

Information Security Policy

1. Purpose

- (1) CINCON Electronics, Inc. (the “Company”) is committed to safeguarding information assets and personal data, minimizing operational risks and potential losses arising from human error, intentional misconduct, information system failures, cyberattacks, natural disasters, and other potential threats. The Company strives to establish, maintain, and continuously enhance its information and communications security management mechanisms.
- (2) The Company is committed to maintaining the **confidentiality, integrity, and availability** of its information assets. It aims to prevent unauthorized access, use, disclosure, alteration, destruction, or loss of information and personal data. Through risk management, security controls, education and training, incident reporting, and continuous improvement, the Company seeks to enhance the overall effectiveness of its information and communications security management.

2. Scope of Application

- (1) This Policy applies to all employees, contract personnel, outsourced service providers, and other relevant parties who access, use, or manage the Company's information assets for business purposes.
- (2) The Information assets covered by this Policy include information systems, networks and related equipment, software, electronic data, documents, personal data, user accounts, access privileges, and other resources of informational value. This policy also applies to associated information processing activities and business operations.

3. Information and Communications Security Management Objectives

The Company is committed to protecting its information assets, ensuring the confidentiality, integrity, and availability of information, complying with applicable laws, regulations, and contractual requirements, and continuously enhancing its information and communications security management and protection capabilities.

The objectives of this policy are as follows:

- (1) **Ensure Information Security**
Prevent unauthorized access, use, alteration, or disclosure of information and personal data.
- (2) **Maintain Information Services**
Implement appropriate security management, backup, and recovery measures to ensure the stability of information systems and business operations.
- (3) **Ensure Regulatory Compliance**
Comply with applicable laws and regulations related to information and communications security, personal data protection, and relevant contractual requirements.
- (4) **Enhance Security Awareness**
Improve the information security awareness and protection capabilities of employees and relevant personnel through education, training, and awareness programs.
- (5) **Promote Continuous Improvement**
Regularly review and improve information and communications security management measures to strengthen overall protection capabilities.

4. Information and Communications Security Management Measures

- (1) To achieve its information and communications security management objectives, the Company establishes, implements, and continuously improves appropriate security management measures based on the importance of information assets, operational requirements, and associated risks.
- (2) These measures are intended to safeguard the confidentiality, integrity, and availability of information and to ensure the security and stability of information systems and business operations.

5. Information and Communications Security Management and Implementation Mechanism

- (1) The Company establishes an Information and Communications Security Management Team responsible for planning, coordinating, and promoting information and communications security activities.
- (2) The team shall hold meetings at least annually or as necessary to review the implementation and effectiveness of information security management measures, promote security inspections, establish mechanisms for reporting and handling information security incidents, and adjust relevant resources as needed to ensure the effective implementation of information and communications security management.

6. Information and Communications Security Incident Reporting and Response

- (1) Employees and relevant personnel who identify or suspect an information and communications security incident shall report it promptly in accordance with the Company's established procedures.
- (2) The Company shall implement appropriate incident response, recovery, and corrective measures based on the nature and severity of the incident, and shall fulfill applicable incident reporting and handling obligations in accordance with relevant laws, regulations, and other requirements.

7. Information and Communications Security Training and Personnel Responsibilities

All employees and relevant personnel shall receive information and communications security training, comply with applicable security policies and procedures, and fulfill their respective responsibilities in maintaining information security to ensure that the Company's information assets are adequately protected.

8. Continuous Improvement

The Company continuously monitors developments in information security threats, technological advancements, and changes in applicable laws and regulations.

The Company shall periodically review its information and communications security policy, management systems, and security control measures, and make necessary adjustments and improvements based on risk assessments and actual operational requirements.

Through these efforts, the Company aims to enhance the effectiveness of its information and communications security management and strengthen organizational operational resilience.