ESMT 晶豪科技股份有限公司

Elite Semiconductor Microelectronics Technology Inc.

Information Security Policy and Management Plan

1. Information Security Management Framework

The Information Technology Department is responsible for information security and formulating and implementing information security policies. Every three months, the information security implementation plan and implementation status are reported to the management to ensure the continuous and effective operation of the internal security management mechanism.

The Internal Audit Department is the audit unit of the Information Technology Department. If the audit discovers any discrepancies, the department shall require the audit unit to propose relevant improvement plans and regularly track the improvement results to reduce internal security risks.

The organization's operation mode adopts PDCA (Plan-Do-Check-Act) circular management to build a complete security management system to effectively prevent the occurrence of information security incidents, ensure the achievement of information security goals, and continue to optimize and improve.

2. Information Security Policy

This policy is to protect the security of all information assets of Elite Semiconductor Microelectronics Technology Inc., and to prevent internal or external, intentional or accidental threats and destruction that may result in business failure or information tampering, fetching or damage, so as to fulfill our goal of sustainability operation.

i. Definition of Information Security

Protect the Company's information and information systems from unauthorized entry, use, disclosure, destruction, modification, inspection, recording and destruction, and maintain the availability of existing information systems.

ii. Information Security Objective

a. Ensure the confidentiality of business-related information and protect company confidentiality.

b. Ensure the integrity and availability of business-related information.

c. Improve Information Security Protection Capabilities.

iii. Scope of Information Security

This policy applies to various information systems within the Company, internal colleagues, and vendors and third-party personnel who have access to business information or provide services.

3. Information Security Management Solution

The Company has invested in hardware equipment electronic insurance for business assets, such as information systems, network equipment and other information equipment, and avoids equipment being stolen or malicious damage through security monitoring operations. In view of the fact that information security is an emerging type of insurance, considering the comprehensive effect of topics such as insurance coverage, claims coverage, claims identification, and qualifications of identification institutions, the Company will not purchase information security insurance for the time being after evaluation. However, in response to the challenges faced by information security, such as APT advanced persistent attacks, DDos attacks, ransomware, social engineering, and stolen funds and other security issues, the following strategies have been adopted: Keep track of the changes in the information environment in accordance with the Company ’s information security policy, and develop information security protection mechanisms and solutions with reference to technical information. Join ISAC to obtain the latest attack information and take appropriate defensive countermeasures. Conduct regular safety inspections, information security and health consultations, social security and information security drills, strengthen the Company ’s colleagues’ awareness on security crisis and their responsiveness, in order to prevent in advance and effectively identify and prevent proliferation immediately.

The Company has employed corresponding employees responsible for information security according to the Regulations Governing Establishment of Internal Control Systems by Public Companies stipulated by the Financial Supervisory Commission, including dedicated information security managers and personnel. The information security management project above has been integrated to maximize its synergy and to continue increasing investment in information security. ◦

4. Information Security Management Measures, including:

Information Security Management		
Type	Description	Relevant Operation
Access control	Management measures for personnel account, authority management and system operation behavior	● Personnel account permission management and review ● Periodic check of personnel account permissions
Access control	Control measures for personnel to access internal and external systems and data transmission channels	● Internal/external access control measures ● Confidential information leakage control ● Operation behavior track record
External threat	Potential internal weaknesses, poisoning pipelines and protective measures	● Host/computer weakness protection and update measures ● Virus protection and malware detection ● Network threat monitoring
System availability	System availability and measures to deal with service interruption	● System/network availability monitoring and notification mechanism ● Contingency measures for service interruption ● Information backup measures, local/offsite backup mechanism ● Regular disaster recovery drills