SMK Information Security Policy

SMK Corporation and its domestic and overseas subsidiaries (hereafter the "SMK Group") recognize that the proper handling and protection of all information and information systems (hereafter "information assets") constitute an important social responsibility in the conduct of the SMK Group's business activities. Accordingly, the SMK Group hereby establishes the SMK Information Security Policy set forth below and is committed to ensuring and enhancing information security.

1. Management Responsibility
   The SMK Group establishes a structure with the CIO serving as the Chief Information Security Officer (CISO) and builds and continually improves the information security management system under the CISO's direction.

2. Protection and Management of Information Assets
   The SMK Group ensures the confidentiality, integrity, and availability of information assets held for business activities and implements physical, technical, and human security measures. Furthermore, the Group appropriately classifies information assets and manages them based on risk assessments.

3. Implementation of Information Security Education and Training
   To ensure thorough understanding of the SMK Information Security Policy, the SMK Group regularly provides education and training to all employees who handle the Group's information assets. Such education and training cover the importance of information security, the proper handling and management of information assets, and emergency response procedures.

4. Information Security Monitoring and Auditing
   To identify information security threats, the SMK Group continuously monitors its information systems and networks, detects anomalies, and takes necessary actions. Furthermore, to maintain and improve information security, the SMK Group conducts internal audits as appropriate and third-party audits as necessary and endeavors to promptly address any audit findings.

5. Response to Information Security Incidents
   The SMK Group establishes emergency response systems and procedures in preparation for information security incidents, disasters, and similar emergencies. When an information security incident occurs, the SMK Group promptly reports it to relevant parties, minimizes damage, and endeavors to prevent its recurrence.

6. Requirements for Suppliers
   The SMK Group endeavors to understand information security measures across the entire supply chain and requires suppliers to implement appropriate information security measures.

7. Compliance with Laws and Regulations
   The SMK Group complies with the laws, regulations, and contractual obligations relating to information security in each country, and endeavors to adhere to other social norms and guidelines.

The SMK Information Security Policy is reviewed periodically in response to changes in the social and business environments, with a view to continual improvement.

SMK Corporation
June 12, 2026

Executive Vice President (CIO)
Hiroshi Usami