Document Control Number	2025-S-12
First Enacted	June 18, 2025
Last Revised	June 18, 2025
Chief Information Security Officer (CISO)	Minjung Seo, Vice President, Information Security Group 1
Document Administrator	Hyundai Information Security Team

Hyundai Motor Company
Information Security Policy

June 2025

Table of Contents

1. General Provisions

a. Purpose

This policy aims to define a system necessary for protecting Hyundai Motor Company's (hereinafter referred to as "the Company") tangible and intangible trade secrets and business operations, to carry out such protection activities on an ongoing basis, and ultimately to prevent information security breaches and contribute to the Company's growth.

b. Scope of Application

This policy applies to all employees of the Company, external parties, all individuals entering the Company premises, and all information assets owned and operated by the Company.

2. Information Security Compliance Obligations

a. Responsibilities for Compliance with Information Security Policy

① The Company holds the responsibility to make continuous efforts to assess and improve its information security management system. 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 not be used for purposes other than business. It must not be disclosed or leaked, without authorization, to anyone other than those authorized under the Company's information security policy, including employees and external parties.

③ Employees and external parties must use the Company's information assets securely. In the event they become aware of an information security incident, they must immediately report it to the Company-wide information security department.

④ 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.

3. Information Security in External Collaboration

a. 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 necessary scope.

b. Information Security Management in External Collaboration

① 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.

② External personnel must comply with the Company's information security policy and attend the relevant information security training sessions.

c. Coordinating Department for Collaboration

① The department responsible for the collaboration must regularly provide training on information security compliance requirements and monitor participation to ensure completion.

4. Prevention and Response to Information Security Incidents

a. 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 All employees must not, at their own discretion and without prior approval from the Chief Information Security Officer (CISO), disclose any information related to information security incidents to personnel not involved in the investigation or to external parties, including the media.

③ If an information security officer detects unauthorized activities or suspicious signs in the system, they must verify and assess the situation, and if it is determined to be an information security incident, report to the CISO.

④ Incident response and analysis, root cause investigation, and incident investigation must be carried out and reported to the CISO.

b. 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.

c. Prevention of Information Security Incidents

① A monitoring, detection, and response system must be established and operated for identifying suspicious signs, thereby preventing information security incidents. In addition, regular incident response drills must be conducted.

② In preparation for potential security breaches, incident response drills must be planned and conducted at least once a year to ensure prompt response.

5. Integrity and Protection of Data

a. Database Security

① The Company must control direct user access to databases to ensure the integrity of data.

② Any modification of database 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 database administrator.

③ 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.

b. Information Security System Log Management

① The Company must implement administrative and technical controls to protect information security system logs from falsification or alteration.

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

This policy shall take effect from June 18, 2025.