Last Edited	2025.07
Managed by	Information Security Sector

HEC Information Security Policy

Tabel of Contents

1. Overview

A. Purpose of Establishment

The purpose of this policy is to securely protect all tangible and intangible assets of Hyundai Engineering Co., Ltd. (hereinafter referred to as the "Company" or "we") from internal and external threats, thereby maintaining and enhancing the Company's competitiveness. Furthermore, this policy aims to create a sound and secure environment for the use of information assets, contributing to the Company's development and enhancing external trust.

B. Scope of Application

This policy shall apply to all employees of the Company, third parties under contractual relationships such as business partners, and visitors. The scope also extends to all information assets, including any media, IT equipment, and related facilities in which the Company's information is recorded, stored, or utilized. All individuals in contractual relationships with the Company, including employees, are required to comply with this policy and the guidelines established thereunder in good faith and with integrity.

C. General Provisions

1. The Company endeavors to prevent the leakage and destruction of critical assets such as trade secrets, ensure reliable business continuity through the stable operation of information systems, and minimize business losses resulting from security incidents. In response to the rapidly changing cyber environment, the Company regularly reviews its information security management system and continuously improves it by incorporating the latest technologies and response strategies.
2. To implement the established information security policies, the Company pursues the following objectives:
   (1) Protect information assets within the organization from various threats
   (2) Establish operational measures including personnel, facilities, and systems to perform information security tasks
   (3) Operate access control measures to ensure only authorized individuals can access information assets
   (4) Implement administrative, physical, and technical security measures for the protection of information assets
   (5) Provide information security training, including asset management practices

(6) Establish and operate incident response plans for security breaches and disasters
(7) Ensure business continuity and maintain continuous service and operational availability
(8) Comply with relevant laws and regulations and maintain legal and regulatory conformity
(9) Address other matters as separately stipulated by the Company

2. Security Roles and Organizational Structure

A. Responsibilities

This section outlines the primary responsibilities related to information security, focusing on overall security management and specifying the duties of employees.

1. The Company's Chief Security Representative shall be the Chief Executive Officer (CEO), who holds ultimate authority and responsibility for the Company's overall security operations. The Chief Security Representative may delegate security responsibilities for each division to designated Division/Center/Department Security Officers and delegate overall management of security governance activities to the Chief Information Security Officer (CISO).
2. The Chief Information Security Officer (CISO) serves as the Head of Security and is responsible for all policies related to security. The CISO is tasked with establishing, implementing, and improving the company-wide information security plan; auditing the current state of security; issuing and managing improvement directives; identifying and assessing information security risks; developing countermeasures; and planning and conducting security education and simulation training.
3. The Chief Privacy Officer (CPO) is responsible for planning, implementing, managing, and supervising the Company's personal data protection activities.
4. All employees of the Company are required to be familiar with and comply with the Company's security standards (including policies and guidelines). They must actively participate in security-related activities such as security training and internal audits. Upon recognizing any potential security incident or violation of security standards, employees must promptly report the matter to the relevant team/site security officer or the Company-wide security personnel.

B. Fostering an Information Security Culture and Organizational Management

1. The Company-wide Security Officer shall establish an annual information security training plan and obtain review and approval from the Chief Information Security Officer (CISO).
2. Based on the approved annual training plan, the Company-wide Security Officer shall

conduct regular security training at least once a year. Additional training may be provided in the event of significant changes to relevant laws or internal regulations.

3. The Company-wide Security Officer may provide employees and external personnel with educational materials that include the Company's security compliance requirements and case studies of damage caused by security violations.
4. To strengthen expertise in information security, the Company-wide Security Officer shall periodically complete internal and external professional training programs.
5. All employees are required to complete security training at least once a year.
6. After conducting security training, the Company-wide Security Officer shall assess the effectiveness of the training (e.g., through surveys, tests, etc.) and reflect identified improvements in the subsequent annual training plan.
7. Team/Site Security Officers may provide additional security training to their team members when necessary, such as in response to internal or external security incidents.
8. In cases where updates to internal regulations or important notices need to be communicated, Team/Site Security Officers shall conduct internal briefings or training sessions within their teams.

3. Security Threats and Incident Response

A. Risk Identification

1. The Company-wide Security Officer shall conduct issue-based risk analysis at least once per year, based on relevant issues and contextual factors, and report the results to the Chief Information Security Officer (CISO).

2. The Company's risk management procedures are aligned with the risk management frameworks outlined in ISO 31000 and ISO 27005.

3. Risk management methods are established at a practically achievable level to meet security objectives.

4. The Chief Information Security Officer may initiate an ad-hoc risk analysis at any time if a significant change occurs in the Company's security environment or if it is deemed necessary, regardless of the regular schedule.

B. Incident Response and Reporting Procedures

1. The Company shall establish and operate a response system to effectively manage security incidents, and shall develop response guidelines that include specific actions to be taken by employees in the event of unauthorized leakage or breach attempts.
2. All employees must report any signs of a potential security incident to the Company-wide Security Officer as soon as possible.
3. If evidence of external intrusion is suspected, the Company-wide Security Officer must conduct an inspection using security diagnostic tools or checklists. If data tampering or unauthorized access is detected, the relevant service must be immediately suspended.
4. In the event of a system failure caused by a security breach, the affected information system must be promptly restored. Mock recovery drills shall be conducted at least once a year on a regular basis.
5. Any security incident that is authorized for public disclosure must be communicated to or used as training material for employees.
6. In the event of a security incident, the Company shall respond promptly in accordance with established procedures to minimize damage.

4. Appendix

This policy document has been prepared as a public disclosure to transparently communicate Hyundai Engineering's information security regulations to external stakeholders and to share the company's principles of sustainable and responsible management.