Hyundai MOBIS

Information Security Regulation

2025.11.

Number	Date	Effective date	Major Revisions
1	2025.11.06	2025.11.06	enactment

Contents

Article 1. General Provisions

① Purpose

The purpose of this Policy is to prescribe matters concerning the business and operations of information security of Hyundai Mobis CO.,Ltd (hereinafter referred to as the "Company") and to protect the company's information assets and support safe management activities through information security activities.

② Scope

This Policy shall apply to all persons related to the information of the Company, such as all employees, contractual persons, visitors, etc. working for the Company, and shall apply to all affairs related to tangible and intangible information assets held and operated by the Company.

Article 2. Security Policy Operation

① Structure of the Information Security Organization

1. To systematically implement information security management activities, the organization is composed of the company-wide Chief Information Security Officer(CISO), the information security department, departmental information security officers/staff, and the company-wide Information Security Committee.

② Information Security Policy Management

1. The basic principles of Information Security Regulations are defined, and policies are applied in accordance with these principles.
2. Tasks are carried out in compliance with legal requirements, security-related regulations, guidelines, and procedures.
3. The information security department announces any changes-such as amendments to laws or client policy updates-through the bulletin board, along with internal

Article 3. Protection of information assets

① Information Security Education

1. The information security department of the enterprise establishes and implements the information security education and training plan required for employees and external personnel.
2. The information security department of the enterprise shall maintain the security level and prevent accidents through regular activities to raise security awareness.
3. Other information Security education shall be conducted according to the level of each subject.

② Information asset management

1. Employees and outsiders shall safely use and manage our information assets.
2. The Company shall establish and operate physical security policies and management procedures to maintain a safe working environment for all workplaces and to protect information assets in the workplace.
3. The Company classifies information assets according to defined criteria and applies management policies tailored to their characteristics.

③ Information System Security Management

1. The Company information assets, the Company shall establish and operate a security management system for all types of information systems.
2. The network shall be operated separately according to the necessity and importance of access, and shall not be used without permission.
3. The introduction and modification of the information system shall comply with appropriate standards (access rights, user accounts, password management, network separation, etc.) and procedures.
4. Prepare a recovery plan for system failure and prepare and operate continuous inspection and vulnerability preparation procedures to prevent hacking incidents from occurring/spreading.

Article 4. Privacy

① Composition of Privacy Protection Organization

1. The Company shall organize and operate a personal information protection organization for the safe processing of personal information, including the Personal Information Officer (CPO) and the Personal Information Protection Department.
2. The Privacy Organization shall perform the duties of protecting personal information and other matters deemed necessary by the Company to ensure the safety of personal information.

② Privacy Principles

1. The Company shall disclose the processing of personal information in a transparent manner and disclose what purpose it is used for and how it is managed through the 'Privacy Policy'.
2. The Company shall collect personal information required for business purposes at a minimum and manage the personal information held with responsibility.
3. Recognizing the importance of personal information, the Company conducts education on personal information protection so that employees can utilize and protect personal information in accordance with relevant policies and regulations.

Article 5. Information Security Incident Response and Prevention

① Recognizing and responding to accidents

1. In order to maintain a rapid security reporting system, the general affairs department of enterprise information protection shall operate a "security reporting and reporting center"
2. In case of an IT infringement incident, respond according to the company's plan to respond to the infringement incident.

② Recovery procedure and follow-up measures

1. The information security department of the company shall report the details of the accident, details, and processing details according to the analysis results, and organize a security incident response organization.
2. The information security department shall analyze the causes of security incidents and establish measures to prevent recurrence, report them to CISO, and apply measures to prevent recurrence.

③ Information security accident prevention

1. The information security department of the company shall establish a security education plan so that all employees of the company can receive information security education and training suitable for their duties.
2. In preparation for cyber-attacks, The Information Security Department of the company conducts simulated training for executives and employees of the company on a regular basis.

This policy will take effect on November 6, 2025.