ASE TECHNOLOGY HOLDING CO., LTD.

Information Security Policy

2025/7

I. Purpose

ASE Technology Holding Co., Ltd. (hereinafter referred to as the "Company"), in light of increasing digitalization and growing reliance on information systems for its operations, recognizes that the protection of information assets is critical to sustainable corporate development and effective risk management. The Company is committed to safeguarding its information assets from external threats and internal risks, including but not limited to malicious attacks, data loss, system outages, and unauthorized access, through the implementation of a comprehensive information security management system. The Company strives to ensure the confidentiality, integrity, and availability of information assets, thereby maintaining customer trust, corporate reputation, and long-term value.

II. Information Security Governance Requirements

1. The Company has established the "Sustainable Development and Information Security Committee" as its highest governing body for information security. This committee is responsible for formulating and promoting information security policies for the Company and its subsidiaries, as well as regularly identifying and assessing information security risks to ensure that strategies and practices comply with applicable laws and meet the needs and expectations of stakeholders.

2. Senior management is committed to the continuous allocation of resources for information security management, including the upgrading of information infrastructure, adoption of cybersecurity defense technologies, and establishment of incident response capabilities, in order to enhance system resilience and risk response capabilities. The information security management system incorporates mechanisms for continual improvement to ensure that security practices remain up to date and capable of effectively addressing dynamic risks.

3. To ensure the accuracy, consistency, and security of data, the Company continuously strengthens governance and control measures, including access rights management, audit logs, and anomaly reporting mechanisms, ensuring that information remains protected against unauthorized access, tampering, or destruction throughout its entire lifecycle, and that only authorized personnel may access or modify sensitive information.

4. The Company has established incident reporting and response procedures to actively monitor potential cybersecurity risks and abnormal activities, and to take immediate countermeasures when necessary. In the event of a major information security incident, the Company will follow internal procedures for resolution, continuously track corrective actions, reassess associated risks, and, where

applicable, communicate the incident impact and corresponding remedial measures to relevant stakeholders to ensure transparency and foster trust.

5. Information security is a shared responsibility of all employees. Each employee shall assume security obligations commensurate with their role, comply with the Company’s information security policies and guidelines, and proactively report any suspicious activities or incidents. The Company has clearly defined an information security maintenance program applicable to all employees and conducts regular training and awareness programs to enhance security awareness and ensure operational compliance with established standards.

6. The Company has also stipulated information security maturity requirements for suppliers and external partners, incorporating confidentiality agreements, information security clauses, and incident reporting and response obligations into contractual arrangements. Where necessary, the Company shall conduct assessments and audits based on risk levels to ensure the security of the information supply chain.

III. Review and Improvement

The Company’s Information Security Policy shall be periodically reviewed and updated in accordance with regulatory amendments, technological advancements, and emerging information security trends, in order to strengthen the effectiveness and forward-looking nature of the management system and ensure alignment with operational objectives.

IV. Publication and Implementation

This policy shall be published and implemented upon approval by the Chief Information Security Officer (CISO), and the same procedure shall apply for future amendments.