



## ACME SOLAR HOLDINGS LIMITED

### ENTERPRISE CYBER SECURITY POLICY

#### 1. Introduction

ACME Solar Holdings Limited (“ACME” or the “Company”) recognizes that its information and cyber assets are fundamentally essential for its business operations and effective customer service. We are committed to establishing and improving our cyber security posture to safeguard these assets by ensuring their confidentiality, integrity, and availability at all times.

#### 2. Purpose

This Policy establishes the management framework to protect our stakeholders, brand, and reputation from cyber risks that could disrupt our business.

#### 3. Applicability

This Policy is applicable to (a) the Company, its subsidiaries, joint ventures and affiliates where it exercises management control; (b) their respective employees, whether permanent, contractual, trainees or interns; (c) vendors, service providers, consultants and value chain partners; and (d) any third party working for or associated with the Company. It covers all information, computer systems, communication services, and cyber systems owned or licensed by ACME, including all personnel from external organizations with access to ACME's network and resources.

#### 4. Guiding Principles

- a. **Shared Responsibility:** All employees and users of ACME's resources are responsible for understanding and adhering to this Policy. All functional heads are directly responsible for ensuring compliance within their respective domains.
- b. **Risk-Based Approach:** The Company's security efforts will be prioritized based on risk. The Company will apply effective risk management to formally identify, treat, and mitigate current and expected cyber risks to an acceptable level.
- c. **Operational Resilience:** The Company will maintain and test a Business Continuity Plan for all business-critical information and cyber assets to ensure efficient recovery from any material disruptions.
- d. **Compliance by Default:** The Company will ensure compliance with all applicable legal, statutory, regulatory, and contractual requirements. This Policy is designed to align with applicable laws and recognized standards like ISO/IEC 27001.
- e. **Continuous Improvement:** The Company's information security systems shall undergo continual improvement to ensure the integrity and protection of data across all operations.

#### 5. Key Policy Areas

- a. **Information Governance:** Critical information shall be protected from unauthorized access, use, disclosure, modification, and disposal. Its confidentiality, integrity, and availability shall be ensured whether it is at rest, in transit, or being processed. Formal transfer policies and controls shall be in place for all communications facilities.

- b. **Access Control:** Access to sensitive and confidential resources shall be restricted to authorized users only, and any unauthorized use of another user's identity is strictly prohibited.
- c. **IT/OT Infrastructure Security:** Robust systems shall be established for monitoring, detecting, and responding to information security threats. This includes implementation of network security controls such as firewalls, encrypted channels for remote administration, and disabling services not needed for business. A formal Change Management Process must be followed for any modifications to devices.
- d. **Third-Party Risk Management:** Information security requirements shall be established and enforced for all third parties, including vendors and consultants, to safeguard our data and systems. Secure information transfer agreements including any confidentiality or non-disclosure agreements (NDAs) shall be executed with external parties before sharing any data/information.
- e. **Incident Response & Resilience:** All actual or suspected breaches of cyber security shall be reported and investigated by designated personnel. Appropriate corrective and preventive actions will be initiated to manage the incident and prevent recurrence.
- f. **Acceptable Use of AI:** The principles of protecting confidentiality, integrity, and availability apply to any data which may be used for training and operating AI models.

## 6. Roles & Responsibilities

- a. **All Employees, Vendors, and Partners:** Responsible for compliance with this Policy.
- b. **Business/Department Heads:** Responsible for ensuring Policy compliance within their respective domains and conducting self-assessments.
- c. **IT Department:** Responsible for Network Security.
- d. **Legal Department:** Responsible for establishing and reviewing appropriate contractual terms including any confidentiality or non-disclosure agreements.

## 7. Training and Awareness

ACME believes that informed and aware individuals form the foundation of effective cyber security. To support this, ACME will:

- a. Provide regular, role-based cyber security trainings.
- b. Conduct awareness programs that promote safe digital practices, phishing prevention, responsible use of technology, and secure handling of data.

## 8. Monitoring and Risk Management

ACME shall deploy robust monitoring mechanisms across its IT and OT environments to ensure early detection of anomalies, unauthorized activities, and emerging threats. Monitoring activities will include:

- a. Continuous network surveillance, log review, and alert analysis.
- b. Automated and manual monitoring tools to ensure visibility across all critical systems.
- c. Regular vulnerability assessments and threat-hunting exercises.
- d. Ongoing review of user access, administrator privileges, and system changes.

Cyber risk management will be embedded into organizational decision-making through:

- a. Formal risk identification, assessment, and prioritization.
- b. Implementation of preventive and corrective controls based on impact.
- c. Ongoing review of risks associated with new technologies and third-party engagements.
- d. Maintenance of updated cyber risk registers reviewed by senior leadership.

**9. Governance and Implementation**

The Board of Directors is responsible for the approval and oversight of this Policy. The Corporate Social Responsibility and Sustainability Committee of the Board shall oversee the implementation of this Policy and review its effectiveness periodically. Senior management and the relevant functional heads shall be responsible for operationalising this Policy across the Company's operations and ensuring compliance with its requirements.

**10. Review and Amendment**

This Policy is approved by the Board of Directors of ACME. This Policy shall be reviewed periodically, or earlier if warranted by changes in applicable laws, regulations, business operations, or stakeholder expectations. Any material changes to this Policy shall be subject to the approval of the Board of Directors.

**11. Version History:**

Date of Board Approval	Particulars	Effective Date
27 <sup>th</sup> March 2026	Introduction and implementation of Enterprise Cybersecurity Policy	27 <sup>th</sup> March 2026