is found vulnerable to any exploits or upon any patch updates or major configuration changes, then further Penetration Testing may be carried out offline or in a suitably configured laboratory test-bed to determine other vulnerabilities that may have not been identified so far.
- c) The Responsible Entity shall specify security requirement and evaluation criteria during each phase of their procurement Process.
- d) The Responsible Entity shall ensure that all Cyber Assets being procured shall conform to the type tests as mentioned in the specification for type testing listed in the bid document. Type test reports of tests conducted in NABL accredited Labs or internationally accredited labs (with in last 5 years from the date of bid opening) shall be mandated to be submitted along with bid. In case, the submitted Type Test reports are not as per specification, the re-tests shall be conducted without any cost implication to the Responsible Entity.
- e) The Responsible Entity shall ensure that all Communicable devices are tested for communication protocol as per the ISO/IEC/IS standards listed in **MoP Order No. 12/13/2020-T&R dated 8<sup>th</sup> June, 2021(Annexure-B)**.
- f) The Responsible Entity shall ensure that all Critical Systems designed with Open Source Software are adequately cyber secured.
- g) The Responsible Entity as a best practise upon any incidence of Cyber Security Breach shall carry out cyber security tests at any lab designated for cyber testing by Ministry of Power. These tests shall be similar to Pre Commissioning Security Test and those essential for carrying out Post Incident Forensics Analysis.

#### Article 14 Cyber Security Audit

- a) The Responsible Entity shall implement Information Security Management System (ISMS) covering all its Critical Systems.
- b) The Responsible Entity shall through a CERT-In Empanelled Cyber Security OT Auditor shall get their IT as well as OT System audited at least once in every 6 (six) months and shall close all critical and high vulnerabilities within a period of one month and medium as well as low non-conformity before the next audit. Effective closure of all non-conformities shall be verified during the next audit.
- c) The Cyber Security Audit shall be as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335 and other guidelines issued by appropriate Authority if any. These mentioned standards shall be current with all amendments if any and in case if any standard is superseded, the new standard shall be applicable. CISO shall ensure immediate closure of non-conformance, based on the criticality and by means all non-conformances are to be closed before the next



audit.

- d) The Responsible Entity shall ensure that CISO has all the required systems and documents in place, as mandated by NSCS for base line cyber security audit.

#### FAT & SAT

1. During FAT stage, the customer has to verify all types test reports / certificates including Communication protocol and security conformance tests of the devices offered for FAT.
2. FAT of SCADA involves testing as a whole system in the integrated scale down set up. For SCADA, Indian standard IS 15953: 2011 “SCADA System for Power System Applications” provides definition and guidelines for the specification, performance analysis and application of SCADA systems for use in electrical utilities (for transmission & Distribution) including guidance on Tests and inspections.
3. The SAT will be done at customer site as per the SAT document mutually agreed by buyer and supplier. For SAT also, guidance from IS 15953: 2011 need to be applied.
4. IEC 61850-10-3 Communication Networks and Systems For Power Utility Automation- Functional testing of IEC 61850 systems (in draft stage - CDTR) covers testing of applications within substations covering
  - a. A methodical approach to the verification and validation of a substation solution
  - b. The use of IEC 61850 resources for testing in Edition 2.1
  - c. Recommended testing practices for different use cases
  - d. Definition of the process for testing of IEC 61850 based devices and systems using communications instead of hard wired system interfaces (ex. GOOSE and SV instead of hardwired interfaces)
  - e. Use cases related to protection and control functions verification and testing.

This standard may be used as a guidelines for FAT & SAT for Substation Automation System (SAS) based on IEC 61850.

Annexure - B

**Annexure – 1**

**List of designated laboratories for cyber security conformance testing**

**Table -A. Field Equipment /Operational Technology (OT)**

Sl. No.	Equipment	Communication Protocol Conformance Standards	Protocol Security Conformance Standards	Designated Laboratories
1	Remote Terminal Units (RTUs) & PLCs with IEC communications protocols	IEC 60870-5 -101 / IEC 60870-5 -104 (Test Details Annexure 2)	IEC 60870-5- 7 Security extension & IEC 62351 series (specifically IEC 62351-100 parts 1 & 3) ( Test Details Annexure-2)	Central Power Research Institute (CPRI), Prof Sir C V Raman Road, Sadashivanagar P O, Bengaluru – 560080, Karnataka
2	Intelligent Electronic Equipment / Numerical Protection Relays / Bay Control Units / Bay Protection Units, Gateways, Transformer Tap controller/ changer, etc. with IEC 61850 communication protocol	IEC 61850 – 5 to IEC 61850 – 10  ( Test Details Annexure 2)		CPRI
3	Smart meters with IEC 62056 communication protocols	IEC 62056 series / DLMS & IS 15959 series and IS 16444 series ( Test details Annexure 2)	IEC 62056 series / DLMS & IS 15959 series and IS 16444 series (Test Details Annexure 2)	1. CPRI 2. Electrical Research and Development Association (ERDA), ERDA Road, GIDC, Makarpura, Vadodara - 390 010 Gujarat 3. Yadav Measurements Pvt. Ltd. (YMPL) 373-375, RIICO Bhamashah Industrial Area Kaladwas 313003 Udaipur – Rajasthan

**Information Technology (IT) Equipment (Main / Backup / Disaster recovery (DR) Control Centre / Substation control centre IT equipment)**

All IT products procured /supplied shall have a valid Certificate of Common Criteria as per ISO/IEC 15408 issued by signatories of the Common Criteria Recognition Agreement (CCRA)

( [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)).

Import/procurement/supplied from vendors sourcing from prior reference countries, the Certificate for Common Criteria shall be from Government Laboratories in India according to the IC3S scheme operated by Ministry of Electronics and Information Technology, which is a signatory to CCRA. <https://www.commoncriteria-india.gov.in/>

**Annexure - 2****Details of tests for various identified products****Remote Terminal Units (RTUs) (Sl. No. 1 of Table – A of Annexure –****1) Test protocol:**

Utilities / manufacturers will submit the sample along with all the required technical documentation for taking up testing to the designated laboratory.

**Reference standards**

- 1) IEC 60870-5-101 & IEC 60870-5-104 as applicable
- 2) IEC 60870-5-7 Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)
- 3) IEC 62351-100-1 & IEC 62351-100-3 and other cross referenced standards.

**Test cases****Extract from standard (IEC 62351-100-1)**

The conformance test cases are divided into four clauses:

- Clause 5: Verification of configuration parameters. This clause contains the configuration parameters affecting the message contents and/or the protocol behaviour.
- Clause 6: Verification of communication. The goal of this clause is to verify that Device Under Test (DUT) is able to implement the security extension messages as described in IEC TS 60870-5-7.
- Clause 7: Verification of procedures. The goal of this clause is to verify that DUT is able to execute the security extension procedures as described in IEC TS 62351-5.
- Clause 8: Test result chart. This clause contains the results of the test cases listed in Clauses 6 and 7 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables. They are numbered; their numbering syntax is: Subclause number (where the Table is located) + test case number.

In the column 'reference' each test case has a direct reference to IEC TS 62351-5 or IEC TS 60870-5- 7 where the clause under test is defined.

Test cases are mandatory depending on the description in the column 'Required'. The following situations are possible:

M= Mandatory test case. The test is referencing a clause that is mandatory in IEC TS 62351-5 or IEC TS 60870-5-7.

Protocol Information Conformance Statement (PICS) x, x = Mandatory test case if the functionality is enabled in the PICS (by marking the applicable check box), with a reference to the section number of the PICS (x.x).

### Conformance testing of security extension procedures

The security extension procedures can be summarized as follows:

- User management
- Update key maintenance
- Session key maintenance
- Challenge/Reply authentication
- Aggressive Mode authentication

### Extract from standard (IEC 62351-100-3)

IEC 62351-3 defines the requirements related to the authentication/encryption protocol, procedures and methods to be implemented at TCP/IP (transport) level.

The conformance test cases are divided into three clauses:

- Clause 5: Verification of configuration parameters. This clause contains the parameters specified by the standards referencing IEC 62351-3 (see IEC 62351-3:2014/AMD1:2018, Clause 7) and affecting the protocol behaviour.
- Clause 6: Verification of IEC 62351-3 requirements. The goal of this clause is to verify that DUT is conformant to the requirements of the IEC 62351-3.
- Clause 7: Test result chart. This clause contains the results of the test cases listed in Clause 6 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables. They are numbered, their numbering syntax is: Subclause number (where the table is located) + test case number.

In the column 'Reference' each test case has a direct reference to IEC 62351-3 where the clause under test is defined. PICS or Protocol Implementation eXtra Information for Testing (PIXIT) could be found in the "Reference" column for some test cases whenever the execution of the test case shall take into account specific parameter values declared in the PICS or PIXIT of the DUT.

Test cases are mandatory depending on the description in the column 'Required'. The following situations are possible:

M = Mandatory test case. The test is referencing to a clause that is mandatory in IEC 62351-3. PICS

or

PIXIT = Mandatory test case if the functionality is enabled in the PICS or PIXIT by marking the applicable check box or declaring the applicable value.

### **Intelligent Electronic Devices (IEDs) (Sl. No. 2 of Table – A of Annexure – 1)**

Utilities / manufacturers will submit the sample along with all the required technical documentation for taking up testing to the designated laboratory.

#### **Reference standards**

IEC 61850 series

Specifically IEC 61850-5, IEC 61850-6, IEC 61850-7, IEC 61850-8, IEC 61850-9 and IEC 61850-10

#### **Test cases**

Communication protocol conformance as per IEC 61850 -10. This part of standard defines methods and abstract test cases for conformance testing of client, server and sampled values devices used in power utility automation systems, the methods and abstract test cases for conformance testing of engineering tools used in power utility automation systems, and the metrics to be measured within devices according to the requirements defined in IEC 61850-5. Further this part of standard specifies standard techniques for testing of conformance of client, server and sampled value devices and engineering tools, as well as specific measurement techniques to be applied when declaring performance parameters. The use of these techniques will enhance the ability of the system integrator to integrate IEDs easily, operate IEDs correctly, and support the applications as intended.

### **Smart Meters (Sl. No. 3 of Table – A of Annexure – 1)**

Utilities / manufacturers will submit the sample along with all the required technical documentation for taking up testing to the designated laboratory.

IEC 62056 series of standards (Electricity metering data exchange – The DLMS/COSEM suite) specifies details of communication protocol requirements, conformance testing and security requirements. The Part 5-3 (DLMS/COSEM application layer) specifies the DLMS/COSEM application layer in terms of structure, services and protocols for DLMS/COSEM clients and servers, and defines rules to specify the DLMS/COSEM communication profiles. It defines services for establishing and releasing application associations, and data communication

services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2 using either logical name (LN) or short name (SN) referencing.

Clause 5 and sub clauses specifies security requirements. It cover security concepts, Identification and authentication, Cryptographic algorithms, Cryptographic keys – overview, Key used with symmetric key algorithms, Keys used with public key algorithms and Applying cryptographic protection.

**Note:** All above referred standards shall be latest with amendments if any at the time of submission of sample(s) for testing.

**Testing Criteria****1) Supply from Trusted Sources**

The sample size shall be as specified by CEA as per the approved criteria for Trusted Vendors

**2) Supply from other than trusted vendors**

The sample size shall be shall be 5% of the supply lot / ordered quantity (minimum one). The manufacturer shall submit request to the Nodal agency along with vendor's / manufacturer's certifications for supply chain management system practices and secure product development process implementations based on any one or more of standards ISO / IEC 27036, ISO / IEC 20243, IEC 62443 for verification.

After scrutiny of vendor's / manufacturer's certifications the supplier / utilities shall be asked to submit product to the designated laboratory for communication and cyber security conformance testing.

The supply lot shall stand rejected on failure to comply with the test requirements.

**3) Supply from prior reference countries**

The utility shall obtain prior permission from the Government of India for importing the product / system from prior reference countries.

The sample size shall be shall be 10 % of the supply lot / ordered quantity (minimum one). The manufacturer shall submit request to the Nodal agency along with vendor's / manufacturer's certifications for supply chain management system practices and secure product development process implementations based on any one or more of standards ISO / IEC 27036, ISO / IEC 20243, IEC 62443 for verification.

After scrutiny of vendor's / manufacturer's certifications the supplier / utilities shall be asked to submit product to the designated Government / Government controlled Autonomous laboratory for type tests (Annexure – 4) and communication & cyber security conformance testing.

The supply lot shall stand rejected on failure to comply with the test requirements.



**Annexure – 4****Type Tests**

Products imported from prior reference countries shall also undergo type testing as per following standards in addition to communication protocol and security conformance testing at the designated Government / Government controlled Autonomous laboratory:

**Type test standards for RTUs**

1. IEC 60870-1-2:1989 Telecontrol equipment and systems. Part 1: General considerations. Section Two: Guide for specifications.
2. IEC 60870-2-1:1995 Telecontrol equipment and systems - Part 2: Operating conditions - Section 1: Power supply and electromagnetic compatibility.
3. IEC 60870-2-2:1996 Telecontrol equipment and systems - Part 2: Operating conditions -Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences).
4. IEC 60870-3:1989 Telecontrol equipment and systems. Part 3: Interfaces (electrical characteristics)

**Type test standard for IEDs / Numerical Protection Relays / Bay controls units**

1. IEC 61850-3: 2013, Ed. 2 Communication networks and systems for power utility automation – Part 3: General requirements.

**Type test standards for Smart meters**

1. IS 16444: 2015 AC static direct connected watthour smart meter class 1 and 2 – Specification.
2. IS 16444 Part 2: 2017 AC static transformer operated watthour and var - Hour smart meters, class 0.2 S, 0.5 S and 1.0 S: Part 2 specification transformer operated smart meters.

**Note:**

1. All above referred standards shall be latest with amendments if any at the time of submission of sample(s) for testing.
2. Type tests generally covers functionality, environmental, mechanical, EMI/ EMC and electrical safety related tests.

**Annexure -A**

**Inoxwind Limited**

S. No.	Site/ Location	State	Address
1	Noida	UP	Plot No. 17, Sector 16A, Noida - 201301, Uttar Pradesh Tel. No.: +91 120 6149 600 Fax No.: +91 120 6149 610
2	Vadodara	Gujarat	3rd Floor ABS Towers Old Padra Road Vadodara - 390007
3	Rohika	Gujarat	Plot No. 128, Ahmedabad-Rajkot Highway (NH-8A), Village-Rohika, Tehsil- Bavla, District Ahmedabad-382 220, Gujarat
4	Bhuj	Gujarat	Inside AMW Campus, Village Kanaiyabe, District Kutch, Bhuj - 370020, Gujarat
5	Barwani	MP	Plot No. 20, AKVN Industrial Area, Relwa Khurd, Tehsil – Rajpur, District Barwani – 451449, Madhya Pradesh
6	Una	HP	Plot No. – 1, Khasra Nos. 264 to 267 Industrial Area, Village Basal, District Una174 303, Himachal Pradesh

**Inox Green Energy Services Ltd.**

S. No.	Site	State	Address
1	CKPalli	AP	Inox Green Energy Services Ltd Vill-Valasala, Post-malkapuram, Dhone mandal, Dist-kurnool, AP-518222
2	Payal Kuntala		Inox Green Energy Services Ltd PTC wind farms Vill-Payalakuntala, Kodur Mandal, Dist-Kadappa, AP-516228
3	Tallimadugula		Inox Green Energy Services Ltd Vill-Tallimadugula, Kanaganapalli mandal, Dist-Anantapur, AP-515641
4	Palakkad	KL	Inox Green Energy Services Ltd Kinfra Industrial park,Vill-Pudussery Central, Tal-Kanjikode, Dist-Palakkad , Kerala-678621.
5	Jaora	MP	Inox Green Energy Services Ltd Bhatkheda Substation,khasra No.2, Vill-Bhatkheda, Post- Kalukheda, Tehsil- Piploda, Dist- Ratlam, M.P.-457340
6	Kukru		Inox Green Energy Services Ltd Near by loc. KKT15, Vill: Kordi, Tehsil- Bhainsdehi, Dist- Betul, M.P.-460220
7	Nipaniya		Inox Green Energy Services Ltd 220/33 KV, Nipaniya SS, Vill-Nipaniya, Tehsil- Garauth, Dist-Mandasaur, M.P.- 458883

8	Bhendewade		Inox Green Energy Services Ltd At- bhendwade, vill- Altur, Tal- Shauwadi, dist- kolhapur, Maharastra-415101
9	South Budh	MH	Inox Green Energy Services Ltd Gat No 663, Khanakpur, Jadhavwadi Road, Sangli-Maharashtra- 415307
10	Vaspeth		Inox Green Energy Services Ltd Vill-ravalgundwadi, gat no-62, Pacchapur phata vaspeth (tal-jath), Sangali, Maharastra-416404
11	Dangri	RJ	Inox Green Energy Services Ltd Inox GSS, Vill- Dangri, Post-Phatehgarh, Dist- Jaisalmer, Rajasthan- 345001
12	Kayathar	TN	Inox Green Energy Services Ltd No. 2/47A, Madurai road, Vill-Savalaperi, Post-Villiseri, Nalatinputhur (via), Tal-Kovilpatti, Dist-Tuticorin, Tamilnadu- 628715
13	Bagewadi	KA	Inox Green Energy Services Ltd jayanapur cross, Opposite old BSNL office basavana bagewadi, Vijayapura (KA)-586203
14	Ujjani	KA	Inox Green Energy Services Ltd Vill- Ujjini, Tal- Kudligi, Dist-Bellary, KA
15	Dayapar	GJ	Inox Green Energy Services Ltd Inox PSS,Vill-Meghpar, Dayapar, Bhuj
16	Savarkundla	GJ	Inox Green Energy Services Ltd 33/66 kv substation, At chapri, Savrkundla-Mahuva Highway, TAL-Savrkjndla, Dist-Amreli, GJ-364522
17	Sadla	GJ	Inox Green Energy Services Ltd Inox PSS,Vill-Sadla, tal-Muli, Dist-Surendra nagar, GJ-363520
18	Rojmal	GJ	Inox Green Energy Services Ltd Inox PSS,Vill-Sukhpar, Tal-Babra, Dist-Amreli, GJ
19	Tankara	GJ	Inox Green Energy Services Ltd Vill- Virvav, Dist-Morvi, GJ-363650
20	Mahidad	GJ	Inox Green Energy Services Ltd Inox PSS,Vill-Devpura, Tal-Chotila, Dist- surendra nagar, GJ-363620