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

2. Purpose of this Policy

2.1 The Cybersecurity Policy of Suzlon Energy Limited ("**SEL** or the "**Company**") aims to establish the basic principles and the general framework for the control and management of Cyber Security risks faced by the Company and for that purpose provide an integrated set of protection measures that must be uniformly applied across the organization to ensure a secured operating environment for its business operations.

2.2 The availability, integrity and confidentiality of information are essential in building and maintaining the competitive edge, legal compliance and information security for the Company.

2.3 The Cybersecurity framework contains the rules and regulations that set the organizational, procedural, and technical requirements for protecting the Company's information, assets as well as products, solutions and services from internal and external cyber threats and enhance the resilience of the businesses.

3. Applicability of this Policy

3.1 The Policy applies to Suzlon Energy Limited and its Material Subsidiaries.

3.2 This Policy covers all employees, contractors, interns / trainees working in Suzlon. This Policy also covers business partners, vendors, suppliers, customers, third party service providers providing development / support / network / hardware services. This Policy will also apply where data of the Company is held outside the Company's premises.

3.3 This Policy may be adopted by other subsidiaries of the Company subject to suitable modifications, if and to the extent required.

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

4.6 "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.

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

4.8 "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.

4.9 "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.

4.10 "Policy" or "this Policy" shall mean the Cybersecurity Policy.

4.11 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 This Policy has been implemented w.e.f. 5th April 2024.

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

5.3 The Cyber Security Policy is in compliance of Applicable Law and is subject to annual review as per Applicable Law. The policy will be reviewed by the Chief Information Security Officer ("CISO") in compliance with the business, legal and statutory requirements and approved by the Board.

5.4 To the extent any change or amendment is required due to change in the Applicable Laws, the CISO, in consultation with the CEO shall be authorised to review and amend the Policy to give effect to any such changes or amendments. Such amended Policy shall be placed before the Board for noting and necessary ratification.

5.5 This Policy is subordinate to the Listing Regulations or other applicable statutory provisions including the Act, and in the event of inconsistency between this 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 In today's world, with the rising needs of digitalisation and modern technology in the power energy sector have undeniable benefits and are major drivers towards green environment. A robust cybersecurity system helps to protect key information and devices from cyber threats against vulnerable attacks that possess threat to important information, may it be on the cloud, across various applications, networks, and devices. Moreover, an effective cybersecurity builds the capabilities of strong defence against threats and preservation of organizational information.

6.2 Cyber assets are under constant threat from attacks which can cause serious damages of critical information equipment (with potential cascading failures in other interconnected assets), data loss, information transfer to unauthorised / illegal entities, environmental damage, widespread electricity supply disruption with devastating impacts on critical services, assets and operations, and reputational damage.

6.3 The policy aims to establish the basic principles and the general framework for the control and management of Cyber Security risks faced by Suzlon and for that purpose provide an integrated set of protection measures that must be uniformly applied across the organization to ensure a secured operating environment for its business operations. The availability, integrity and confidentiality of information are essential in building and maintaining the competitive edge, legal compliance and information security for Suzlon.

6.4 The main objectives of the Cybersecurity Policy is to:

- Align cyber security with business strategy to support organisational objectives.
- Manage and mitigate risks and reduction of potential impacts on information resources to an acceptable level
- Establish Operational Technology (OT) Cybersecurity to protect critical infrastructure by providing relevant product offerings supporting security throughout the lifecycle of the asset, customized to meet strategy, internal legislative and regulatory environments
- Secure the OT environment by implementing the necessary security controls, process and policies.

7. Classification of Cybersecurity

7.1 Cyber Security 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. Basic Principles of Cybersecurity at Suzlon

8.1 The Cybersecurity policy is based on the following basic principles:

- Protect the company's critical information and technology assets from Cyber Security threats.

- Raise awareness of Cyber Security risks among employees, contractors, and associates through Cyber Security programs and workshops, amongst others.

- Improve the employees, contractors, suppliers, vendors, customers, business partners, and others awareness on Cyber Security related risks and threats, as well as build technological capabilities to meet the objectives of the Company.

- Promote the incident reporting, prevention, recovery, and response mechanism within the Company, such that the potential damage and harm is limited.

- Ensure that information security and incident reporting is a part of employees' performance evaluation. Ensure participation in the policy advocacy through trade associations and other platforms to influence and strengthen the policies and regulations pertaining to information and Cyber Security.

- Collaborate with organizations, government agencies and major associations to contribute to the improvement of Cyber Security.

- Ensure regulatory compliance related to the areas of Cyber Security throughout the company.

- Conduct adequate research and development activities to ensure up-to-date Cyber Security protection and assessments.

- Provide the processes and resources to quickly adapt to changes in the emerging technology and new threats.

9. Cybersecurity Framework at Suzlon

9.1 The Cyber Security 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 27001:2013, governance of the critical assets with the help of policies and processes, and periodic review of the security health check.

9.2 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.

9.3 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.

9.4 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.

9.5 The Cyber Security Framework at Suzlon comprises of the domains:

a. Risk Identification

This contemplates identification of risks, implementing controls and processes to maintain and develop security capabilities, which includes the following objectives:

- Promotion of the Cybersecurity of organisation within the company by adopting continuous risks assessments and reduction of level of exposure
- Ensuring compliance with commitments to stakeholders (shareholders / regulators / customers / suppliers).
- Standardising and maintain a risk-based Cybersecurity governance model, implement right standards and supervised controls that optimise resource investment.

b. Risk Prevention

This contemplates:

- Prevention against identified threats, risks during the Risk assessments / GAP assessments
- Implement the security tools and applications to prevent the virus, malwares, external attacks
- Vulnerabilities Assessments to address the legacy and unprotected systems with precautionary Measurements
- Security Awareness to prevent human incidents

c. Risk Protection

This contemplates:

- Protection against threats, viruses, data loss by implementing the required controls, solutions before the risk materialises,
- Risk Treatment to the identified risks to reduce impact by applying the necessary protection strategies.

d. Risk Detection

This will involve:

- Detection of threats through the use of multiple intelligence and authorised advisory sources in order to be able to proactively manage them with appropriate tools and technologies.

e. Response to Incident

This will involve:

- Implementing Incident Management procedures and Cyber Crisis Management Plan (CCMP) to address the incidents arises due to cyber threat.
- Ensuring that the incident response activities are carried out in accordance with legal, contractual, and regulatory requirements.
- Ensuring the continuity of the services / restoration of services affected due to incident and lower the impact to the organization
- Ensuring that personnel are trained on how to report a potential incident
- Ensuring that notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements take place in a timely manner.

f. Recovery

This will involve:

- Recovery and restoration of any capabilities or services that were impaired due to a Cybersecurity event.

10. Cybersecurity Governance Model

10.1 The Cyber Security Policy is implemented by the Information Security Management (ISM) Team of Suzlon. The ISM is tasked with the responsibility of enacting and upholding comprehensive information security policies, norms, directives, and protocols across the organization. Their duties encompass delivering educational programs on security awareness and ensuring that all individuals are well-informed about their respective responsibilities in preserving security.

a. Planning

- Identify cyber security requirement to implement security framework and controls.
- Define the scope and boundaries of cyber security program and its implementation strategy.

- Understand the legal and regulatory requirements.
- Estimate Resource, technology, people, logistic and budgetary requirements and ensure adequate arrangement for planning, maintenance and management of Information Security.
- Define risk management framework after planning organisation wide Information Security Management System (ISMS) in accordance with ISO/IEC 27001 Standard and other relevant security standards.

b. Development

- Lead in the development of information security policies, standards, guidelines, processes, and procedures.
- Define formal processes for creating, documenting, reviewing, updating and implementing security policies.
- Design and development of Information and asset classification policy.
- Lead and coordinate development of organisation specific information security policies, procedures, guidelines and processes in consultation with various stake holders.

c. Management

- Dissemination of information security policies, procedures and guidelines.
- Conduct risk assessments, manage incidents, and provide internal and external reporting.
- Involvement in security awareness education and training.
- Integration of information security processes with organisation's business processes.
- Periodic evaluation and review effectiveness of information security policies, procedures, standards, guidelines and processes etc.
- Maintain a record of information security incidents and breaches including for the statutorily prescribed timelines.
- Coordinate and lead in implementation of 'Business Continuity Plan' and conduct mock drills to evaluate effective implementation of the same.
- Ensure HR management policies adequately incorporate Information Security Guidelines, including entry and exit checks such as Character and Antecedents check and exit management strategies.
- Secure disposal of E – Waste.
- Ensure that all information systems within the organisation are adequately patched and updated.
- Interface regularly with the core organisational Perspective planning Team to remain abreast of new technologies / equipment being considered for deployment within the organisation, and evaluate their possible implications on existing systems.

d. Oversight

- Evaluate the effectiveness of ongoing security operational processes, monitor compliance for internal and external requirements.
- Evaluate compliance with respect to legal and regulatory requirements for information security.
- Carry out a review of cyber risk assessment at least once in a quarter. The actionable of risk treatment and mitigation shall be tracked in this review for its effectiveness.

- Perform information security audit at least annually or whenever significant changes have been made in IT Systems/Infrastructure.

e. Building cyber resilience

- Ensure the maintenance of a state of informed preparedness to forestall compromises of mission/business functions from adversary attacks.
- Continue essential mission/business functions despite the successful execution of an attack by an adversary.
- Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber-attacks.
- Restore mission/business functions to the maximum extent possible after the successful execution of an attack by an adversary.
- Ensure adequate evolution to the missions/business functions and/or the supporting cyber capabilities, to minimize adverse impacts from actual or predicted adversary attacks.

10.2 The CISO shall also be assisted by various departments in ensuring its effective implementation. The governance model is aligned with the ISO 27001:2013 standards.

10.3 Other additional activities to be undertaken by the ISM are:

- Ensuring implementation and formulation of a cyber-crisis management plan, business continuity plan and disaster recovery plan.
- Conduct background checks and audits to ensure Cyber Security and mitigate cyber risks.
- Share information regarding any incident which may occur with the competent authorities.

11. Compliance

To ensure compliance with the Policy, compliance is three-fold:

a. Compliance with requirements

- The Company works to ensure compliance of requirements under Applicable Law including any compliance requirements of of various government agencies.

b. Compliance with Cybersecurity policy and procedures

- An Information Security Management Framework and Information processing facilities shall be used as per information security policy and acceptable usage policy for monitoring compliance;
- Exception to security policy and procedure shall be approved through the exception management process;
- Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.
- Violations or any attempted violations of security policies and procedures shall result in disciplinary actions.

c. Information Systems Audit

- Audits shall be conducted to ensure compliance with the information security policies, procedures and guidelines.

12. Enforcement

12.1 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.
- Person will be issued a warning or will face stricter action depending upon nature of incidence, for first time of violation.
- Any further violation on part of the same person would result in strict disciplinary action up to termination of employment.

*****