Eris Technology Corporation

Cyber Security & Management Policies

Chapter 1 General Provisions

Article 1 To ensure the confidentiality, integrity, and availability of important information among the Company's various locations, this policy is formulated in accordance with Article 9 of the "Regulations Governing Establishment of Internal Control Systems by Public Companies", relevant control operations for computerized information systems, and with reference to the information security control guidelines for TWSE/TPEx listed companies.

Article 2 Definitions

1. **Information and Communication System (ICS):** Refers to a system used for collecting, controlling, transmitting, storing, circulating, deleting information, or for other processing, use, or sharing of information.
2. **Information and Communication Service (ICS):** Refers to services related to the collection, control, transmission, storage, circulation, deletion, other processing, use, or sharing of information.
3. **Core Business:** Refers to the essential operations required for the Company's continued operation and development.
4. **Core Information and Communication System:** Refers to the ICS necessary to support the continuous operation of core business.
5. **Sensitive Data:** Refers to important data assessed as requiring confidentiality or being sensitive based on the Company's business considerations, such as trade secret data or personal data.

Chapter 2 Information Security Policy and Promotion Organization

Article 3 Information Security Policy

To maintain the confidentiality, integrity, and availability of the Company's assets, and to protect the privacy and security of user data. This is achieved through the collective efforts of all Company colleagues to meet the following objectives:

1. Protect the information security of the Company's R&D, business, production, and services, ensuring that information can only be accessed by authorized personnel to maintain its confidentiality.
2. Protect the information security of the Company's R&D, business, production, and services, preventing unauthorized modifications to ensure its accuracy and integrity.
3. Ensure that the execution of all the Company's businesses and services complies with relevant legal and regulatory requirements.

Article 4 Information Security Management Framework and Division of Responsibilities

The Company's information security policy and objectives are approved by the General Manager. The highest-ranking executive of the Company's management center serves as the dedicated information security supervisor (designating appropriate personnel as dedicated information security staff to be responsible for promoting, coordinating, supervising, and reviewing information security management matters), and is jointly formed by network management members from the Information Technology Department who are actually implementing information security plans. The main tasks are:

1. Integrate internal information security resources, with the management center serving as the highest-level information security unit, responsible for coordinating and overseeing the operation of information security related policies, measures, and mechanisms.
2. The formulation of information security related measures, technical specifications, and the research and establishment of security technologies will be assisted by the information units at each location.
3. The deliberation of data and report security requirements, usage management, protection, and information confidentiality maintenance among the Company's various locations are handled by the respective business units.
4. Information confidentiality audit and management matters within the Company are handled jointly by the Company's audit unit and relevant business units.

Article 5 Information Security Management Guiding Principles

Information security operating procedures shall be formulated, including core business and its importance, ICS inventory and risk assessment, ICS development and maintenance security, information security protection and control measures, management measures for outsourced ICS or ICS services, information security incident reporting and response and intelligence assessment and response, continuous improvement of information security, and performance management mechanisms. All personnel using information systems shall undergo information security awareness training annually, and supervisors and personnel responsible for information security shall receive information security course training.

Chapter 3 Core Business and its Importance

Article 6 Identify and regularly review the Company's core business and sensitive data that needs protection.

Article 7 Identify applicable laws and contractual requirements that must be complied with.

Article 8 Identify the probability and impact of potential operational disruption incidents, and clearly define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for core business, and establish appropriate backup mechanisms and disaster recovery plans.

Article 9 Formulate a core business continuity plan, and regularly conduct drills for core business continuity. The drill content includes core business backup measures, personnel responsibilities, emergency operating procedures, resource allocation, and review and improvement of drill results.

Chapter 4 Information and Communication System Inventory and Risk Assessment

Article 10 Regularly inventory information and communication systems and establish a core system information asset inventory list to identify their information asset value.

Article 11 Regularly conduct information security risk assessments, identify potential information security risks for core business and core information and communication systems, analyze the impact of loss of confidentiality, integrity, and availability, and implement corresponding information security management or technical control measures.

Chapter 5 Information and Communication System Development and Maintenance Security

Article 12 Incorporate information security requirements into the demand specifications for ICS development and maintenance, including sensitive data access control, user login authentication, and user input/output inspection and filtering.

Article 13 Regularly perform ICS security requirement testing, including sensitive data access control, user login authentication, and user input/output inspection and filtering tests.

Article 14 Properly store and manage ICS development and maintenance related documents.

Article 15 Regularly conduct vulnerability scanning for core ICS and perform system vulnerability patching.

Chapter 6 Information Security Protection and Control Measures

Article 16 Based on network service needs, separate independent logical domains (DMZ, internal, and external networks), and segregate development/testing environments from production environments, and establish appropriate information security protection control measures for different operating environments.

Article 17 Possess the following information security protection control measures:

1. Antivirus software.
2. Network firewall.
3. If there is a mail server, it shall have an email filtering mechanism.
4. Intrusion detection and prevention mechanism.
5. If there are core ICS with external services, they shall have an application firewall.
6. Advanced persistent threat attack defense measures.

Article 18 Establish appropriate protection measures for the processing and storage of sensitive data, such as: physical isolation, dedicated computer operating environment, access rights, data encryption, transmission encryption, data masking, personnel management, and processing regulations.

Article 19 Formulate onboarding, in-service, and offboarding management procedures, and sign confidentiality agreements to clearly inform about confidential matters.

Article 20 Establish operating regulations for user password management, such as: default password, password length, password complexity, password history, minimum and maximum password validity period restrictions, login failure lockout mechanism, and evaluate the adoption of multi-factor authentication technology for core ICS.

Article 21 Regularly review privileged accounts, user accounts, and permissions, and disable accounts that have not been used for a long time.

Article 22 Establish appropriate monitoring measures for ICS and related equipment, such as: authentication failures, resource access failures, important behaviors, important data changes, functional errors, and administrator actions, and establish appropriate protection mechanisms for logs.

Article 23 Establish appropriate management measures for computer rooms and important areas' security control, personnel access control, environmental maintenance (such as temperature and humidity control), and other items.

Article 24 Pay attention to security vulnerability notices, promptly patch high-risk vulnerabilities, and regularly evaluate and perform security vulnerability patching for equipment, system components, database systems, and software.

Article 25 Formulate secure control operating procedures for the recycling, reuse, and disposal of information and communication equipment to ensure the proper deletion of sensitive data.

Article 26 Formulate management regulations for personnel device usage, such as: software installation, email, instant messaging software, personal mobile devices, and portable media.

Article 27 Annually conduct regular email social engineering drills, and provide education and training to personnel who mistakenly open emails or links, and retain relevant records.

Chapter 7 Management Measures for Outsourced Information and Communication Systems or Services

Article 28 When outsourcing, formulate information operations outsourcing security management procedures, including supplier selection, supervision and management (e.g., auditing suppliers and partners), and relevant provisions for termination of outsourcing relationships, to ensure that outsourced vendors have comprehensive information security management measures when performing outsourced operations.

Article 29 When outsourcing, establish information security responsibilities and confidentiality regulations for outsourced vendors, and specify Service Level Agreements (SLA), information security requirements, and the right to audit outsourced vendors for information security in procurement documents.

Article 30 When the outsourcing relationship terminates or is rescinded, the Company shall confirm that the outsourced vendor returns, transfers, deletes, or destroys data held for contract performance.

Chapter 8 Information Security Incident Reporting, Response, and Intelligence Assessment and Response

Article 31 Formulate information security incident response and reporting operating procedures, including determining event impact and damage assessment, internal and external reporting processes, methods for notifying other affected agencies, reporting contacts, and contact information.

Article 32 Join information security intelligence sharing organizations or subscribe to information security intelligence sharing websites to obtain information security early warning intelligence, information security threats, and vulnerability information.

Article 33 In the event of a significant information security incident that meets the specifications of the "Taiwan Stock Exchange Corporation Procedures for Verification and Disclosure of Material Information of Companies with Listed Securities" or the "Taipei Exchange Procedures for Verification and Disclosure of Material Information of Companies with TPEx Listed Securities", relevant regulations shall be followed.

Chapter 9 Continuous Improvement of Information Security and Performance Management Mechanism

Article 34 Information security promotion personnel shall regularly report the implementation status of information security to the management level, ensuring the appropriateness and effectiveness of operations.

Article 35 Regularly conduct internal or outsourced information security audits, formulate improvement measures for discovered issues, and regularly track the improvement status.

Chapter 10 Supplementary Provisions

Article 36 This policy shall take effect after being passed by the Board of Directors, and the same shall apply to any revisions.

This policy was formulated on July 25, 2022.