



ASUS Group Information Security Policy

Purpose:

To ensure compliance with information security regulatory requirements, international information security standards, and industry best practices. It is also designed to protect company assets from external threats and internal misuse or mismanagement, safeguard customer data, enhance product security, strengthen market competitiveness, and foster innovation. Ultimately, it aims to reduce product design and maintenance costs and establish a strong foundation for sustainable development and long-term market advantage.

Coverage:

ASUS Group's employees, suppliers, contractors, and partners.

Commitment:

1. Ensure the confidentiality, integrity, and availability of all information assets.
2. Evaluate and adopt cutting-edge technologies to strengthen our defense-in-depth security architecture.
3. Ensure security requirements are addressed throughout product design, development, and deployment.
4. Regularly reassess the effectiveness of both detective and preventive measures to enhance the organization's overall cyber resilience.

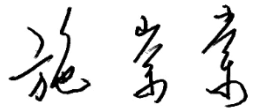
Management Principles:

1. Risk management: Establish an information asset risk assessment mechanism to determine acceptable risk levels and ensure that information assets are adequately protected to prevent damage from unauthorized access or operational negligence.
2. Monitoring and responding to information security threat: Monitor and identify sources of cyber threats and respond accordingly, participate in international cyber defense to strengthen information sharing and enhance ASUS's overall cybersecurity resilience.
3. Information security incident management: Ensure that all information security incidents or suspected security vulnerabilities are reported, investigated, and handled according to the appropriate procedures.
4. Business continuity management: Establish operational continuity management control principles to ensure that systems and business processes continue to operate without disruption, meet high availability requirements, and can recover quickly to an



acceptable operational level.

5. Supply chain security management: Ensure that suppliers comply with the ASUS's information security policy and enter into the necessary confidentiality or information security agreements.
6. Product security: Ensure strong security practices at every stage of product development, promote security-first culture, and deliver products that are both reliable and secure.
7. Training: Conduct information security awareness programs to cultivate culture of cybersecurity.

Chairman: 

Date: 2025/06/25