SUZLON
POWERING A GREENER TOMORROW

SUZLON ENERGY LIMITED

CYBER SECURITY POLICY

1. Policy History

Date of Board approval	Particulars	Effective Date
5th April 2024	Implementation and approval of separate policy on Cyber Security	5th April 2024
5th February 2026	Amendment to the Policy in terms of proposed CEA Guidelines	15th February 2026

2. Purpose of this Policy

2.1 The Cybersecurity Policy of Suzlon Energy Limited ("SEL" or the "Company") aims to establish the fundamental principles and overarching framework for managing and mitigating cybersecurity risks across the organization. Its purpose is to define an integrated set of protection measures that must be consistently implemented throughout the Company to safeguard its information assets and ensure a secure operating environment for all business operation.

~~2.2~~ The availability, integrity, and confidentiality of information are critical for maintaining the Company's competitive advantage, ensuring legal and regulatory compliance, and upholding robust information security standards.

2.3 The Company's Cybersecurity Framework defines the rules and regulations that establish organizational, procedural, and technical requirements for safeguarding information assets, products, solutions, and services. It is designed to protect against internal and external cyber threats and to strengthen the resilience of the Company's business operations.

3. Scope

This Policy applies to:

3.1 the Company and its subsidiaries, and affiliates.
3.2 **All employees, contractors,** and **third-party service providers** who access the information systems, networks, or data of the Company **("Users").**
3.3 **All information assets,** including data stored on premises, in the cloud, across applications, networks, and connected device of the Company.
3.4 **All technology platforms and digital services** utilized for business operations, including IT and OT (Operational Technology) environment.

4. Definitions

Unless repugnant to the context:

4.1 **"Act"** shall mean the Companies Act, 2013 including the Rules made thereunder, as amended from time to time.

4.2 **"Applicable Laws"** shall mean the Act and Rules made thereunder, the IT Act and rules made thereunder, the Central Electricity Authority (CEA) Guidelines, the Digital Personal Data Protection Act, 2023, the Listing Regulations (as defined hereafter), and

/ or such other Act, Rules or Regulations, which are / may be applicable to the Company for protecting its information, assets, products and solutions from internal and external cyber threats and for reporting such threats.

4.3 **"Board"** or **"Board of Directors"** shall mean the Board of Directors of the Company.

4.4 **"Company"** or **"SEL"** shall mean Suzlon Energy Limited.

4.5 "**CEA Guidelines**" means all Cyber Security Guidelines, Rules and Regulations given by CEA for the Power Sector and any other applicable guideline or regulation passed by the Central Electricity Authority for protecting the power infrastructure against cybersecurity threats.

4.6 **"Cyber Security"** means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction.

4.7 **"Information Technology"** or **"IT"** shall include the full spectrum of information processing technology, including software, hardware, communications technology, and related services, as well as the processes implemented for their support and management.

4.8 **"IT Act"** shall mean the Information Technology Act, 2000 including the rules made thereunder, as amended from time to time.

4.9 **"Listing Regulations"** shall mean the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended from time to time, together with the circulars issued thereunder, including any statutory modification(s) or re-enactment(s) thereof for the time being in force.

4.10 **"Operational Technology"** or **"OT"** shall include all hardware, software, processes and policies provided as part of the products, solutions and services, including: hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems, as well as associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

4.11 **"Policy"** or **"this Policy"** shall mean the Cybersecurity Policy.

4.12 **Interpretation** – In this Policy unless the contrary intention appears, words and expressions used and not defined in this Policy but defined in the Applicable Laws shall have the meanings respectively assigned to them in those Applicable Laws.

5. Review of the Policy and disclosure requirements:

5.1 The Policy has been implemented w.e.f. 5th April 2024 and has been amended with effect from 15th February 2026.

5.2 The Policy shall be disclosed on the website of the Company and a weblink shall be provided in the Annual Report.

5.3 The Policy is subject to annual review as per Applicable Law. The Policy will be reviewed periodically by the Chief Information Security Officer ("Head of Information

Security") to check for its effectiveness, changes in technology, changes in risk levels, and changes in Applicable Law.

5.4 To the extent any change or amendment is required due to changes in Applicable Laws, the Head of Information Security, in consultation with the CIO shall pursuant to the review, update the Policy where required. However, any major change to the Policy shall be placed before the Board for noting and necessary ratification.

5.5 The Policy is subordinate to the Listing Regulations or other applicable statutory provisions including the Act, and in the event of inconsistency between the Policy and the Applicable Laws (including due to subsequent amendments to the Applicable Laws), the provisions of the Applicable Laws will prevail.

6. Objective of the Policy

6.1 The power and energy sector is undergoing a rapid transformation driven by digitalization and modern technologies. These advancements deliver significant benefits, including improved efficiency, sustainability, and progress toward a greener environment. However, with increased connectivity and reliance on digital platforms, the sector faces heightened exposure to cyber threats.

6.2 A robust cybersecurity framework protects sensitive information and critical infrastructure from malicious attacks, whether on the cloud, across applications, networks, or connected devices. Effective cybersecurity measures not only mitigate risks but also strengthen organizational resilience, ensuring business continuity and compliance with regulatory standards.

6.3 By prioritizing cybersecurity, the Company aims on building strong defences against evolving threats, safeguard operational integrity, and maintain stakeholder trust. This policy accordingly sets out the principles, responsibilities, and practices necessary to achieve these objectives and support the secure adoption of digital technologies in the energy sector and providing a comprehensive framework for managing and mitigating cybersecurity risks. It aims to ensure the protection of critical information assets, systems, and infrastructure from evolving cyber threats. By implementing an integrated set of security measures, this Policy seeks to provide a framework to create a secure operating environment that supports the Company's business objectives and digital transformation initiatives including for maintaining the availability, integrity, and confidentiality of information—which are key elements that underpin Suzlon's competitive advantage, regulatory compliance, and overall information security posture. This Policy reinforces the Company's commitment to safeguarding its digital ecosystem and ensuring resilience against cyber incidents.

6.4 Main Objectives

1. **Strategic Alignment**
   Align cybersecurity initiatives with the organization's business strategy to ensure security supports and enables overall organizational objectives.
2. **Risk Management**
   Identify, manage, and mitigate cybersecurity risks to reduce potential impacts on information resources to an acceptable level.
3. **Information Technology (IT) and Operational Technology (OT) Security**
   Establish IT and OT cybersecurity measures to protect critical infrastructure by:
   - Providing relevant product offerings that support security throughout the asset lifecycle.

- Customizing solutions to meet organizational strategy, internal legislative requirements, and regulatory environments.

4. **IT and OT Environment Protection**
   Secure the IT and OT environment by implementing necessary security controls, processes, and policies to safeguard against threats and vulnerabilities.

7 Classification of Cybersecurity

7.1 Cybersecurity measures of Suzlon are classified into two segments:

a. Information Technology Cybersecurity
b. Operational Technology Cyber security

a. Information Technology Cybersecurity

- **Information security -** Information security protects critical information from unauthorized access, identity theft and protects the privacy of information and hardware that use, store, and transmit data. Examples of Information security: Authorization of user and Cryptography.

- **Network security -** Network security protects the usability, integrity and safety of a network, associated components, connection, and information shared over the network.

- **Application security -** Application security protects applications from threats that occur due to the flaws in application design, development, installation, and upgrade or maintenance phases.

b. Operational Technology Cyber security

- Operational technology (OT) security designs meet the security needs of OT environments. This includes protecting system availability, understanding OT-specific protocols, and blocking attacks targeting the legacy systems commonly used in OT environments.

- OT Security comprises technologies, organizational measures, and processes aimed at monitoring and protecting the availability and integrity of the systems, including hardware, software, processes and policies provided as part of the products, solutions and services, hardware and software systems such as SCADA, networked electronic sensing, and monitoring and diagnostic systems, as well as associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

8 Cybersecurity Framework

8.1 The Cybersecurity framework has been set up with well-organized approach towards the periodic risk assessments, preventive measurements against the identified risks, implementation of the security framework like ISO 27001:2022, governance of the critical assets with the help of policies and processes, and periodic review of the security health check.

8.2 The IT and OT team is responsible to maintain the Cyber Security for IT/OT Infrastructure respectively under the governance of Information Security Management (ISM) Team. Technology and technical solutions such as Antivirus, Firewalls, DLP, VPN, File Encryption and multi-factor authentication within IT and OT infrastructure have been implemented to protect against risks.

8.3 The Cyber Security Framework has been implemented to reduce the loss that can be incurred from digital attacks that compromise the availability, validity, confidentiality, integrity, and dependability of data and assets.

8.4 On occurrence of security incidents, internal team identifies the causes and take the necessary steps to minimize and negate the impact and ensure that there is no repeat incident of such security threats.

8.5 The Cybersecurity Framework works on the following principles:

- Safeguarding the Company's critical information and technology assets from Cybersecurity threats.
- Strengthen cybersecurity awareness among employees, contractors, suppliers, vendors, customers, and business partners, while building technological capabilities to support the Company's business growth.
- Encourage timely reporting of cybersecurity incidents and implement robust prevention, response, and recovery mechanisms to minimize potential damage and operational impact.
- Encourage active participation in policy advocacy through trade associations and industry platforms to influence and strengthen cybersecurity regulations.
- Foster strong alliances with organizations, government authorities, and major associations to shape the future of cybersecurity.
- Ensuring company-wide adherence to all cybersecurity-related regulatory requirements.
- Develop adaptive processes and ensure resource readiness to address emerging technologies and evolving threat landscapes.
- Having in place security safeguards to prevent personal data breach, as specified by Applicable Law, and such measures to control access to the computer resources in compliance with Applicable Law and the Data Privacy Policy.

8.6 The Cyber Security Framework comprises of the domains:

1 <u>Cyber Risk Assessment and Mitigation Plan (CRAMP)</u>

1) The **Information Security team** shall maintain the risk register, which will be periodically reviewed by the **Head of Information Security**.
2) The severity of risks shall be determined and maintained based on their likelihood and probability of occurrence.
3) Risks related to end-of-life (EOL) and end-of-support (EOS) assets shall be maintained separately and reviewed every **three months.**
4) The Company shall implement alternate security controls to minimize the impact of identified risks.
5) The Company shall review the risk register at least **once every year**.

6) The Company shall only allow secured use of external removable and mobile devices including restriction on the use of Bring Your own Device (BYOD) within critical & associated networks.

The following steps shall be taken for risk identification:

1. Activate crisis response protocols immediately upon declaration of a critical incident.
2. Suspend non-essential system changes and deployments during the crisis period.
3. Coordinate internal communications to ensure accurate and timely information flow to management and employees.
4. Manage external communications, including regulators, customers, vendors, and media, through approved spokespersons.
5. Engage external forensic experts, legal advisors, or cybersecurity specialists where required.
6. Monitor crisis response effectiveness and adjust strategy as needed.
7. Conduct a post-crisis review to assess decision-making, response adequacy, and improvement opportunities.

2 Asset Management

1) The Company to shall maintain Asset Register that includes all critical assets.
2) Risks related to asset shall be evaluated periodically and documented in the risk register.
3) All assets shall be protected with appropriate security controls, including but not limited to access management, encryption, and monitoring.
4) The designated asset owner shall ensure the hygiene, integrity, and compliance of the assets under their control.
5) Documented guidelines for acceptable usage of assets shall be created and communicated to all asset owners.
6) Assets that have reached End of Life (EOL) or End of Support (EOS) shall be recorded separately within the Asset Register for proper tracking and risk management.
7) All Public IPs shall be register with Cyber Swachchata Kendra **(CSK)**
8) Assets / Information shall be securely disposed of upon completion of their lifecycle and in accordance with applicable requirements.

3 Physical Security

1) All critical IT and OT infrastructure including servers, SCADA systems, network assets, PLC devices, turbines, and other essential components must be housed in physically secured environments.
2) Access to secured / restricted premises shall be allowed to authorized members.
3) All necessary hazardous materials and associated safety equipment shall be stocked and readily available at designated locations to effectively manage and mitigate disaster situations.

4 Access Control

1) All IT and OT assets shall be safeguarded with appropriate security controls to defend against cyber threats, vulnerabilities, and attacks.
2) Access to data stored on IT and OT systems shall be restricted to authorized users only, following the **Principle of Least Privilege**.
3) Access to network infrastructure components such as firewalls, switches, and routers shall be limited to authorized personnel only.
4) Internet connectivity for OT systems shall be restricted and granted only upon approval from the **Head of Information Security**.
5) The **Head of Information Security** shall periodically review and validate all Internet access permissions for OT systems to ensure compliance and security.

5 Patch and Vulnerability Management

1) All security patches and necessary controls shall be deployed promptly on all assets to mitigate identified vulnerabilities and reduce security risks.
2) All critical assets shall undergo vulnerability checks at least **once every year** to ensure compliance and identify potential weaknesses.
3) Any critical vulnerability discovered shall be addressed and remediated within the defined timelines as per the organization's vulnerability management standards.
4) The **Network Team** shall be responsible for closing the reported vulnerabilities by **CSK** within the stipulated timelines.
5) Periodic vulnerability assessments and scans on critical IT and OT assets shall be conducted. Prioritizing remediation of critical and high-risk vulnerabilities within defined timelines.
6) Compensating controls shall be implemented where patching is not immediately feasible, especially for legacy OT systems.
7) Vulnerabilities reported by Cyber Swachchata Kendra shall be tracked and timely closure shall be ensured.
8) Records of vulnerabilities, remediation actions, and residual risks shall be maintained along with reviewing vulnerability trends to enhance preventive security measures.

6 Change Management

1) A change management process shall be implemented for all IT and OT assets. This process will include planning, approval, testing, implementation, and documentation of changes.
2) Any changes to critical assets—such as configuration settings, security parameters, privileged access, hardware, or software—must be:
   a. Logged in the Change Management System.
   b. Reported to the Head of Security for review and compliance.
3) Emergency changes, particularly those related to security vulnerabilities or incidents, must be addressed immediately.
4) Such changes should follow an expedited approval process and be documented post-implementation.

7 Cyber Security Incident Response Plan

1) The Company shall establish and enforce a comprehensive **Incident Management Policy** and associated procedures to effectively detect, analyse, respond to, and recover from cybersecurity incidents.
2) A documented **Cyber Crisis Management Plan (CCMP)** shall be maintained and referred to during Cyber incidents to ensure coordinated and timely response.
3) The **Information Security Division (ISD)** shall operate on a 24x7 basis to monitor, detect, and address cybersecurity incidents promptly.
4) All incidents shall be classified based on severity (e.g., Critical, High, Medium, Low) and tracked until formal closure. Incident records shall include root cause analysis and corrective actions.
5) The Information Security team shall be responsible for reporting any major cybersecurity incident or outage to relevant regulatory bodies in compliance with applicable laws and industry standards.
6) The Information Security team shall maintain detailed reports of all cybersecurity incidents, including timelines, actions taken, and lessons learned, for audit and continuous improvement purposes.
7) Establish continuous monitoring mechanisms through SOC tools, system logs, and threat intelligence feeds to detect anomalies and potential incidents.
8) Mandate immediate reporting of suspected cybersecurity incidents by employees, contractors, and third parties through defined escalation channels.
9) Isolate affected systems and networks to prevent lateral movement and further compromise.
10) Revoke or suspend compromised credentials and enforce emergency access controls.
11) Identify and remediate root causes through forensic analysis, patch deployment, and configuration hardening.
12) Restore systems and data from validated backups in accordance with defined recovery objectives.
13) Report notifiable incidents to CERT-In, CEA, SEBI, or other authorities as required under Applicable Law.
14) Document incident details, response actions, lessons learned, and preventive measures.
15) Review incident trends periodically and update controls to reduce recurrence.

8 Cyber Security Backup and Disaster Incident Recovery Plan

1) All critical assets, including systems, applications, and data, shall be identified and backed up periodically to ensure data availability and resilience against disruptions.
2) The IT team is responsible for performing periodic backups of all IT infrastructure components, ensuring integrity and recoverability.
3) A disaster recovery plan for critical infrastructure shall be implemented. Copies of periodic backups will be securely maintained to support disaster recovery objectives.
4) Failover mechanisms for critical assets shall be identified, assessed, and implemented to minimize downtime during disruptions or system failures.

5) Automated and secure backup mechanism with encryption for data at rest and in transit shall be implemented. Backup failures, restoration issues, and corrective actions shall be documented.
6) Offline, offsite, or immutable backups shall be maintained to protect against ransomware and data corruption.
7) Test backup restoration processes at defined intervals to validate data integrity and recoverability.
8) Review and update disaster recovery arrangements following major incidents or system changes.

9 Business Continuity

1) The Company shall establish a Business Continuity Plan (BCP) to ensure resilience and continuity of critical operations.
2) The BCP must be reviewed, updated, and tested at defined intervals to validate its effectiveness and alignment with organizational objectives.

10 Data Protection and Privacy Policy

1) The Company shall establish a Data Protection and Privacy Policy in compliance with the Digital Personal Data Protection Act, 2023 and Applicable Law which shall include encryption for sensitive data when data is at rest on the device or on a removable media or in transit.
2) Sensitive data, such as Personally Information (PII), stored on or sent to or transmitted from telecommuting devices shall be protected from unauthorized access or corruption.

11 Cyber Security Training Program

1) Mandatory annual cybersecurity awareness training for all personnel **shall be conducted**.
2) Role-specific cybersecurity training for administrators, developers, OT operators, and security teams **shall be provided** based on access levels and responsibilities.
3) Periodic cybersecurity awareness campaigns addressing phishing, social engineering, and data protection risks **shall be conducted**.
4) Simulated cyberattack and phishing exercises **shall be conducted** to assess awareness levels and response readiness.
5) Records of training attendance, assessment results, and exercise outcomes **shall be maintained** for audit and compliance purposes.
6) Cybersecurity training content **shall be periodically reviewed and updated** based on emerging threats, regulatory developments, and lessons learned from incidents.

12 Data Retention Policy

In terms of the Data Retention Policy documents, records data and information shall be retained:

1) backup of data of critical systems.
2) logs, risk assessment, and approval for grant of remote access to critical systems.
3) logs and approval associated with interconnection of OT system with IT system.
4) certificates of cyber security tests, results, cyber security audit reports, and other documents as mandated under Applicable Law
5) record of changes, including software updates and patches, implemented in critical systems.

9 Compliance

1) Responsibility and Accountability

a. Compliance with this Cyber Security Policy and all associated Plan and procedures shall be mandated for all Users having access to the Company's IT or OT systems or information assets.
b. The Board shall have the overall oversight of cybersecurity governance. For the convenience of the Board, the Head of Information Security shall ensure organisational enforcement of the policy and shall be responsible and accountable for implementation, monitoring, regulatory reporting, and enforcement of this Policy.
c. The IT, OT and Information Security Teams shall execute required controls, monitoring, audits, and remediation actions.
d. All Users shall comply will the Policy, complete mandatory training and promptly report cybersecurity incidents or violations.
e. Compliance shall be monitored through audits, reviews, and continuous security monitoring. Any exception to this Policy shall be formally approved in writing, time bound and periodically reviewed.

2) Procedure

a. All reports, complaints, incidents, vulnerabilities, doubts, or concerns relating to this Policy shall be reported to the Head of Information Security.
b. Any suspected or actual violation of this Policy shall be examined and investigated by the Head of Information Security in accordance with the Incident Response Plan.
c. The Head of Information Security shall maintain a centralised compliance and incident log, recording the nature of the issue, date of reporting, systems impacted, actions taken, and closure status.
d. Compliance shall be monitored through continuous monitoring tools, system logs, access reviews, vulnerability assessments, internal audits, and periodic compliance reviews conducted by the Security, IT and OT teams.
e. Records shall be retained for a period of One (1) year.

3) Cyber Security Audit

Audits shall be conducted to ensure compliance with the information security policies, procedures, and guidelines for IT infrastructure.
(A) Twice every financial year by the internal team
(B) Once every financial year by external resources.

4) Enforcement

Enforcement of this Policy is mandatory, and violations of this Policy will be reported through the Security Operations Management Team (SOC) procedure. The action taken after a violation is encountered is as follows:

- All violations will be reported to ISM.
- Any person violating the Policy will be issued a warning or will face stricter action depending upon nature of incidence, including whether the offender is a first-time offender.
- Any further violation on part of the offender will result in strict disciplinary action against the person and can lead to termination of employment.

*****