SOLEX ENERGY LIMITED

Cyber Security Policy

(Approved by the Board of Directors in its Meeting dated August 7, 2025)

1. Purpose

The purpose of this Cyber Security Policy is to protect Solex Energy Limited (Solex) digital assets, sensitive information, and infrastructure from cyber threats and ensure business continuity. It establishes responsibilities, acceptable practices, and security controls across all departments to safeguard against data breaches, cyberattacks, and misuse of company resources.

2. Scope

This policy applies to:

- All employees, contractors, consultants, vendors, and third-party users
- All IT infrastructure: servers, networks, devices, emails, software, applications, cloud services
- All data handled by the company, including internal, customer, OEM partner, vendor, and project data

3. Key Principles

- **Confidentiality** – Only authorized individuals should access sensitive data.
- **Integrity** – Data should be accurate, consistent, and protected from unauthorized changes.
- **Availability** – Systems and data must be accessible when required by authorized users.

4. Roles and Responsibilities

Role	Responsibility
IT Department	Implement and maintain cybersecurity infrastructure and protocols
Department Heads	Ensure team compliance with cybersecurity policies
Employees	Adhere to safe IT practices and report suspicious activities
Third-party Vendors	Follow security requirements as outlined in contracts and NDA's

5. Security Controls

5.1 Access Control

- Passwords must be strong and changed regularly
- Multi-Factor Authentication (MFA) will be enforced where possible
- Access to sensitive data is granted based on the principle of least privilege

5.2 Endpoint Protection

- All company devices must have updated antivirus and anti-malware software
- Unauthorized software installation is prohibited
- Removable storage must be scanned before use

5.3 Network Security

- Firewalls and intrusion detection/prevention systems (IDS/IPS) will be used
- VPN must be used for remote access
- Wi-Fi networks must be encrypted and password-protected

5.4 Email and Communication Security

- Phishing awareness training will be conducted regularly
- Attachments and links must be handled cautiously
- Official communications must use the company's secured email domain

5.5 Data Protection

- Regular data backups must be performed
- Sensitive data must be encrypted during transmission and storage
- Confidential project and OEM data must be shared through secured channels only

6. Incident Management

- All employees must report cybersecurity incidents (e.g., phishing attempts, data breaches, unauthorized access) immediately to the IT Department
- A formal incident response plan will be followed, including containment, eradication, recovery, and post-incident analysis

7. Training and Awareness

- Mandatory cybersecurity awareness sessions will be conducted at least annually
- Specialized training will be provided to departments handling critical data (e.g., Sales, Purchase, Automation)

8. Third-Party and OEM Security

- All third parties must comply with Solex's cybersecurity and data protection standards
- NDA's and contractual clauses must include cybersecurity obligations
- Access to Solex systems by third parties must be monitored and restricted

9. Policy Violations

Violations of this policy may result in disciplinary action, including termination of employment or contracts and potential legal consequences.

10. Review and Updates

This policy will be reviewed every three (3) years or as needed based on emerging threats or changes in business operations.