Information Security Regulation

1. Scope of Application

1.1 Purpose

The purpose of this Information Security Regulation (hereinafter “this Regulation”) is for SK Square Co., Ltd. (hereinafter “the Company”) to establish an operating standard for information security management system in order to safely and effectively protect the Company's information assets from theft, damage, falsification, leakage, etc., to have the employees comply with the standard, and thereby to strengthen its competitive edge, and to survive and develop in a safe business environment.

1.2 Scope of Application

This Regulation applies to all employees of the Company and all tangible and intangible information assets owned by the Company.

1.3 Definitions

The meanings of key terms used in this Regulation shall follow Annex #7 “Definitions of Information Security Terms.”

1.4 Review of Regulations and Guidelines

1) Internal regulations and guidelines shall be regularly reviewed for feasibility and enactment and amendments shall be made according to the results.
2) In order to continuously identify the information security-related legal requirements and keep them up-to-date, compliance with laws shall be performed as stated by the following procedure.

    (1) In case of changes to information security-related laws, their impact on information security regulations and related procedures shall be identified and reflected, and at that time, the legal affairs department and interested parties shall review it.

    (2) After obtaining approval of the reviewed amendment as required by the relevant regulation, the competent department shall publish and enforce the amendment company-wide.

    (3) Review of information security-related legal requirements shall be conducted on a regular/non-regular basis (regular: once a year, non-regular: when laws are enacted or amended).

2. Roles and Responsibilities of Employees

2.1 Roles and Responsibilities of Employees

1) Employees shall protect the Company's information assets and comply with its information security policies as well as processes.

2) For information security, employees are obligated to comply with the following.

   (1) Prohibition of the use of the Company’s information assets for private purposes (non-business purposes)

   (2) Prohibition of disclosure and provision of internal and external information assets without the Company’s approval

   (3) Compliance with prior control procedures when taking out or transmitting information assets

   (4) Only information assets within the scope of permission shall be used, and unauthorized access to information assets or attempts to acquire authorities other than permitted are prohibited.

   (5) Prohibition of the use of software and information storage media not approved by the Company

   (6) Prohibition of destruction of documents past the storage period and of their saving in user terminals

   (7) Compliance with daily security in the office environment

   (8) Report to the information security department when signs of information security incidents are found or information security incidents occur

   (9) Prohibition of other acts that increase the risk to the Company's information assets

3) When it is necessary to perform work on the internal network (intranet) via an external communication network for the following reasons, employees shall comply with Annex #8 “Remote Work Security Management Guidelines.”

   (1) When it is necessary to perform work in an external network environment for business purposes (business trip, meeting, etc.)

   (2) When physical office attendance is restricted (accident, disaster, infectious disease, etc.)

   (3) When response to information system failure and prompt support for work are required

   (4) In other cases where off-premise work is required for business purposes

4) For other security management standards for employees and outsiders, refer to Annex #2 “Personnel Security Management Guidelines.”

2.2 Roles and Responsibilities of Executives

1) Executives shall ensure that the security level of the organization in their charge can be maintained continuously. They shall encourage members of the organization to comply with security policies, and shall lead by example as an information security leader.
2) Executives shall ensure that their secretaries comply with the following.
   (1) Verify the locking status of laptops and doors in the absence of executives
   (2) Prohibition of direct management of executives' e-mail accounts
   (3) Prohibition of storing confidential documents for executives, handling them arbitrarily, etc.

2.3 Roles and Responsibilities of Organization Heads

1) The heads of organizations shall recognize that they are primarily responsible for information security of the unit organization. They have responsibility and obligation to maintain the unit organization's level of information security.
2) The heads of organizations shall encourage subordinates and the unit organization-managed BP/contractor employees to comply with the information security policies and processes, as well as provide education and supervision regarding information security.
3) The heads of organizations shall prevent vulnerabilities in the unit organization's information assets from occurring. If signs of an information security incident or security vulnerabilities are discovered, they shall promptly notify the information security department.

3. Responsibilities and Roles of Information Security Organizations

3.1 Chief Information Security Officer and Information Security Department

1) The Company shall appoint, from senior management, the Chief Information Security Officer (hereinafter referred to as "CISO"), who shall oversee and manage duties related to the Company's information security (establishment of information security policy, organization and operation of the Information Security Committee, analysis and management of risks, response to security incidents and recovery, etc.).
2) The information security department shall assist CISO's work and support company-wide information security oversight and decision-making. For detailed roles of CISO, refer to Annex #1 "Information Security Organizations and Roles."

3.2 Information Security Manager and Information Security Department, by Area of Work

1) The Company shall have an information security manager for each area of work. For details, refer to Annex #1 "Information Security Organizations and Roles."

2) If not expressly covered in Section 3.2 1), the information security department shall coordinate the roles of related works.

3.3 Information Security and lnformation Security Manager, by Department

1) If necessary, in order to efficiently carry out company-wide information security activities, CISO may designate an information security manager for organizations above a certain size. If necessary, the information security manager can perform security management (self-security diagnosis, etc.), participate in security education managed by the information security department, and can carry out dissemination within the department.

3.4 Composition and Operation of the Information Security Committee

1) The Information Security Committee shall operate to discuss the Company's information security issues.
2) The CISO shall serve as the chairperson of the Information Security Committee, which is composed of information security managers in various areas of work.
3) The roles of the Information Security Committee are as follows.
   (1) Review and approval of key information security policies and security-related issues
   (2) Review of important projects to strengthen information security
   (3) Review of information security plan, awareness, implementation, response measures to infringement incidents, etc.
   (4) Consultation and implementation of a company-wide information security activity plan
   (5) Establishment of company-wide information security-related processes
   (6) Consultation of company-wide, security-related work
4) Meetings of the Information Security Committee shall be held regularly, and can be convened by CISO when necessary.

4. Management of Information Assets

4.1 Management of Information Assets

1) Information asset management refers to continuous management of information assets by identifying, classifying, evaluating the importance of, and classifying information assets that are the basic target of information security.

2) The information security department may request information asset ownership departments to manage information assets.

3) Information asset management shall be governed by Annex #9 “Risk Analysis and Asset Management Standards,” and separate standards can be established and managed according to the area of work and the characteristics of the information system environment.

4.2 Identification and Classification of Information Assets

1) Information asset ownership departments have basic responsibility for identifying information assets, and if necessary, the information security department can request information asset ownership departments to identify information assets.

2) Information assets shall be identified and classified according to the criteria of information asset types under Annex #9 “Risk Analysis and Asset Management Standards,” and the classification criteria may be adjusted as stated by the characteristics of duties for the department.

4.3 Evaluation of Information Assets’ Importance and Classification of Security Levels

1) Information asset ownership departments shall evaluate the importance of identified information assets and assign security levels.

2) The information security department shall establish the importance evaluation criteria and the security level classification criteria, and can review the importance evaluation and security level classification of information asset ownership departments and make adjustments so that there is no difference in treatment of similar information assets between departments.

3) Information asset ownership departments shall periodically re-evaluate the importance of information assets and the adequacy of security levels.

5. Information Security, by Key Area of Work

5.1 IT Security Area

The IT security area covers information systems, manpower, facilities, etc. included in the internal network (intranet) and external services.

5.2 IT Security Information Security Activities

1) The information security department shall perform information security activities in the IT security area, and the IT security manager shall perform detailed roles under Annex #1 “Information Security Organizations and Roles.”

2) The information system operation department shall operate the information system in compliance with security policies and processes. If security vulnerabilities are discovered, the department shall take prompt actions after confirming them.

3) Details of IT security shall be governed by the IT Security Procedure Regulation.

5.3 Human and Physical Security Areas

Human and physical security areas refer to the human area of the Company's employees, BPs' employees, contractors' employees, and the Company's visitors. They also refer to the physical area of the Company's office buildings, leased offices and facilities.

5.4 Human and Physical Information Security Activities

1) The human and physical security management department shall perform information security activities in the human and physical security areas, and the human and physical security manager shall perform detailed roles as stipulated in Annex #1 "Information Security Organizations and Roles."

2) Human and physical information security activities can be directly performed by the information security department in consideration of the characteristics of work.

3) Details of human security shall be governed by Annex #2 "Human Security Management Standards," and details of physical security shall be governed by the regulations of the human and physical security management department.

6. Information Security Diagnosis

6.1 Performing Information Security Diagnosis

1) Information security diagnosis is to verify the compliance with information security policies and processes as well as the implementation of information security activities in the information security area.

2) The information security department is responsible for establishing an annual plan and performing information security diagnosis.

3) In the event of an information security diagnosis, the employees of the diagnosed department shall actively cooperate.

4) Information security diagnosis shall be carried out as follows.

   (1) Diagnosis of security policy and process implementation, etc.

   (2) Mock hacking

   (3) Diagnosis of information system security

   (4) Inspection of PC security

(5) Mock security training

(6) Diagnosis of new technology security, etc.

(7) Additional activities of security vulnerability-related diagnosis

6.2 Notification and Actions on Information Security Diagnosis

1) The information security diagnosis department shall notify the diagnosed department of the results, and the diagnosed department shall establish and implement an action plan based on the results.
2) The information security department shall collect the diagnosis results and the diagnosed department's action plan, report them to CISO, and manage implementation until the actions are completed.
3) In the case of technical vulnerabilities, measures can be taken in stages according to the severity and system situation, but in the case of serious vulnerabilities that may cause information security incidents, measures shall be taken immediately.

7. Information Security Education and Change Management

7.1 Establishment and Implementation of Education Plan

1) The information security department shall establish an annual plan for information security education and change management and conduct it regularly for employees.
2) Information security education and change management shall consist of required contents based on the subjects' position and the characteristics of their duties.

7.2 Review and Supplement Education Results

1) The information security department shall consider feedback on the results of education so that they can be reflected in the next education.

8. Establishment and Management of Information Security Investment Plan

8.1 Establishment and Management of Information Security Investment Plan

1) In order to improve the Company's level of information security and continuously carry out information security activities, the information security department shall establish an information security investment plan for the relevant area every year.
2) So that the information security investment plan can be smoothly implemented throughout the Company, the information security department shall manage the implementation of the plan.

9. Response to Information Security Incidents

9.1 Response to Information Security Incidents

1) In the event of an information security incident (and a personal information security incident), the information security control room shall be operated according to the severity of the incident and its impact shall be identified. The risks that may occur to the Company shall be minimized through prompt recovery measures.
2) Information security incidents occur in complex forms capable of damaging the Company's information assets and customers (external factors such as hacking and malware infection and internal factors such as theft, damage, and leakage of information assets). For details, refer to the Information Security Incident Response Regulation.

9.2 Roles and Main Activities of Organizations Related to the Information Security Incident Response

1) The information security department shall control and disseminate the situation of the information security incident and operate the information security general situation room.
2) The information security department shall analyze the causes and damage scale of the information security incident and take technical and administrative measures for recovery from the information security incident.
3) The company-wide crisis response organization shall figure out the situation in the media, government, and investigative agencies and perform duties according to the company-wide risk management system.
4) Details of response to information security incidents shall be governed by the Information Security Incident Response Regulation.

10. Information Security Rewards and Disciplinary Actions

10.1 Information Security Rewards

1) The CISO may request rewards for the organizations that practice excellent information security and customer information protection or for employees who have actively performed security activities and prevented information security incidents in advance.

10.2 Information Security Disciplinary Actions

1) If any of the following is suspected, the CISO may request disciplinary actions for the relevant organizations or employees according to internal regulations.

(1) In case of violation of this Regulation and the Company's security policies, principles, and guidelines

(2) In case of non-compliance with the obligation related to information security

(3) Where a security incident occurs or the Company’s risk thereof increases due to a lack of, or insufficient, information security measures

2) The agenda for rewards and disciplinary actions for organizations and employees shall be submitted through the Information Security Committee. Requests shall be made in consultation with the department in charge of the work concerned.

3) The Company may discipline the second-line supervisor and the first-line supervisor based on their responsibility for managing those who are subject to disciplinary action.

Addendum

This Regulation shall become effective on January 3, 2022.