SK Planet Information Security Policy

1 Purpose and Objective

1.1 This policy aims to elevate the Company's security and competitive standing by detailing the structure, roles, and core principles of IT security to all employees of SK Planet Co., Ltd. (hereinafter referred to as the "Company"), as well as all employees of suppliers and contracted companies who handle the Company's information, in compliance with the Information and Communications Network Utilization and Information Protection Act, the Personal Information Protection Act, and the Electronic Financial Transactions Act.

2 Scope

2.1 The Information Security Policy applies to all employees of the Company, as well as employees of its suppliers and contracted companies that handle the Company's information. It covers all types of information assets, including both tangible and intangible assets, as well as trade secrets.

3 Definition of Terms

3.1 Definitions for the key terms used in this policy can be found in the Regulation on IT Security Procedures.

4 Chief Information Security Officer

4.1 The Chief Information Security Officer is responsible for:

1) Developing the information security policy and management system

2) Monitoring and Diagnosing information protection levels

3) Overseeing the information protection organization

4) Reporting on the status of information security

5) Collaborating with external entities to enhance information security

6) Identifying and evaluating information security threats and offering protective measures

7) Establishing and conducting security awareness training and cybersecurity drills

5 Information Security Manager

5.1 The Information Security Manager is responsible for:

1) Developing and managing information security policy
2) Analyzing and ensuring compliance with legal and regulatory information security requirements
3) Providing information protection services
4) Performing IT security risk assessments and supporting audits
5) Monitoring for internal data leaks
6) Adopting, deploying, and improving information security solutions
7) Implementing information security controls and responding to data breach incidents
8) Diagnosing and monitoring IT security vulnerabilities
9) Conducting IT security technical training

6 Information Security Administrator

6.1 The Information Security Administrator is responsible for:

1) Establishing and implementing information security policies
2) Planning and implementing security awareness training
3) Overseeing information protection in the operation of the information system
4) Developing and implementing risk control measures
5) Developing and conducting remediation and mitigation actions following vulnerability assessments
6) Monitoring and responding to data breaches

7 Information Security Department and User

7.1 The Information Security Department is an expert team that supports the work of CISO and systematically implements the organization’s information protection activities. The department head is designated as the Information Security Manager, while the Information Security Administrator is appointed to perform a working-level role.

8 Information Protection Committee

8.1 The Information Protection Committee (herein after referred to as the “Committee”) is established to efficiently perform security functions and deliberate and decide on proactive security measures for major business plans. The Committee deliberates and decides on the following matters:

1) Planning and coordination of information security functions
2) Vulnerability assessment and evaluation
3) Establishment of proactive security measures when formulating major business plans
4) Security risks that cause major social concern
5) Major security incidents within the organization
6) Other matters related to the management of major security tasks

9 Asset Management

9.1 All information within the Company is considered an important asset, and the Company takes ownership of it.

9.2 All information assets will be classified according to their value, with classification indicating appropriate handling and management requirements.

9.3 Periodic risk assessments should be performed on all information assets and information system assets, and appropriate security controls must be applied based on the results.

9.4 The Regulation on IT Security Procedures stipulates extensive provisions for asset management.

10 User Account Management

10.1. User accounts should be registered, with their registration information recorded, maintained, and managed. Periodic checks should be conducted to ensure their validity.

10.2. The Regulation on IT Security Procedures stipulates extensive provisions for user account management.

11 Password

11.1. Each user must have a unique, strong password that is difficult to guess and must not share it with anyone.

11.2. The Regulation on IT Security Procedures stipulates extensive provisions for password.

12 Access Management

12.1 User access to information assets is determined by the need-to-know principle, adhering to the principle of least privilege.

12.2 The Regulation on IT Security Procedures stipulates extensive provisions for access management.

13 Access control

13.1 Users should not attempt to access the system without approval from the relevant authority.

13.2 Remote connections should occur only for authorized work, and protected information should not be leaked or disclosed.

13.3 The Regulation on IT Security Procedures stipulates extensive provisions for access control.

14 Security review

14.1 When introducing any hardware or software, the purchasing procedures must be adhered to, and any service program must be developed with security in mind. Additionally, personnel responsible for information protection diagnostics must assess their information security functions.

14.2 The Regulation on IT Security Procedures stipulates extensive provisions for security review.

15 Software

15.1 Users are prohibited from using illegal software, and will be held accountable for any consequences resulting from such use.

15.2 The Regulation on IT Security Procedures stipulates extensive provisions for software use.

16 Computer Virus Control

16.1. The Information Security Manager must equip all Company computers with antivirus software capable of detecting and removing viruses.

16.2 The Regulation on IT Security Procedures stipulates extensive provisions for computer virus control.

17 Security Checks

17.1 The Information Security Manager is responsible for ensuring compliance with this policy and related procedures by conducting regular security level checks and recommending necessary remedial measures when needed.

17.2 The Regulation on IT Security Procedures stipulates extensive provisions for security checks.

18 Security Incident Reporting

18.1 Any executive or employee who is aware of security incidents and information leakage must immediately report them to the Information Security Manager.

18.2 The Regulation on IT Security Procedures stipulates extensive provisions for security incident reporting.

19 Education and Training

19.1 The Company, its employees, and all users bound by a business contract are required to follow the education and training outlined in the information security regulations and procedures, to ensure ongoing protection of the Company’s assets.

19.2 The Regulation on IT Security Procedures stipulates extensive provisions for education and training.

20 Recovery Plan

20.1 For each information asset, information system operators must independently establish and execute a disaster recovery plan. This plan should encompass recovery priorities, operational procedures, emergency communication networks, testing methodologies, and inspection intervals, all aimed at ensuring effective recovery in the event of a disaster.

20.2 The Regulation on IT Security Procedures stipulates extensive provisions for recovery plan.

21 Addressing an Infringement Incident

21.1 In the event of an infringement incident, the Chief Information Security Officer has the authority to temporarily establish and manage a response team to ensure an effective reaction.

21.2 The individual responsible for handling infringement incidents should facilitate the collection of pertinent evidence for subsequent investigation. They should also analyze the root cause of the infringement to expedite the restoration of the service.

21.3 The Regulation on IT Security Procedures stipulates extensive provisions for addressing infringement incidents.

22 Disciplinary Measures

22.1 The nature of disciplinary measures is governed by the disciplinary rules outlined in the personnel regulations. Nonetheless, based on the personnel committee’s deliberation results, a warning can be issued to the individual facing disciplinary action, instead of enforcing a disciplinary measure.

22.2 The Regulation on IT Security Procedures stipulates extensive provisions for disciplinary measures.

23 Maintenance of IT Security Management Policies

23.1 The information security policy officer must conduct an annual review of the feasibility of IT security management and procedural policies, with the discretion to conduct additional reviews as needed.

23.2 Revisions to the IT security management policies must be approved by the Chief Information Security Officer after consultations with the relevant practitioners to consider the revision factors.

23.3 The Regulation on IT Security Procedures stipulates extensive provisions for the maintenance of IT security management policies.

24 Information Protection Management System

24.1 The Information Security Department must identify all tangible and intangible assets that impact the Company’s core services, define the scope of information protection management system, and develop and implement an annual information protection plan to maintain it.

24.2 The Regulation on IT Security Procedures stipulates extensive provisions for information protection management system.