SINENG Electric Co., Ltd.

Information Security Management Systems Manual

To sharpen the Company's information security management capabilities, ensure the normal conduct of business activities, and prevent losses to the Company and its customers arising from information security incidents, including interruptions to information systems, data loss, and disclosure of sensitive information, the Company has undertaken efforts to implement the international standard *Cybersecurity—Information Security Management Systems—Requirements* (GB/T 22080-2025 / ISO/IEC 27001:2022). Accordingly, the Company has established, implemented, and committed to constantly improving a documented Information Security Management System (ISMS) and has formulated the *Information Security Management Systems Manual*.

The *Information Security Management Systems Manual* is a regulatory document of the Company and serves as the overarching framework and code of practice for establishing and implementing the Company's ISMS. It provides the basis for implementing the Company's information security management policies and objectives, ensuring the valid operation and ongoing improvement of the ISMS, and demonstrating the Company's commitment to society.

All employees shall strictly comply with the requirements of the *Information Security Management Systems Manual*, consciously adhere to the information

security management policies, implement all requirements set forth herein, and work diligently to achieve the Company's information security management policies and objectives.

The *Information Security Management Systems Manual* is formulated, reviewed, and approved by the Company's Information Security Management Committee, which is responsible for tracking its progress and conducting periodic reviews.

1. Management Scope

1.1. General Provisions

To establish, implement, operate, monitor, review, maintain, and improve a documented ISMS, define information security policies and objectives, effectively manage information security risks, ensure that all employees understand and comply with the ISMS, and continuously improve the effectiveness of the ISMS, this Manual is hereby established.

1.2. Scope of Coverage

The Manual sets out the basic requirements for information security governance and management at SINENG Electric Co., Ltd., covering organizational responsibilities, handling of information security risks, planning of objectives, supportive resources, operational controls, performance evaluations, and ongoing improvements.

This Manual applies to the Company's information security management

activities. The specific scope covered by the GB/T 22080-2025 / ISO/IEC 27001:2022 ISMS certification shall be as stated in the valid certification certificate.

This Manual incorporates all requirements set forth in the main body of GB/T 22080-2025 / ISO/IEC 27001:2022, with no requirements deemed inapplicable.

2. Information Security Management Organizational Structure

(1) Information Security Management Committee:The Information Security Management Committee is the highest-level organizational body responsible for information security management within the Company. It is responsible for collective decision-making and coordination on major matters concerning the Company's ISMS and assumes responsibility for the Company's information security management.The Committee conducts management reviews on a regular basis to evaluate how the ISMS operates.

(2) Management Representative:As authorized by the General Manager, the Management Representative is responsible for establishing, implementing, examining, and improving the ISMS and reporting the Company's information security performance to senior management.

(3) Management Review Team:The Management Review Team conducts management reviews as planned, makes decisions based on audit results and significant changes in the business and management environment, and sets the course for service improvements.

(4) Risk Assessment Team:The Risk Assessment Team is responsible for

preparing the *Risk Treatment Plan*, confirming risk assessment results, and formulating the *Risk Assessment Report*.

(5) Implementation Team:The Implementation Team is responsible for developing procedural documents based on the results of risk assessments and promoting the implementation of the ISMS throughout the Company.

(6) Internal Audit Team:The Internal Audit Team is responsible for preparing internal audit plans, conducting internal audits, and submitting internal audit reports in accordance with the requirements of the *Internal Audit Management Procedure*.

3. Information Security Management Policy and Objectives

To prevent losses to the Company and its customers arising from interruptions to information systems, data loss, and disclosure of sensitive information, the Company has established an ISMS, formulated an information security management policy, and defined information security objectives.

Information Security Management Policy:Heighten information security awareness, manage all types of risks, take a proactive approach to prevention, and pursue ongoing improvement.

3.1. Information Security Management Framework

The Company adopts a systematic approach to establishing an ISMS in accordance with GB/T 22080-2025 / ISO/IEC 27001:2022, with the aim of ensuring the Company's information security across the board.

3.2. Information Security Management Organization

(1) The Audit Committee of the Board of Directors is responsible for overseeing major risks relating to the Company's information security and cybersecurity.

(2) The General Manager, as the person with ultimate management responsibility for information security, assumes overall responsibility for the Company's information security activities. The General Manager is responsible for assessing and managing information security-related risks and major matters, approving information security policies, objectives, and resource allocation, and receiving regular reports on information security management activities.

(3) The General Manager shall appoint a Management Representative responsible for establishing, implementing, examining, and improving the ISMS to ensure its continued suitability and validity.

(4) The Company shall establish an information security organizational structure, including an Information Security Management Committee and an information security coordination body, to ensure the effective operation of the ISMS.

(5) The Company shall maintain regular and ongoing communication with competent authorities, local governments, and relevant professional organizations to keep abreast of security requirements and developments and obtain support for information security management.

3.3. Personnel Security

Information security requires the participation and support of all employees. All employees are responsible for protecting information security, and information security requirements shall be incorporated into employment contracts and job responsibilities. Specific security responsibilities shall be defined for personnel in special positions. The security responsibilities and access rights of personnel shall be promptly adjusted when they are transferred to other positions or leave the Company.

Security requirements and responsibilities shall be clearly defined for relevant parties in connection with the Company's applicable policies.The Company shall regularly provide all employees with information security training sessions covering skills, responsibilities, and security awareness, with the aim of heightening their information security awareness.

All employees and relevant parties must fulfill their information security responsibilities and comply with applicable security policies, procedures, and measures.

3.4. Identification of Information Security Requirements in Laws, Regulations and Contracts

The Company shall promptly identify information security requirements arising from customers, suppliers, service providers, and other business partners, as well as applicable laws and regulations and contractual obligations, and shall implement appropriate third-party information security management

requirements based on the nature of the business and the associated level of risk.

3.5. Risk Assessment

The Company shall establish risk assessment procedures and define risk acceptance criteria based on the characteristics of its business information security environment and applicable legal and regulatory requirements.

The Company shall conduct information security risk assessments on a regular basis, together with vulnerability analyses and technical assessments where necessary, to identify changes in the risk environment. Special risk assessments shall be conducted promptly when significant changes occur in the Company's business or external environment. Appropriate measures shall be implemented based on the results of risk assessments to mitigate identified risks.

3.6. Reporting of Information Security Incidents

The Company shall establish channels for reporting information security incidents and designate the responsible departments for receiving and handling such reports.

All employees are responsible for reporting information security risks, threats, vulnerabilities, and incidents. Upon identifying an information security incident, employees shall immediately report it through the designated channels in accordance with applicable procedures.

The responsible department receiving information security incident reports shall record all reported incidents, take appropriate action in a timely manner, and

provide feedback to the reporting personnel on the outcome of the handling process.

Major information security incidents shall be promptly reported to the General Manager. Where a significant risk is involved, the matter shall be reported to the Audit Committee of the Board of Directors in accordance with the Company's corporate governance procedures.

3.7. Supervision and Inspection

The Company shall conduct regular supervision and inspection of information security, including routine inspections, special-purpose inspections, technical inspections, and internal audits. The Company shall accept ISMS audits conducted by independent third parties and shall continuously maintain relevant ISMS certifications, including ISO/IEC 27001:2022 certification.

3.8. Business Continuity

Based on the results of risk assessments, the Company shall establish business continuity plans to mitigate the impacts of information system disruptions, prevent critical business processes from being severely affected by major information system failures or disasters, and ensure timely recovery of critical business operations.Business continuity plans shall be tested and updated on a regular basis.

3.9. Disciplinary Measures for Violations of Information Security Requirements

Personnel who violate the Company's information security policies,

responsibilities, procedures, or measures shall be subject to appropriate disciplinary action in accordance with applicable rules and procedures.Information Security Objectives:

(1) Customer information leakage incidents: 0.

(2) Unauthorized access incidents: ⩽1 incident

(3) System failures caused by malware: ⩽1 incident

(4) Malware incidents involving servers: zero tolerance

(5) Incidents involving information assets caused by fire, theft, or other hazards: zero tolerance

(6) Implementation rate of information security training plans: ⩾90%

(7) Customer complaints concerning information security: ⩽1 complaint

4. Information Security Management Policy

4.1. General Principles

4.1.1. Purpose

To further bolster information security and strengthen risk controls for the Company's networks, hosts, and information systems, this Information Security Management Policy is hereby established.

4.1.2. Scope

This Policy applies to the information security management of the Company's networks, hosts, and information systems.

4.1.3. Responsibilities

The IT Department is responsible for the information security management of

the Company's networks, hosts, and information systems.

4.2. Password Management Policy

(1) Where required for security purposes, the Technology Center may require users to change their passwords upon login. When a notification indicates that a password has expired and must be changed, the user shall complete the password change.

(2) Where required for security purposes, users may also be permitted to change their passwords directly from their own terminals.

(3) Password validity periods shall be subject to defined limits, with passwords remaining valid only for a specified period.

(4) Where necessary, individual user accounts may be temporarily disabled.

(5) The Company may configure user accounts to allow an unlimited number of login attempts or may impose a limit on the number of login attempts. An account may be disabled after a specified number of failed attempts to mitigate password-guessing attacks through technical controls. Based on system administration requirements, the Company may determine whether remote users are required to be forcibly disconnected from the domain when their permitted login time expires.

(6) Different network access permissions may be assigned to different users, and permitted connection times for Internet access may be configured to facilitate time-based access management.

(7) Users may be permitted to connect at any time, or individual users may be

restricted from connecting on specified days or during specified hours.

(8) Depending on the application system and the applicable information security level, password change frequency and password length requirements may vary.

(9) As a general principle, passwords for network user accounts shall be changed every 30 days, shall not be left blank, and shall meet the required password strength standards.

(10) Passwords for application systems shall be changed periodically on an irregular basis, with password length determined according to the requirements of the relevant application system. The password change frequency shall be every 30 days.

(11) Information system administrators shall regularly inspect the implementation of password management requirements. Any identified issues shall be promptly reported to the head of the Technology Center, together with proposed corrective measures, in order to eliminate potential information security vulnerabilities.

4.3. Internet Use Guidelines

(1) Internet browsing software provided to authorized users may be used solely for corporate business purposes.

(2) All software used to access the Internet must be approved by the Company and kept up to date with security patches provided by the software vendor.

(3) All files downloaded from the Internet must be scanned for viruses using

Company-approved antivirus software.

(4) All software used for Internet access shall be configured to operate through the Company's firewall and proxy server.

(5) All websites accessed must comply with the Company's Information Resource Use Policy.

(6) All user activities involving information assets shall be logged and reviewed.

(7) All content published on or accessed through websites must comply with the Company's Information Resource Use Policy.

(8) Users shall not access offensive or harassing materials through websites.

(9) Private commercial advertisements shall not be published through websites.

(10) The Internet shall not be used for personal gain.

(11) Data shall not be obtained through websites where it cannot be ensured that the data will be used only by authorized persons or organizations.

(12) All sensitive information transmitted over external networks must be encrypted.

(13) Electronic documents shall be retained in accordance with the applicable retention requirements for their respective document types and in accordance with the Company's records retention schedule.

(14) Documents and files sent or received shall be handled in a manner that does not incur legal liability or impede legitimate business activities.Private documents and files stored in information resources shall be clearly named.

(15) All documents and files, including private documents and files, shall comply

with applicable records disclosure requirements.

4.4. Project Development Document Management Policy

(1) Newly hired employees shall register with the administrator to obtain the necessary access permissions and have a personal directory created.

(2) For each newly initiated project, the Project Manager shall contact the administrator to create a new directory and provide a list of project members and an access permission allocation list.

(3) All project documents of the Company and its departments shall be promptly updated and uploaded to the file server. Only working copies may be retained on personal computers.

(4) All program source code shall be stored on the file server. During working hours, source code shall be checked out from the file server, and at lunchtime and after working hours, it shall be checked back into the file server.

(5) Project Manager: The Project Manager shall assume overall responsibility for project documentation and shall be responsible for organizing and maintaining all documents relating to the project, ensuring that documentation required for project management is complete and up to date, and supervising and urging project members to update the project documents for which they are responsible accurately and in a timely manner.

(6) Project Members: Project members shall promptly and accurately update the

project documents for which they are responsible and upload them to the file server. Only working copies may be retained on personal computers.

(7) Upon completion of a project, the Project Manager shall register with the file server administrator and have write access revoked. Read-only access may be granted to relevant personnel as necessary.

4.5. AI Application Management Policy

4.5.1. Management Objectives

The purpose is to regulate the entire lifecycle of AI tool development, deployment, and use, prevent data leakage, intellectual property infringement, and compliance risks, and ensure that AI applications are secure and controllable.

4.5.2. Scope of Application

This Policy applies to all employees, outsourced personnel, and business partners, and covers all workplace applications involving generative AI, decision-making systems, automated tools, and so forth.

4.5.3. Organizational Responsibilities

(1) AI Management Team:Oversee AI lifecycle management, approve the admission of AI tools, handle major risk incidents (the team shall comprise heads responsible for legal affairs, information security, and technology), organize the investigation and handling of major errors, harm, or compliance incidents arising from AI applications, and promote the implementation of corrective measures.

(2) Information Security Department:Conduct data security reviews, manage access permissions, perform log auditing, and track data leakage.

(3) Business Department Heads:Supervise employees' use of AI tools, review AI-generated outputs, and conduct risk self-assessments.

(4) Employees:Use AI tools in compliance with applicable requirements, manually review AI-generated outputs, and assume responsibility for violations.

4.5.4. Tiered Risk Control Mechanism

(1) Application Risk Classification Criteria

Risk Level	Applicable Scenarios	Control Requirements
High Risk	Core business data / financial transactions	Use is restricted to privately deployed environments; use of public-cloud AI services is prohibited
Medium Risk	Code generation / initial drafting of copy / internal reference materials	Only whitelisted tools may be used; customer information, contracts, and other sensitive data must not be entered
Low Risk	Translation of publicly available information / format optimization / basic data organization	Approved and registered tools may be used; all outputs must be subject to human review

(2) AI Tool Admission Rules

1) A whitelist system shall be implemented. All AI tools shall undergo joint review and registration by the Information Security Department and Legal Affairs Department before use.

2) The use of unregistered overseas AI services, free web-based AI tools, and cracked software is prohibited.

3) Any new AI tool shall be submitted for approval using the *AI Tool Approval Form*, and the publicly available list of approved tools shall be updated dynamically.

4.5.5. Data Security Red Lines

(1) Three Strict Prohibitions on Input Data

1) Trade secrets (strategic plans, source code, unpublished financial statements, etc.)

2) Critical business data (customer lists, contract texts, suppliers' floor prices, etc.)

3) Personal privacy information (identity card numbers, facial information, precise location data, etc.)

(2) Data Retention Requirements

1) AI conversation logs shall be retained for at least six months. Caches associated with confidential conversations shall be cleared immediately.

2) Cloud-based automatic synchronization shall be disabled, and the use of enterprise-shared documents shall not be linked to AI tools.

4.5.6. Use Requirements

(1) Algorithmic Fairness and Bias Management

In developing, deploying, and using AI systems, the Company shall identify and mitigate potential bias and discrimination risks arising from data, algorithms, and models. AI systems must not produce unfair or discriminatory outcomes based on factors such as gender, age, race, ethnicity, religion, or disability. For AI applications that may have a significant impact, the Company shall conduct necessary testing, assessment, and bias mitigation measures commensurate with the associated risks.

(2) Transparency and Explainability

For AI applications with a significant impact on business operations, the Company shall ensure an appropriate degree of transparency and traceability throughout their use and retain necessary records of models, data, versions, and usage commensurate with the associated risks. Where AI-generated outputs may affect material business judgments or decisions, the Company shall be able to provide reasonable explanations and ensure that such outputs are subject to human review.

(3) Environmental Impact

When developing, procuring, and using AI technologies, models, computing services, and data center resources, the Company shall pay due attention to and seek to reduce energy and water consumption and carbon emissions, while giving priority to technologies and service solutions that offer higher energy

efficiency and lower environmental impact.

(4) Prohibited Activities

1) The Company prohibits the development, deployment, or use of the following AI applications:

- AI applications that influence individuals' autonomous decision-making through deception, manipulation, or similar means and may cause significant harm.
- AI applications that improperly influence individuals or specific groups by exploiting vulnerabilities associated with factors such as age, disability, or socioeconomic status.
- AI applications that conduct improper social scoring based on individuals' behavior, characteristics, or social attributes.
- AI applications that conduct biometric identification, identity recognition, or surveillance without lawful authorization.

2) Inputting confidential information into public AI services.

3) Using AI to generate false data or falsify work records.

4) Directly using AI to send business documents or responses to customers or other external parties.

5) Submitting AI-generated outputs without human review.

(5) Mandatory Review Process

All AI-generated outputs shall undergo a two-level review:Employee self-review (data accuracy / infringement risks) → final review and sign-off

by the Department Head → approval for use as an official deliverable.

4.5.7. Responsible AI Operations Management

(1) Management of Sensitive AI Capabilities

The Company shall implement authorization and approval procedures and least-privilege access controls for sensitive AI capabilities involving biometric identification, identity recognition, surveillance, and other similar functions. Such capabilities must not be enabled or used without authorization. Necessary access and operation logs shall be retained based on the associated risks.

(2) Labeling of AI-Generated Content

For AI-generated content provided to external parties and AI-assisted decision-making results that may have a significant impact on individuals or business operations, the Company shall, as appropriate to the application scenario, disclose or otherwise indicate the involvement of AI.

(3) Model Monitoring and Fairness Assessment

Based on the risk level of AI applications, the Company shall conduct continuous or periodic monitoring of important or high-risk AI applications, with particular attention to model accuracy, stability, performance changes, and anomalous outputs. Fairness and bias assessments shall be conducted as appropriate to the associated risks. Where model drift, performance degradation, unreasonable bias, or other significant anomalies are identified, the Company shall promptly take measures such as review, adjustment, suspension, rollback, or revalidation, as appropriate.

(4) Environmental Impact Management for AI

Where applicable, the Company shall incorporate energy efficiency and environmental performance into the selection and assessment of AI models, computing services, and third-party data centers. The Company shall reduce the environmental impact of AI applications by optimizing the allocation of computing resources, boosting the efficiency for utilizing resources, and taking other appropriate measures. For AI projects with significant sustainability impacts, appropriate quantitative indicators shall be established based on the application scenario to assess and track energy consumption, resource efficiency, carbon emissions, and other relevant sustainability outcomes.

(5) AI Decision-Making Challenges and Human Review

Where AI-assisted decisions may have a significant impact on users, customers, or other relevant parties, the Company shall provide appropriate channels for feedback, complaints, or challenges and, where applicable, conduct human review of the relevant decision outcomes.

(6) AI Training and Awareness-Raising

Based on job responsibilities and the risks associated with AI applications, the Company shall provide relevant employees with AI usage training and awareness-raising sessions covering AI ethics, data privacy, information security, intellectual property, bias risks, human review, and compliant use requirements.

4.5.8. Intellectual Property and Emergency Response Mechanisms

(1) Ownership of Work Products

Intellectual property rights in work products generated using AI shall belong to the Company. Employees are prohibited from retaining or using such work products for commercial purposes without authorization.

(2) Emergency Response

1) An emergency mechanism shall be established for the immediate suspension of services involving unlawful content.

2) In the event of a security incident such as data leakage, the Company's information security incident response mechanism shall be activated promptly for appropriate handling.

3) High-risk AI applications shall undergo a security audit annually.

4.5.9. Dynamic Management

(1) Changes in Parameters or User Scale: The relevant party shall proactively apply for reassessment and adjustment of the risk classification within 30 days.

(2) Annual Compliance Review: The Regulatory Team shall review the appropriateness of risk classifications and the effectiveness of this Policy on an annual basis.

(3) Disciplinary Measures for Violations: Depending on the severity of the violation, disciplinary measures may include a warning, suspension of access privileges, termination of employment, and legal liability.

(4) Effectiveness of this Policy: This Policy shall be implemented in conjunction with the Company's data security management system and the *Interim*

Measures for the Management of Generative Artificial Intelligence Services (Cyberspace Administration of China, 2026). Matters not covered herein shall be governed by the latest applicable national laws and regulations.