Information Security Policy

S. No.	Type of Information	Document Data
1	Document Title	Information Security Policy
2	Date of Release	21-02-2025
3	Date of Approval	17-02-2025
4	Document Revision No	2.1
5	Document Approver	RPL board

List of Abbreviations

RPL	ReNew Private Limited
ISO	International Organization for Standardization
ISMS	Information Security Management System
CEA	Central Electricity Authority
NCIIPC	National Critical Information Infrastructure Protection Centre
SECI	Solar Energy Corporation of India Limited
DPDPA	Digital Personal Data Protection Act
ISGC	Information Security Governing Committee
ISSC	Information Security Steering Committee
CISO	Chief Information Security Officer
ICT	Information and Communication Technology
CSP	Cloud Service Provider
IPR	Intellectual Property Right
PII	Personally Identifiable Information
VAPT	Vulnerability Assessment and Penetration Testing
KPI	Key Performance Indicators
SOC	Security Operations Centre
SIEM	Security Information and Event Management

Contents

1 Information Security Policy

1.1 Introduction

The Information Security policy provides management direction and support to ensure protection of ReNew Private Limited (hereinafter referred to as 'ReNew') information assets and IT services, and to allow access, use and disclosure of such information in accordance with appropriate policies, laws and regulations. The purpose of the information security policy is to protect and preserve the confidentiality, integrity, and availability of information. Input has also been taken from various standards and regulatory guidelines to prepare this policy. The various guidelines are as under:

1.1.1 ISO 27001:2022: ISO 27001 provides a framework for establishing, implementing, maintaining and continually improving Information Security Management System (ISMS).

1.1.2 Central Electricity Authority Guidelines, 2021 emphasizes the need for robust cybersecurity practices in the power sector, given the increasing reliance on digital systems for grid management and operations.

1.1.3 National Critical Information Infrastructure Protection Centre (NCIIPC): NCIIPC guidelines are designed to protect and ensure resilience of critical information infrastructure sectors such as energy, telecommunications etc. against cyber threats and disruptions.

1.2 Policy Scope

The Information Security Policy applies to all employees, contractors, consultants and third-party workers who access ReNew Private Limited (RPL's) information or assets.

The information and assets included in the scope of this security policy statement are:

1.2.1 ReNew information in any medium or form such as printed paper, digital, video, and audio representations.

1.2.2 ReNew information systems which process information.

1.2.3 ReNew communication systems which transport information.

1.3 Policy Statement

Renew is committed to protecting the confidentiality, integrity, and availability of all its key information assets to maintain a secure system. The information security framework (comprising this policy, supporting policies, processes and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing. Renew shall implement policies, associated procedures and controls that protect information assets, including but not limited to personal information and IT resources through a risk-based approach. This acknowledges that it is not possible to protect against all threats, whether internal or external, deliberate, or accidental. Instead, efforts will focus on mitigating identified risks to an acceptable level.

1.4 Policy Objectives

This policy provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage

information security in Renew. Renew shall secure information by: -

1.4.1 Creating, maintaining and continuously updating security systems to ensure protection of Renew assets, systems and data.

1.4.2 Ensuring compliance with all legal, regulatory, statutory, and contractual requirements.

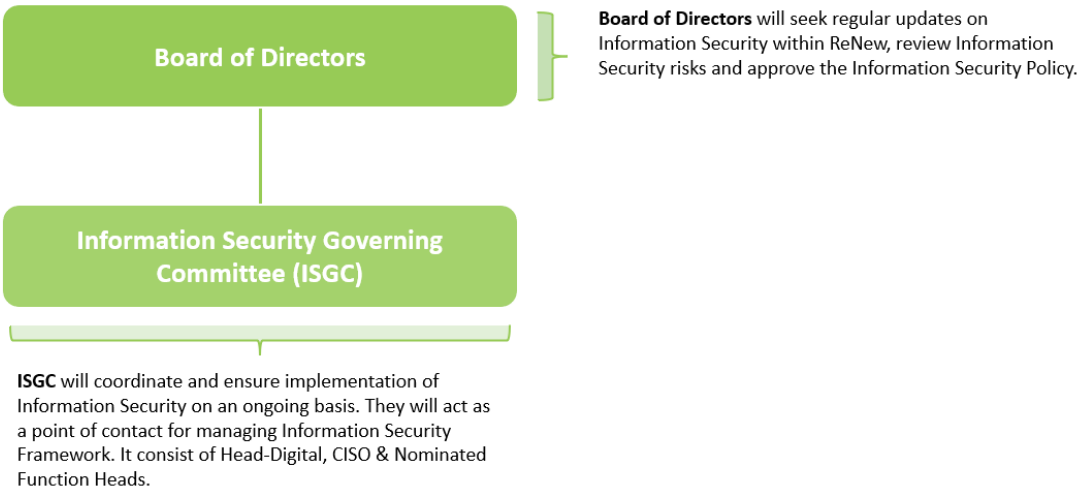
1.4.3 Encouraging management and staff to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimize the occurrence and severity of Information Security incidents.

1.4.4 Enable mechanisms to facilitate reporting of security alerts and timely assessment.

1.4.5 Taking appropriate actions for any violations of the information security policy.

1.5 Governance Structure

The Information Security Organization was established to coordinate and control the implementation of information security within the organization. ReNew believes in a multi-disciplinary approach to information security.



Refer: ReNew-ISMS-Governance Process

1.6 Roles and Responsibilities

To maintain accountability and protect information assets, information security roles and responsibilities shall be clearly defined and communicated within the organization. ReNew shall ensure the same by:

i. Clearly define who is responsible for key aspects of information security, such as managing security, responding to incidents, maintaining necessary segregation of duties as feasible and ensuring compliance with policies.

ii. Security responsibilities shall be assigned to individuals or teams based on their expertise.

iii. Roles and responsibilities shall be clearly communicated to all relevant stakeholders.

iv. Roles shall be regularly reviewed and updated in response to changes in job roles, personnel, or business processes.

1.6.1 *Board of Directors*

The Board of Directors shall be responsible for directing all activities necessary for promoting a strong culture of information security to manage information security risk at Renew. They shall provide the oversight, governance, and resources required in complying with Information Security policies and procedures. The Board of Directors shall mandate that all personnel adhere to ReNew's information security policy.

1.6.2 *Information Security Governing Committee (ISGC)*

The ISGC shall be chaired by Head –Digital and shall comprised of nominated function heads. Members of ISGC collaboratively shall oversee and approve security policies, initiatives, and risk management practices. They shall ensure that the information security strategy aligns with the overall business objectives.

1.6.3 *Chief Information Security Officer (CISO)*

CISO shall be accountable for enforcing the information security policy and its governance. The CISO is responsible for overseeing all aspects related to security operations and driving the overall information security within the organization.

1.6.4 *User*

All the employees shall have the responsibility to read, understand and adhere to the Information Security Policy. Users shall be responsible/ accountable for actions associated with their use of information assets. They shall ensure that Renew information is not made available to unauthorized parties. They shall follow the mandated requirements towards securing ReNew assets. They shall ensure completion of assigned training within stipulated timelines. Users are also responsible for reporting suspected security alerts through recommended channels such as central email or by logging tickets

1.6.5 *Third Party/Vendors/Dealers/Distributors*

The third party/ vendors shall be responsible for understanding and abiding by Renew's Security Policy. They shall provide compliance with defined norms as and when required.

1.7 Review and Evaluation

This policy shall be reviewed at the time of any major change(s) in the existing environment affecting policies and processes or at least on an annual basis, whichever is earlier. This document shall be reviewed by ISGC and shall be approved by the Board of Directors. The document shall be updated based on the review comments.

1.8 Non-Compliance

All employees, contractors, consultants, and vendors are required to comply with the Information Security policy and corresponding process. Any non-compliance shall result in disciplinary action.

2 Organization Controls

2.1 Policies for Information Security

2.1.1 Objective

To ensure that ReNew's information security management system (ISMS) is consistently aligned with business objectives and remains robust against evolving security risks by establishing, implementing, and maintaining topic specific policies.

2.2 Contact with authorities and special interest groups

2.2.1 Objective

To ensure that ReNew maintains active and ongoing communication with relevant authorities and special interest groups, security forums and professional associations to stay informed about regulatory requirements, industry standards and legal obligations and to facilitate effective collaboration during incidents or emergencies.

2.3 Information security in project management

2.3.1 Objective

To ensure that information security considerations are embedded in all phases of project management. This involves incorporating security measures from the outset of a project and throughout its lifecycle to protect ReNew's information assets.

2.4 Asset and User Endpoint Devices Management

2.4.1 Objective

To efficiently manage and optimize organizational assets and information throughout their lifecycle, ensuring risks are reduced to an acceptable level.

2.5 Acceptable use of information assets

2.5.1 Objective

To establish a clear policy for the acceptable use and formal return of organizational information and assets. This ensures proper handling, security, and monitoring of assets, while safeguarding data during employment or contract transitions.

2.6 Access Management

2.6.1 Objective

To ensure secure authentication for access to information, manage access rights, and control the secure transfer of data while implementing strict identity and access management controls.

2.7 Managing Information Security in the Information and Communication Technology (ICT) Supply Chain

2.7.1 Objective

To ensure that all information security risks associated with ICT products and services in the supply chain are effectively managed.

2.8 Information Security for use of Cloud Services

2.8.1 Objective

To ensure that the acquisition, use, management, and termination of cloud services align with ReNew's information security requirements.

2.9 Intellectual Property Rights

2.9.1 Objective

To ensure that ReNew implements procedures to protect its intellectual property (IP) rights, including copyrights, design rights, trademarks, patents, and source code licenses. ReNew shall also ensure compliance with intellectual property laws and proper management of both its own and third-party IP assets.

2.10 Data Privacy

2.10.1 Objective

The objective is to ensure that the organization identifies and meets all applicable legal, regulatory, and contractual requirements for the privacy and protection of Personally Identifiable Information (PII).

2.11 Independent review of Information Security

2.11.1 Objective

To ensure information security policy and initiatives are reviewed independently on a regular basis.

2.12 Documented Operating Procedures

2.12.1 Objective

To ensure that operating procedures for information processing facilities are properly documented and made accessible to personnel who need them.

2.13 Business Continuity Plan

2.13.1 Objective

To ensure that ReNew maintains a robust level of information security during disruptions, such as disasters or interruptions, by implementing and testing Business Continuity Plans (BCP) and Disaster Recovery (DR) plans.

3 Human Resources Security policy

3.1 Objective

To ensure that all personnel are accountable for upholding information security standards throughout their employment lifecycle.

4 Physical Security policy

4.1 Objective

To establish comprehensive physical security measures which include securing physical perimeters, implementing access control mechanisms, and ensuring the security of offices, rooms, and facilities.

5 Technological Control Policy

5.1 Network Security

5.1.1 Objective

To ensure that network devices, systems, and services are securely managed, monitored, and maintained to protect the integrity, availability, and confidentiality of critical information. Ensure that network configurations, such as routers, switches, and firewalls, are up-to-date, patched, and isolated to prevent unauthorized access and mitigate potential vulnerabilities.

5.2 Backup and Restoration

5.2.1 Objective

Backup copies of servers and storage and systems shall be maintained and regularly tested in accordance with the agreed topic-specific process on backup. Maintain accurate records of all backups, ensuring that backup and restoration processes are documented and regularly tested to confirm reliability.

5.3 Cryptography and Encryption

5.3.1 Objective

To implement encryption protocols to protect sensitive data both at rest and in transit, ensuring that cryptographic methods align with industry standards and best practices.

5.4 Patch Management

5.4.1 Objective

To ensure that all software and systems are up to date, enhancing overall network security. Regular and timely application of patches helps protect against known vulnerabilities, reduces risks of cyber-attacks, data breaches and malware infections

5.5 Capacity Management

5.5.1 Objective

To ensure that IT infrastructure and resources are adequately scaled to meet current and future business demands efficiently. This helps optimize performance, prevent service disruptions, and support growth without compromising on service quality.

5.6 Change Management

5.6.1 Objective

To ensure that all changes to information systems and processing facilities are implemented smoothly, minimizing risks and disruptions, while maintaining system stability.

5.7 Information Exchange

5.7.1 Objective

To implement secure protocols for the exchange of information with internal and external stakeholders to protect sensitive data from unauthorized access or leakage. This involves implementing secure file transfer methods, establishing access controls, and ensuring compliance with data protection regulations during all information exchange activities.

5.8 Protection against Malware

5.8.1 Objective

To implement preventative measures to protect systems from both internal and external malware threats.

5.9 Data Loss Prevention

5.9.1 Objective

To implement data loss prevention (DLP) measures to secure sensitive data in IT systems, networks, and devices, preventing unauthorized transfer of data.

5.10 Logging and Monitoring

5.10.1 Objective

To ensure that all logs related to activities, security events, exceptions, faults, and other relevant events across networks, applications, and IT systems are generated, stored, protected, and regularly analyzed to enhance system performance, ensure security, and quickly address issues to support operational continuity.

5.11 Use of privileged utility programs

5.11.1 Objective

To restrict the use of privileged utility applications (e.g. diagnostic tools) to authorized personnel only, ensuring that only the minimum necessary individuals have access.

5.12 Protection of Information systems during audit testing

5.12.1 Objective

To establish processes to manage access requests during audit testing, ensuring that only necessary data and systems are accessed.

5.13 Remote Working Policy

5.13.1 Objective

To ensure the security of information accessed, processed, or stored by personnel working remotely by implementing robust security measures that protect against unauthorized access and breaches. This includes enforcing secure communication protocols and providing appropriate tools to safeguard data outside ReNew's physical premises.

6 Legal and Compliance Policy

6.1 Objective

To ensure that ReNew identifies, documents, and complies with all applicable legal, statutory, regulatory, and contractual requirements relevant to information security.

7 Cybersecurity controls

7.1. Threat Intelligence

7.1.1 Objective

To gather, analyze, and deliver actionable threat intelligence that is relevant, timely, and aligned with organizational needs to enhance security posture and support proactive defense strategies.

7.2. Threat Hunting

7.2.1 Objective

To actively search for and identify hidden threats within the organization’s systems, aiming to detect and mitigate security risks before they cause significant harm to organizational systems.

7.3. Third Party Cybersecurity Risk Management

7.3.1 Objective

To ensure that ReNew identifies, manages, and mitigates the security risks associated with third-party suppliers, including the protection of sensitive data. Ensure that ReNew regularly monitors and reviews the performance of its suppliers, particularly their adherence to agreed-upon information security practices.

7.4. Security Incident Management

7.4.1 Objective

To ensure that ReNew effectively manages, assesses, and responds to information security incidents by establishing clear processes for incident detection, response, containment, eradication and recovery.

7.5. Technical Vulnerability Management

7.5.1 Objective

To continuously identify, monitor, and assess vulnerabilities in information systems, including endpoints, servers, network devices, cloud environments, applications and take prompt and appropriate actions.

7.5.2.1 Perform thorough and on-going vulnerability assessments and penetration testing to identify potential security gaps in systems, networks, and applications.

7.5.2.2 Maintain a tracker outlining discovered vulnerabilities, exploitability risks, and actionable recommendations tracking them till closure to mitigate risks and enhance security posture.

7.6 System Development lifecycle management

7.6.1 Objective

To integrate security practices into the development, testing and deployment of systems, applications, and environments, ensuring robust protection from the start.

7.7 Red Teaming

7.7.1 Objective

To proactively test and strengthen ReNew's defenses by simulating real-world adversarial techniques, through controlled and authorized simulations.

7.8 Configuration Review

7.8.1 Objective

To ensure that all systems, applications and network components are securely configured according to best practices.

7.9 Information Security Awareness

7.9.1 Objective

To increase awareness and understanding of security practices to protect organizational data and reduce risks to the organization.

7.10 Environment, Social and Governance (ESG)

7.10.1 Objective

Environmental, Social, and Governance (ESG) framework shall be adopted to operate sustainably and responsibly while ensuring transparency and ethical governance.