Information Security Management System

Version 1.0

SK Chemicals Building, 310

Pangyo-ro, Bundang-gu,

Seongnam-si, Gyeonggi-do

Establishment/Amendment History

25 August 2025	Establishment	Version 1.0

Index

Chapter 1: Purpose

This document outlines the management system for implementing our security policy. Its purpose is to ensure that all employees, including our partner companies, are familiar with the management system and contribute to information security compliance.

Chapter 2: Scope

The scope of this document is as follows:

① Applicable Persons:
This document applies to all employees, as well as employees and temporary workers of all partner companies engaged in our business (hereinafter referred to as "Partner Companies").

② Applicable Work:
This document applies to all of our business. The purpose of this regulation also applies to the work of our branches and subsidiaries.

Chapter 3: Information Security Management System

To comply with information security governance, our company establishes and operates the following management system.

A. Information System Security Management System
To continuously monitor and improve our information security system, we strive to establish an information security system management system by establishing necessary procedures and security measures for the introduction, installation, and operation of information systems. Furthermore, to ensure stable operation of the information system and control any abnormalities, information leak paths for each target are controlled during the operation process, and necessary security measures are taken.

① Information system managers must request a prior security review from the security manager during application design and development.

② Information system managers must incorporate application security function requirements, including any supplementary measures based on the security review results.

③ Upon completion of design and development, information system managers must report to the security manager and information security manager whether the application security function requirements have been incorporated.

B. Data Protection Management System

To ensure the confidentiality, integrity, and availability of information, we establish clear operation and management procedures for all information systems.

① Information System Operation Procedures and Responsibilities

② Malicious Software Prevention

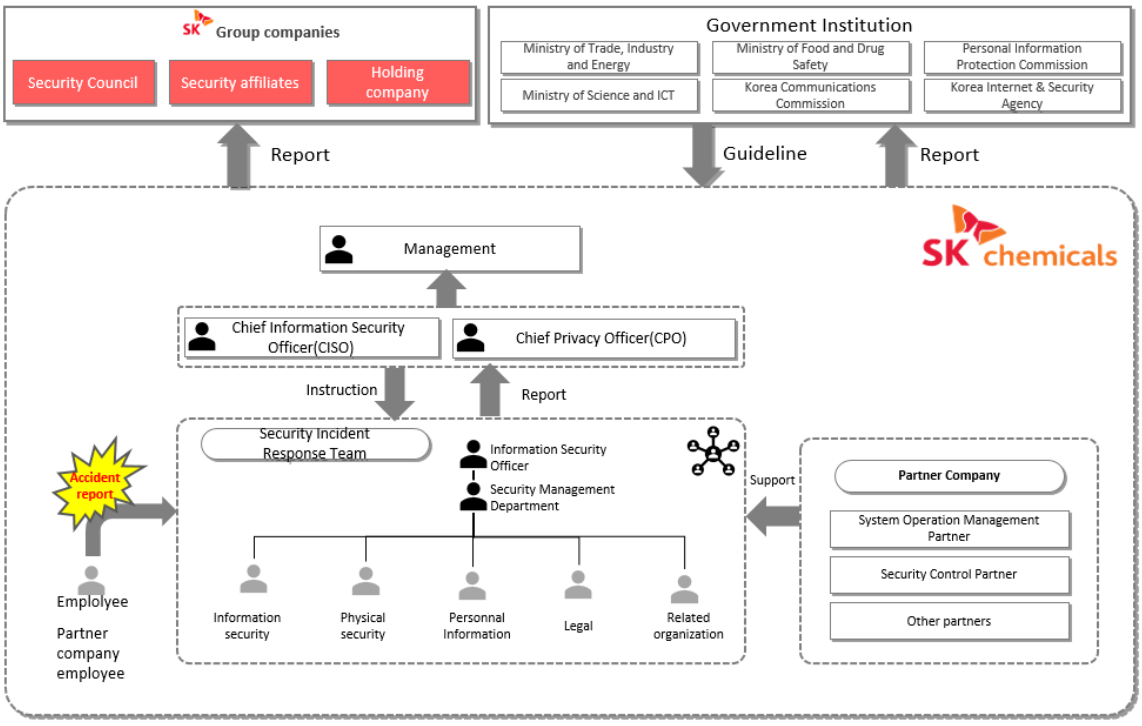
③ Media Management

④ Data Exchange with Other Organizations

⑤ Network Management Controls

C. Information Security Threat Monitoring and Incident Response System

We define prevention, response, and recovery procedures for information security incidents occurring within the company. This aims to prevent incidents in advance, minimize company losses resulting from incidents, and prevent recurrence. To prevent security incidents, we establish and operate a monitoring system that proactively inspects and detects potential security incidents.



[Image 01 : Information Security Threat Response System]

D. Employee Security Compliance System

We provide information protection and personal information training to ensure that our employees and associates adhere to our security policies. Employees and associates are required to comply with the terms of the pledge outlining their responsibilities for information protection and personal information protection.

① Employees
- Complete the Information Protection Pledge
- Complete the Information Protection and Personal Information Training

② Associate Employees
- Complete the Information Protection Pledge
- Complete the Information Protection and Personal Information Training

E. Business Continuity Management

For each major task, business continuity management requirements are defined, and a comprehensive plan is established, including emergency procedures, backups, and business resumption procedures. Furthermore, business continuity management plans are regularly tested and verified.

F. Security Audit

All employees including employees of partner companies, and temporary employees must comply with the company's security-related policies, regulations, and procedures. If necessary, they may conduct internal audits and audits or outsource the work to external experts. Violations of security policies, regulations, and procedures may result in disciplinary action in accordance with company regulations, and, depending on the circumstances, may be subject to criminal penalties.

G. Personal Information Protection

To protect personal information, the purpose of processing must be clearly defined, and only the minimum amount of personal information necessary for that purpose must be lawfully collected. Any use for any other purpose is prohibited.

To ensure the accuracy, completeness, and up-to-dateness of personal information, the personal information processing department must regularly manage the status of the personal information collected and retained, including the items, amount, purpose and method of processing, and retention period. To ensure the secure processing of personal information, the department must comply with

and implement the responsibilities and obligations stipulated in relevant laws and regulations.

Chapter 4: Enforcement Rules

Detailed rules for this security management system are governed by the relevant individual regulations and procedures.