HS HYOSUNG ADVANCED MATERIALS

HS Hyosung Advanced Materials Corp.

Information Security Policy

Security Responsibility Enhancement TFT

March 03, 2026

Table of Contents

01. GENERAL PROVISIONS

01) Purpose

This policy aims to prevent the leakage of critical information—including company confidential data, intellectual property, and customer personal information—of HS Hyosung Advanced Materials Corporation (hereinafter referred to as "the Company"), to minimize the risk of asset loss due to information security incidents, and to support safe and sound business operations.

02) Scope of Application

This policy applies to all employees of the Company, all external parties including employees of partner companies, and all individuals who use the Company's information and communications networks and facilities. It applies to all information assets owned, managed, or obtained by the Company in the course of business, including information provided by third parties.

02. INFORMATION SECURITY MANAGEMENT SYSTEM

01) Information Security Governance

① The Company shall continuously assess and improve its information security management system, monitor changes in domestic and international information security laws and regulatory requirements, and reflect them in its security regulations.

② The Company shall appoint a Chief Information Security Officer (CISO) to oversee all Company-wide information security activities.

③ The CISO is responsible for overseeing company-wide information security activities and monitoring potential data breach incidents. In collaboration with relevant departments, the CISO leads the Security Responsibility Enhancement TFT, which regularly reviews the effectiveness and implementation status of current security policies.

④ To further strengthen enterprise-wide security accountability, all department heads shall be designated as departmental security officers, helping to minimize the risk of asset loss due to information leaks.

02) Employee Security Responsibilities

① All employees must understand and comply with the Company's information security policy in good faith.

② Information obtained in the course of business—whether owned by the Company or by third parties—must be used only for business purposes. It must not be disclosed or leaked without authorization to any person not authorized under the Company's information security policy, whether employees or external parties.

③ All information security-related business must be carried out in accordance with relevant security regulations, guidelines, and procedures. Any matters not specified therein must be handled in accordance with applicable laws and internal regulations.

03. INFORMATION SECURITY IN EXTERNAL COLLABORATION

01) Contracts and Agreements

① When the Company engages in collaboration with external parties, a security agreement and confidentiality pledge must be obtained in advance from the relevant third parties.

② When entering into a contract for collaboration with an external party, the department in charge must review and establish the necessary information security requirements for third parties and specify the obligations that the external party must comply with in the contract.

③ When carrying out contracted tasks, the number of external personnel with access to or handling authority over the Company's security documents must be limited to the minimum necessary.

02) Information Security Management in External Collaboration

External personnel may access only the areas of the Company premises authorized for their activities. If bringing IT equipment is required for collaboration, they must comply with the Company's equipment entry and exit procedures.

04. PREVENTION AND RESPONSE TO INFORMATION SECURITY INCIDENTS

01) Prevention of Information Security Incidents

① The Company shall maintain a collaborative system with external expert organizations capable of providing immediate support and an up-to-date emergency contact network to ensure a swift and effective response to security incidents.

② Regular information security risk assessments shall be conducted to ensure the systematic management of information asset leakage risks.

③ Risks shall be managed through the identification and classification of information assets, evaluation of risk levels, and the development of appropriate response strategies. The effectiveness of the risk management system shall be continuously strengthened through periodic reassessments and simulation-based training exercises.

④ Regular simulation-based training shall be conducted to strengthen employee awareness of information security and enhance the Company's capability to respond to cyber threats.

02) Identification and Reporting of Information Security Incidents

① All employees must report any unauthorized activities or suspicious signs they become aware of to the internal reporting unit, the site-level security manager, or the departmental security officer.

② When a security officer detects unauthorized activities or suspicious signs in the system, the officer must verify and assess the situation and, if confirmed as a security incident, report it to the CISO.

③ Incident response and analysis, root cause investigation, and incident investigation must be carried out and reported to the CISO.

03) Recovery Procedures and Follow-up Actions

① A system administrator must back up critical files, update account credentials related to the affected systems, and verify whether the backup images have been compromised or tampered with during system recovery.

② It must be confirmed that the vulnerabilities which caused the incident have been eliminated from the recovered system, and support must be provided to ensure the latest security patches are applied.

③ The security officer must prepare a report containing details of the damage, root cause, and recurrence prevention measures, and submit it to the CISO.

④ Measures must be established to address vulnerabilities and prevent future risks as part of follow-up actions.

05. INTEGRITY AND PROTECTION OF DATA

01) Information Asset Security Management

① "Information assets" refer to all tangible and intangible information held or generated by the Company, including outputs and electronic documents.

② Information asset management process:

- Creation: Information assets shall be classified and managed based on their security level and designated retention period.
- Storage: Electronic information assets shall be registered in the central system; physical information assets shall be managed in accordance with their designated security levels.
- Export: The export of information assets without prior approval is strictly prohibited. All transmission records for approved transfers shall be retained to support potential leak investigations.

02) Data Protection Measures

① Security solutions shall be implemented and operated to prevent the leakage of information assets and to ensure swift response to security breaches.

② The Company shall restrict direct user access to data to ensure data integrity.

③ Any modification of data through methods other than proper authentication is strictly prohibited. If modification is necessary, it may only be performed by authorized personnel with the approval of the relevant system administrator.

④ Sharing between databases or sharing of data files is, in principle, prohibited. In cases where it is necessary, appropriate security measures such as a security review must be applied.

03) Information Security System Log Management

① The Company shall implement administrative and technical controls to protect information security system logs from unauthorized modification.

② Critical logs must be backed up to a separate location and securely managed.