Hyundai Polytech	Information Security Regulation	Document Number	HP-ESG-S-P6-00-E
		Revision No.	0

Revision History	No.	Date of Establishment/ Revision	Enforcement Date	Description
	0	2026.01.02	2026.01.02	Initial Establishment

Hyundai Polytech
Information Security Policy

Approval	Prepared by	Reviewed by	Approved by	Authorized by	CEO

Contents

Chapter 1. General Provisions

Article 1 (Purpose)

Article 2 (Scope of Application and Coverage)

Chapter 2. Basic Principles of Information Security

Article 3 (Basic Principles of Information Security)

Article 4 (Compliance with Laws and Regulations)

Chapter 3. Information Assets and Data Protection

Article 5 (Information Asset Management and Access Control)

Article 6 (Protection of Confidential Information and Third-Party Data)

Article 7 (Personal Data Protection)

Chapter 4. Information Security Incident Response

Article 8 (Information Security Incident Response)

Article 9 (Incident Prevention and Recurrence Prevention)

Chapter 5. Internal Management and Awareness Enhancement

Article 10 (Internal Reporting Procedures)

Article 11 (Employee Awareness Enhancement and Training)

Chapter 6. Supplementary Provisions

Article 12 (Effective Date and Amendments)

Chapter 1. General Provisions

Article 1 (Purpose)

This Information Security Policy aims to protect the information assets of Hyundai Polytech Co., Ltd. (hereinafter referred to as the “Company”), as well as the information of customers, suppliers, and third parties, and to prevent and respond to information security breaches and incidents, thereby ensuring the Company’s reliability and supporting stable business operations.

Article 2 (Scope of Application and Coverage)

① This Policy applies to all executives and employees of the Company, as well as all stakeholders who access or handle the Company’s information.

② This Policy applies to all types of information assets and data processing activities that are owned, managed, or processed by the Company.

Chapter 2. Basic Principles of Information Security

Article 3 (Basic Principles of Information Security)

The Company recognizes information security as an important management element in its business operations and protects information assets and data in accordance with the following basic principles.

① The Company complies with laws and regulations related to information security.

② The Company protects the confidentiality, integrity, and availability of information.

③ The Company recognizes information security risks and establishes reasonable protective measures to respond to such risks.

Article 4 (Compliance with Laws and Regulations)

The Company complies with domestic and international laws and regulations related to

information security and personal data protection and faithfully fulfills its legal obligations.

Chapter 3. Information Assets and Data Protection

Article 5 (Information Asset Management and Access Control)

The Company identifies and appropriately manages information assets required for business operations and applies access control standards to prevent unauthorized access, use, leakage, alteration, or damage.

Article 6 (Protection of Confidential Information and Third-Party Data)

① The Company complies with internal standards when handling, sharing, and storing confidential information and data of customers, suppliers, and other third parties in order to protect such information.

② The Company restricts the use of information beyond business purposes and takes measures to prevent unauthorized provision to third parties.

Article 7 (Personal Data Protection)

The Company complies with laws and regulations related to personal data protection and processes personal data in a minimal manner appropriate to its purpose when collecting, using, and storing such data, and manages it securely.

Chapter 4. Information Security Incident Response

Article 8 (Information Security Incident Response)

① In the event of an information security breach or incident, the Company shall identify the incident and respond promptly and appropriately in accordance with internal procedures.

② The Company shall identify the causes and impacts of information security incidents and take necessary measures to minimize their impact on business continuity.

Article 9 (Incident Prevention and Recurrence Prevention)

To prevent the recurrence of information security incidents, the Company reviews corrective measures related to the causes of incidents and, where necessary, supplements relevant standards and procedures.

Chapter 5. Internal Management and Awareness Enhancement

Article 10 (Internal Reporting Procedures)

① Executives and employees may report violations or potential risks related to information security in accordance with the Company's internal procedures.

② The Company shall take necessary measures to ensure that information security-related reports are handled appropriately.

Article 11 (Employee Awareness Enhancement and Training)

The Company may conduct necessary training or provide guidance to enhance executives' and employees' awareness of the importance of information security.

Chapter 6. Supplementary Provisions

Article 12 (Effective Date and Amendments)

This Information Security Policy shall take effect as of the date of enactment and may be amended in accordance with changes in relevant laws and regulations or the Company's operational environment.