ASE TECHNOLOGY HOLDING CO., LTD.

CYBERSECURITY POLICY

I. Purpose

ASE Technology Holding Co., Ltd. (hereinafter referred to as “ASEH” or “the Company”) creates, processes, and uses proprietary information that is extremely valuable to the Company. To prevent unauthorized access to, tampering with, use of, or disclosure of information relevant to ASEH’s key products and services, and to build trust with its clients, increase its competitive advantage, and ensure the continuity and sustainability of its core operations and businesses, the Company shall ensure the confidentiality, integrity, and availability of crucial proprietary information in accordance with applicable laws and regulations.

II. Requirements and Commitment

A. Cybersecurity governance

1. ASEH cybersecurity management committee established under corporate sustainability committee, oversee the cybersecurity framework of the Company and its subsidiaries in accordance with this Policy. The Company shall conduct periodic internal and external cybersecurity risk audits in order to ensure compliance with the relevant requirements and to meet the expectations of its stakeholders.
2. The Company and its subsidiaries shall organize periodic cybersecurity promotion and training sessions to ensure that employees are made aware of cybersecurity threats and that they comply with applicable laws and regulations.
3. The Company and its subsidiaries shall assign a team of internal IT specialists to monitor potential cybersecurity risks at all times and report any threats identified in accordance with internal protocols.
4. To achieve maximum oversight effectiveness, the Company shall require all subsidiaries to set aside a budget specifically for cybersecurity management.

B. Requirements for suppliers

ASEH suppliers shall abide by this Policy, and they shall sign additional confidentiality or privacy agreements with the Company as necessary.

C. Management commitment

The goal of the Company’s cybersecurity management framework is to ensure business sustainability, prevent or mitigate the impacts of cybersecurity incidents, and minimize losses therefrom.

III. Implementation and Review

This Policy shall be reviewed on a regular basis and updated to comply with applicable regulations as well as the latest developments in cybersecurity.