Document Number	H12300019271-20260602-010830
Initial Enactment Date	June 2026
Department in Charge	Information Security Operation Team

Hyundai Steel
Information Security Policy

	Version	Record on Enactment and Revision	Contents of enactment /revision
Enactment & Revision History	0	June 2026	Initial Enactment

[Team in Charge]	[Division in Charge]
Information Security Operation Team	Head of Business Management Division, Managing Director (CHO)

〈Table of Contents〉

1. General Provisions

① Purpose

The purpose of this Policy is to establish the necessary framework for protecting the tangible and intangible assets, trade secrets, and business operations of HYUNDAI STEEL Co., Ltd. (hereinafter referred to as the "Company"), to prevent security incidents through continuous protection activities, and to contribute to the stable growth of the Company.

② Scope of Application

This Policy applies to all officers and employees of the Company, on-site contractors, and any third parties who access the Company's premises or handle its information assets. Furthermore, it shall apply to all documents, facilities, information systems, and information processing equipment owned or managed by the Company.

③ Continuous Improvement

The Company shall periodically review and continuously enhance its information security management system (ISMS) to effectively respond to changes in the security environment and emerging threats.

2. Information Security Organization and Responsibilities

① Security Organization

1. To systematically implement information security management activities, the Company shall operate a dedicated security organization consisting of the Chief Information Security Officer (CISO), the Corporate Information Security Governance Department, Departmental Security Officers/Managers, and the Corporate Security Committee.

2. The Corporate Information Security Governance Department shall operate a security monitoring system capable of real-time threat detection and immediate response upon identifying any anomalies.

② Information Security Responsibilities and Obligations

1. Officers and employees shall not use the information of the Company or any third party for purposes other than authorized business operations, nor shall they disclose or leak such information externally without prior approval. They must fulfill their responsibilities and roles specified in the Company's security regulations. Furthermore, upon identifying any security violations or vulnerabilities that may cause harm to the Company, they are obligated to immediately report them to the Corporate Information Security Governance Department.

2. External vendors and suppliers are obligated to comply with the information security requirements defined by the Company within the scope of their contract or partnership. The Company may audit vendor compliance with these requirements and take appropriate contractual measures in the event of a violation.

3. Information Asset Management and Protection Principles

① Identification and Classification of Information Assets

The Company shall identify and classify all information assets in its possession, applying appropriate protective measures based on their level of importance. Officers and employees must handle these assets in accordance with their assigned classification levels and strictly adhere to the corresponding protective measures.

② Handling and Protection Standards

Information assets must be handled in accordance with established protection standards based on their classification level, asset type, and intended business purpose. Officers and employees must comply with these standards to prevent unauthorized access, data leakage, and unauthorized modification, thereby ensuring data integrity.

③ Usage and Removal Control

1. Information assets must be used exclusively within the scope required for business execution; any unauthorized access or utilization is strictly prohibited.

2. When removing information assets outside the Company, predefined approval procedures must be followed, and appropriate protective measures must be applied based on the asset's level of importance.

4. Privacy Policy

① Privacy Management System

1. To protect the personal information of officers, employees, and customers, the Company shall operate a comprehensive privacy management system and conduct systematic data protection activities through internal regulations and the designation of responsible privacy officers.

2. In alignment with the personal information lifecycle, the Company shall implement administrative measures—such as consent management, privacy policy establishment, and secure destruction—alongside technical safeguards, including encryption, access control, and malware prevention.

② Principles of Personal Information Protection

1. The Company shall clarify the purpose of processing personal information and shall collect and use only the minimum personal information necessary for such purposes in a lawful and fair manner.

2. The Company shall maintain the accuracy and currency of personal information, and apply appropriate administrative, technical, and physical protection measures to prevent unauthorized alteration or damage during processing.

3. Where applicable, personal information shall be anonymized or pseudonymized to mitigate security risks. Throughout all processing stages, the Company shall comply with its obligations under relevant laws and regulations to maintain the trust of data subjects.

5. Security Incident Response and Management

① Prevention of Security Incidents

1. The Company shall conduct security reviews when introducing or modifying systems, and proactively eliminate potential risks through regular vulnerability assessments and timely security patches.

2. The Company shall continuously minimize security vulnerabilities through inactive/unnecessary account management, preparedness against advanced

hacking techniques, and ongoing technical and administrative measures.

② Security Incident Response and Handling

1. Upon the occurrence of a security incident, priority shall be given to immediate containment, data backup, collection of intrusion traces, and service protection measures. If necessary, immediate response measures, such as network isolation, shall be executed.

2. During the incident handling process, the Company shall precisely determine the status of the intrusion and the scope of damage through log analysis, identification of malware/backdoors, and account integrity verification.

3. Following the elimination of the root cause and the completion of recovery measures, a comprehensive vulnerability check must be conducted; services shall be resumed only after safety and security are fully verified.

③ Post-Incident Follow-up Measures

1. The Company shall eliminate the root causes of temporarily resolved issues, establish measures to prevent recurrence, and, if necessary, issue internal announcements and conduct security training for officers and employees.

2. Incident records and forensic evidence shall be preserved and securely managed for potential legal response. In the event of a violation by internal personnel, disciplinary actions shall be enforced in accordance with company regulations.