Document Number	WMM-IS-A-00200
Final Modification Date	2024. 05. 20
Document Manager	Seung-chul Yang

HYNDAI WIA Data Protection Policy

2024.05.

[Approved by]

[HYUNDAI WIA]

CEO

Jae-Wook Jung

(Signature)

Document Number	WMM-IS-A-00200
Final Modification Date	2024. 05. 20
Document Manager	Seung-chul Yang

HYNDAI WIA Data Protection Policy

2024.05.

[Person in charge]

Information Security Team Leader
Sam-joo Kim (Signature)

[Approver]

Head of Business Management Division
Tae-gyu Yang (Signature)

Chapter 1 Data Protection Declaration

Data protection activities have become indispensable as the threat of information leakage of core technologies (including national core technologies) can seriously impact the work process and intellectual property of Hyundai Wia Co., Ltd. Therefore, executives and employees of Hyundai Wia Co., Ltd. must mobilize all capabilities and put the utmost effort into establishing and implementing the data protection management system to maintain stable and reliable business operations from information leakage and hacking threats, thereby Hyundai Wia Co., Ltd. declares the following policy.

Subjects of security protections include:

1. Information about core technologies (including national core technologies) produced in-house for business
2. Personal information collected through business operation
3. IT infrastructure facilities such as server/network for business operation
4. Important business information and business environmental assets required for the business operation
5. Physical location for processing business operation

We strive to practice safe information security management system and achieve the goal of protecting intellectual properties of Hyundai Wia Co., Ltd. by performing the following activities.

1. Establish the data protection management system to protect information, technology, and other assets.
2. Prepare an appropriate composition of human resource, facility, and regulation for data protection activities.
3. Establish and implement guidelines for managerial, physical, and technical data protection related to information, technology, and other assets.
4. To ensure that the data protection guidelines are properly implemented, inform the organization internally and conduct related education.
5. Establish basic measures for complying legal compliance, security accident management, and business continuity (disaster prevention) management.

In this endeavor, the board of the company shall proactively support necessary resources as follow.

1. Secure a sufficient budget for information security.
2. Organize necessary team for information security and support sufficient human resources.
3. Provide sufficient internal/external training for information security.

4. Ensure and support continuous sustention of the information security activities.

To ensure that this policy is continuously effective in accordance with changes in the external work environment, the person in charge of corporate security shall periodically review and update the data protection policies and guidelines and provide data protection education to executives and employees. In addition, former executives and employees of Hyundai Wia Co., Ltd. shall comply with the data protection policies and guidelines that are based on them in good faith and sincerity and shall fulfill their duties to ensure that data protection activities are maintained and enhanced continuously.

May 2024

Hyundai Wia Co., Ltd.

Chapter 2 General Provisions

Section 1 General Items

Article 1【 Purpose 】

The Data protection Policy is a top-level document with the purpose of determining the basic and necessary policies for Hyundai Wia Co., Ltd.'s (hereinafter referred to as the "Company" or "our Company") data protection activities.

Article 2【 Application Scope 】

1) This policy is subjected to all data protection tasks that are intended to protect all information, computerized infrastructure, and personnel related to the company's domestic and international business.
2) This policy applies equally to all corporate suppliers and overseas subsidiaries.

Article 3【 Terminology 】

Terms used within this Data Protection Policy can be specified separately in each sub-document if necessary.

1) Data Protection Declaration: A document that defines the basic direction and principles of data protection.
2) Information security organization: Refers to an organization (team and personnel) that manages information security.
3) Intellectual property: Information, information systems, facilities, etc. subjected to data protection.
4) Work continuity: Refers to not only the simple data backup, such backup of damaged data, which is difficult to operate in normal state due to natural disasters, but also fostering environment in which can guarantee the continuity of service and critical tasks.

Article 4【 Mutatis Mutandis 】

Security related activities shall comply with this Policy and other activities that are not specified in this Policy shall be governed by the relevant statutes and company's regulations.

Section 2 Responsibility and Authority

Article 5【 Company Security Officer_CSO 】

1) The head of the Business Management shall oversee the company security role.
2) The person in charge of company's security concurrently shall serves as the chairperson of the Information Security Council.
3) The person in charge of company's security shall have overall responsibility for the company's information security affairs and possesses the authority to direct and supervise the performance of information security affairs.
4) The person in charge of company's security shall have the authority to approve all data protection-related regulations (policies, guidelines, procedures, etc.).

Article 6【 Chief Information Security Officer_CISO 】

1) CISO shall be the head of the organization who oversees information security.
2) CISO shall assist the SCO of the company to manage the practical affairs concerning the planning, execution, evaluation, and improvement of information security affairs, and shall concurrently hold the position of executive secretary of the Information Security Council.
3) CISO shall have the responsibility to establish and implement guidelines for the effective operation of data protection tasks.
4) CISO shall check the status of data protection on its own according to the standards of the guidelines related to data protection.
5) CISO shall meet the qualifications required by domestic law.
    ① A person who obtained a master's degree at home or abroad in the field of information security or information technology.
    ② A person who has obtained a domestic or foreign bachelor's degree in the field of information security or information technology and has at least three years of work experience in the field of information security or information technology (including experience before obtaining a degree).
    ③ A person who has obtained a domestic or foreign professional bachelor's degree in the field of information security or information technology and has at least five years of work experience in the field of information security or information technology (including experience before obtaining a degree).
    ④ A person who has at least 10 years of work experience in the field of information

security or information technology.

⑤ A person who has obtained the qualification of an auditor certified as an information security management system.

⑥ A person who has worked for at least one year as the head of the department in charge of information security-related affairs.

6) CISO may concurrently perform only the following duties, and he/she shall not concurrently perform any other duties:

① Duties concerning the disclosure of data protection under Article 13 of Act related to the Promotion of the Information Security Industry.

② Duties of a responsible person in charge of data protection under Article 5(5) of the Information and Communications Infrastructure Protection Act.

③ Duties of the CISO under Article 21-2 (4) of the Electronic Financial Transactions Act.

④ Duties of a person in charge of personal data protection under Article 31(2) of the Personal Data protection Act.

⑤ Other duties that are necessary for the protection of information pursuant to this Act or relevant statutes.

7) If a company has sales assets of at least 5 trillion won in the previous year, the company is required to appoint the Chief Information Security Officer as a director-level executive officer. The term "director" refers to an executor of the company under the Commercial Act who has authority in the company to instruct a director to execute his/her duties, a person who directly executes his/her duties in the name of the director, and a person who is not a director but has the authority to execute the duties of the honorary chairman, chairman, president, vice president, executive director, director, director, and other companies.

8) Other provisions not mentioned in this policy shall be governed by domestic law and other guidelines related to data protection.

Article 7【 Company's Security Working-level Manager 】

1) He / she shall oversee the specific field of information security work.

(1) Working-level Manager of Security Management: Person in charge of managing security under the security related department

(2) Working-level Manager of Physical Security: Person in charge of managing physical security under the security related department

(3) Working-level Manager of Technology Security: Person in charge of managing security of technologies under the security related department

2) He / she shall be responsible for documenting data protection policies and guidelines and updating them.

3) He / she shall be responsible for supporting the data protection activities of the department (team).

4) Other matters not prescribed in this policy shall be governed by domestic law and other guidelines related to data protection.

Article 8【 Regional Security Officer 】

1) A regional security officer other than the headquarters shall be appointed as an executive responsible for his/her working area.

2) He / she shall be responsible for overseeing local information security affairs in accordance with all information security-related regulations of the company.

Article 9【 Department (Team) Security Manager 】

1) The security manager of the team (department) shall be responsible for performing all security protection activities of department (team) and manage the status.

2) The security manager shall be responsible for overall management of department's (team) security protection activities.

3) The security manager shall designate a person in charge of security of the department (team) and shall be responsible for implementing, directing, and supervising the security affairs of the department (team).

Article 10【 Department (Team) Security Officer 】

1) The security officer of the department (team) shall be responsible for performing all information security activities of the department (team) and managing the status quo.

2) The security officer of the department (team) shall continuously communicate with the person in charge of security affairs and seek cooperation for the data protection activities of the department (team).

3) The security officer of the department (team) shall report the results of information security activities to the person in charge of security of the department (team).

4) The security officer of the department (team) shall hold an event for the 'Security Day' every month, conduct security trainings, and report the results to the security portal.

5) The security officer of the department (team) shall conduct information asset classification once a year.

6) The security officer of the department (team) shall maintain the updated version of the security sticker management ledger of the security portal.

7) The security officer of the department (team) shall continuously improve and implement the weak points discovered from the security inspection results.

Chapter 3 Information Security Policy

Article 11【 Basic Principles for Data Protection 】

1) All intellectual properties used by executives and employees for business operation are owned assets of the company.

2) All intellectual properties are classified and managed according to its type and importance.

3) All information assets are accessible only to authorized users.

4) The person in charge of data protection shall restrict access from the outside to the inside to a minimum and shall devise security measures in advance the preparation for an infringement accident when accessing.

5) All purchased software is owned (or licensed) by the company and cannot be illegally copied without being subject to a licensing agreement.

6) The head of technical security shall establish an emergency plan to ensure the stability and reliability of the computer network in the event of various disasters and failures and conduct periodic tests to maintain its effectiveness.

7) Personnels in charge of information security shall verify compliance with information security policies and guidelines through periodic security inspection activities and formulate and implement countermeasures if necessary.

8) Executives and employees shall prevent damage caused by the influx of viruses and malicious code.

9) All employees shall receive information security training in accordance with their individual roles to recognize the importance of data protection and improve the ability to protect the data.

Article 12【 Compliance with Data Protection Policy 】

1) If an employee inflicts property damage or damages the public image of the company by violating this policy or subordinate security regulations, he/she may be disciplined in accordance with the relevant company regulations.

2) Information asset infringement incidents by outsiders shall be investigated in cooperation with related agencies to determine the cause and relevant action shall be taken in accordance with the related laws.

Article 13【 Operation of Data Protection Policy 】

1) All employees, third parties, and employees of cooperate suppliers, including overseas subsidiaries, shall be familiar with and comply with this policy and shall apply it to their duties.

2) The records of the performance of all obligations based on this policy shall be maintained/kept.

3) The Data Protection Regulations, which is a sub-document of this policy shall be applied in accordance with the areas of work defined in the document.

4) Based on this policy standard, each plant shall enact and implement detailed management rules consistent with the actual conditions of its own workplace.

Article 14【 Data Protection Regulations and Processes 】

1) Details for the application of this Data Protection Policy shall be provided separately in the following data protection regulations:

(1) Data Protection Management Regulations

(2) User Security Regulations

(3) Mobile Security Regulations

(4) Human Resource Security Regulations

(5) Regulations for Business Continuity Management

(6) Security Regulations for Computer Infrastructure Operation

(7) Regulations for Data Protection System Management

(8) Physical Security Regulations

(9) Regulations for Personal Data protection Management

(10) Operation Technology (OT) Security Regulations

(11) Defense Technology Protection Regulations

(12) Guidelines for Industrial Technology Protection

(13) Guidelines for Management of Continuity of Information Security Operations

(14) Cloud Security Guidelines

(15) Guidelines for Securing Personal Information Safety

(16) Data Security Guidelines

(17) Software Development Security Guidelines

2) To improve the level of implementation of the data protection policy and guidelines at the user level, the data protection process and method shall be separately documented.

(1) Data Protection Process

(2) Data Protection Regulation Form

Chapter 4 Data Protection Regulations

Article 15【 Regulations on Data protection Management 】

1) The purpose of this regulation is to establish, operate, evaluate, and improve the data protection management system for the safe and continuous operation of the company.

2) The regulation shall consist of the following:

(1) General provisions

(2) Configuration and operation of organization for data protection

(3) Management of data protection policies and regulations

(4) Risk management

(5) Security Incident Management

(6) Data security training

(7) Security audit

Article 16【 User Security Regulations 】

1) The purpose of this regulation is to prescribe data protection activities to be observed by users in order to minimize various accidents such as information leakage, alteration, misuse, and deletion of company's intellectual properties that may be caused by human resources.

2) The regulation shall consist of the following:

(1) General provisions

(2) Responsibilities and authorities

(3) User security compliance

(4) Security management of outsourced human resource

Article 17【 Mobile Security Regulations 】

1) The purpose of this regulation is to prescribe data protection activities that users must comply with in order to minimize various accidents such as information leakage, alteration, misuse, and deletion of company's intellectual properties that may occur through mobile devices.

2) The regulation shall consist of the following:

(1) General provisions

(2) Procedure for mobile business security review

(3) Standards for mobile business work process

(4) Feasibility of mobile work

(5) Mobile device utilization

(6) Mobile infrastructure protection

(7) Mobile app protection

(8) Protection of mobile devices provided by the company

(9) Guidelines for mobile app development and operation

(10) Mobile security management for users

Article 18【 HR Security Regulations 】

1) The purpose of this regulation is to determine the security control and managing the people who violated security regulations during the process of recruitment, retirement, and other personnel transfer.

2) The regulation shall consist of the following:

(1) General provisions

(2) Operation of HR security

(3) Process for data protection policy violators

Article 19【 Regulations on Business Continuity Management 】

1) This regulation sets the standards and procedures necessary for the company's preservation and emergency preparedness in case of emergency.
2) This Regulation shall consist of the following:
   (1) General Provisions
   (2) Establishment of emergency response plan
   (3) Emergency response simulation training
   (4) Maintenance of emergency response plan
   (5) Management of emergency contacts

Article 20【 Security Regulations for Operation of Computer Infrastructure 】

1) The purpose of this regulation is to prescribe the standards and principles of data protection activities in the process of operating computer infrastructure in order to provide safe and continuous services of the company.
2) This Regulation shall consist of the following:
   (1) General provisions
   (2) Responsibilities and authorities
   (3) Security management of computer infrastructure operation
   (4) Server security management
   (5) Network security management
   (6) Security management of applicable work system
   (7) Database security management
   (8) Security Management of computing machine room

Article 21【 Regulations on Information Security System Management 】

1) The purpose of this regulation is to prescribe data protection activities in the process of operating the data protection system in order to provide safe and continuous services of the company.
2) The regulation shall consist of the following:
   (1) General provisions
   (2) Responsibilities and authorities

(3) Operation and management of the information security system

Article 22【 Physical Security Regulations 】

1) The purpose of this regulation is to define the responsibilities and roles related to physical security, such as obtaining, modifying, disposing of, and taking out intellectual property from the company, and to safeguard our employees and facilities from inappropriate acts by unauthorized persons.

2) The regulation shall consist of the following:

(1) General provisions

(2) Access control

(3) Asset transfer control

(4) CCTV operation management

(5) Operation of security center

Article 23【 Regulations for Personal Data Protection Management 】

1) The purpose of this regulation is to manage personal information systemically and safely and to protect privacy from collection, misuse, and abuse of personal information, thereby enhancing the rights and interests of the company, employees, and customers, and further to realize the dignity and value of individuals by developing detailed rules concerning all personal information processing.

2) The regulation shall consist of the following:

(1) General Provisions

(2) Privacy protection organization

(3) Management and supervision of personal information

(4) Compliance with privacy

(5) Restrictions on the processing of personal data

(6) Infringement and processing of personal data

(7) Penalties

Article 24【 Supply network (OT) security regulations 】

The purpose of this regulation is for a stable operation of production plant by prescribing management and technical protection measures to protect the supply network (OT) consisting of

manufacturing facilities, manufacturing systems, and networks in the production plant for product manufacturing from cybersecurity threats.

This Regulation shall consist of the following:

(1) Overview

(2) Network protection measures

(3) Unit facility/system protection measures

Article 25【 Defense Technology Protection Regulations 】

The purpose of this Regulation is to prescribe provisions necessary for the protection of defense technology (hereinafter referred to as "defense technology") of the Company in accordance with the Defense Technology Protection Guidelines.

This Regulation shall consist of the following:

(1) General provisions

(2) Identification and management of technology

(3) Personnel control and facility protection

(4) Data protection

(5) Protection of defense technology in R&D

(6) Protection of technology in export and domestic transfer

Article 26【 Industrial Technology Protection Guidelines 】

The purpose of this guideline is to prescribe provisions necessary to prevent and protect the leakage of industrial technologies, such as national core technologies, in accordance with Article 8 of the Act on the Prevention and Protection of Industrial Technology from Leakage (hereinafter referred to as the "Act") and Article 10 of the Enforcement Decree of the Act on the Prevention and Compensation of Industrial Technology from Leakage (hereinafter referred to as the "Decree").

(1) General provisions

(2) Technical judgment and registration management

(3) Protection measures for core national technology

(4) Export of core national technology

(5) Foreign investment of organizations with core national technology, such as

overseas mergers and acquisitions, joint ventures, etc.

(6) Infringement report and recovery response

(7) Survey

(8) Supplementary provisions

Article 27【 Guidelines on Work Continuity of Data Protection Management 】

The purpose of this guideline is to prescribe provisions for the management and operation of the Company's information system to minimize damage and resume business at a normal state within a short period of time through prompt response in the event of an emergency such as an information system failure or disaster.

(1) General provisions

(2) Roles and responsibilities

(3) Establishment of a continuity plan for data protection work

(4) Data backup and dissipation measures

(5) Default measures

(6) Emergency measures

(7) Disaster recovery plan

Article 28【 Cloud Security Guidelines 】

The purpose of this guideline is to secure and protect the company's confidentialities by establishing the security principles of the cloud and prevent information leakage.

(1) Overview

(2) Cloud security review

(3) Private cloud security

(4) Public cloud security

Article 29【 Guidelines for Securing Personal Information Safety 】

The purpose of this guideline is to prescribe minimum standards pursuant to the Personal Data

protection Act for technical, administrative, and physical safety measures necessary to ensure safety and prevent the personal information from being lost, stolen, leaked, forged altered or damaged by the personal information processor.

(1) Purpose

(2) Definition

(3) Application of safety measure standards

(4) Establishment and implementation of internal management plans

(5) Management of access rights

(6) Access control

(7) Encryption of personal data

(8) Storage and inspection of access records

(9) Prevention of malware

(10) Safety measures of the management terminal

(11) Physical safety measures

(12) Safety measures for disasters

(13) Disposal of personal information

Article 30【 Data Security Guidelines 】

The purpose of this guideline is to safely protect administrative information and technical information in the creation, storage, utilization, and disposal of data in the information system for the safe and swift operation of the Company's business, and to comply with domestic and international regulations.

(1) Data security

(2) Data definition

(3) Data lifecycle management

Article 31【 Software development security guidelines 】

The purpose of this guideline is to secure the confidentiality, integrity, and availability of intellectual property through the security review procedure (process) of the entire process from the planning stage to the completion of development in order to develop safe software that can

counter cyber security threats when establishing a system and also for the safe and sustainable business operation of the Company.

(1) General provisions

(2) Compliance with software development methodologies

(3) Software development security procedure

(4) Secure coding security guideline