AUO Information Security Policy and Governance Framework

AUO Information Security Policy

"Protect the company's intellectual property, comprehensively raise awareness of information security, and jointly create an opportunity to win (profit)" is the core principle of AUO's information security. The Company places great importance on information security and regards it as a fundamental pillar for sustainable business development. With the objective of safeguarding critical information assets of customers, the Company, and all stakeholders, AUO continuously strengthens its overall information security governance and protection capabilities.

AUO Information Security Commitment

The Company is committed to continuously advancing its information security governance and strives to:

- Continuously enhance the Information Security Management System (ISMS) to strengthen the overall protection of information assets
- Ensure the confidentiality, integrity, and availability of information assets, including but not limited to customer data, personal data, and the company's proprietary information
- Continuously monitor and effectively respond to information security threats and incidents to minimize impacts on operations and stakeholders
- Uphold every employee's responsibility and accountability for information security, reinforcing security awareness and adherence in daily operations
- Strengthen information security requirements for suppliers and business partners to jointly safeguard the security of the information ecosystem

Information Security Governance Structure

The Company's Board-level Sustainability and Risk Management Committee oversees information security risks and integrates them into the enterprise risk management framework through dedicated governance mechanisms. An Information Security Committee is also established to review policies and strategies. The Chief Information Security Officer (CISO) leads dedicated teams and cross-functional collaboration to drive information security initiatives, ensuring effective top-down governance implementation.

Standards Compliance and Certification

The Company has established its Information Security Management System (ISMS) in reference to international standards (including, but not limited to, ISO/IEC 27001).

Through systematic, documented, and structured management practices, AUO continuously enhances its information security capabilities and operational resilience. Information security strategies and action plans are developed to align with overall business objectives, and relevant certifications (including but not limited to ISO/IEC 27001) have been obtained.

Regulatory Compliance and Privacy Protection

The Company complies with applicable information security and personal data protection regulations (including, but not limited to, GDPR). A privacy policy is established to specify the processes for collection, processing, and use of personal data, as well as mechanisms to safeguard data subject rights.

Risk Management and Protection Mechanisms

The Company implements a systematic risk assessment process to regularly identify and analyze information security risks, incorporating them into the enterprise risk management framework to ensure appropriate protection of critical assets. Multi-layered defense strategies are deployed, including system protection, vulnerability management, and incident detection and response mechanisms, to continuously enhance security defense and response efficiency.

Access Control and Data Protection

To ensure data security, the Company manages access rights in accordance with the principle of Least Privilege. Multiple administrative and technical controls (including, but not limited to, multi-factor authentication and encryption for data in transit and at rest) are implemented to ensure data is properly protected throughout its lifecycle.

Information Security Incident Management and Notification

The Company has established incident response procedures covering detection, reporting, analysis, containment, and recovery to minimize impact. In the event of significant security incidents, relevant stakeholders and regulatory authorities will be notified within the required timeframe in accordance with applicable regulations and contractual obligations.

Operational Resilience and Business Continuity

The Company has established a Business Continuity Plan (BCP) and disaster recovery mechanisms. Through redundancy design, data backup, recovery procedures, and regular drills, critical systems and operations can be restored within acceptable timeframes during disruptions.

Information Security Culture and Employee Responsibility

The Company promotes a company-wide information security culture through training, awareness programs, and policies to enhance employee understanding and compliance. Shared responsibility and accountability are embedded as core management principles.

Supply Chain and Ecosystem Security

The Company extends information security management to its supply chain and partners by requiring compliance with applicable security standards. Through assessments, contractual requirements, and ongoing management processes, AUO works collaboratively to enhance overall security posture and establish a trusted ecosystem.

Secure System Development and Technology Security

Information security requirements are integrated into the system development lifecycle (SDLC), including secure design, code review, vulnerability scanning, and penetration testing. System change management and vulnerability remediation processes are implemented to reduce system risks.

Performance, Continuous Improvement, and Audit

The Company defines key performance indicators (KPIs) for information security (e.g., vulnerability remediation rate, incident response time, training completion rate) and regularly monitors and reviews them to ensure effective implementation and continuous improvement. Internal and external audits are conducted periodically to assess the effectiveness of the information security management system, and management reviews are performed to continuously strengthen governance and controls.

Continuous Collaboration and Industry Engagement

The Company actively participates in industry collaboration and talent development in information security. Through cross-organizational cooperation and professional engagement, AUO contributes to enhancing the overall cyber resilience of society.

Chief Digital Officer 

Version 1, July 2026