posco
포스코퓨처엠

정보보호 및 개인정보보호 정책
(Information Security & Privacy Policy)

Last revision on	**'24. 05. 31.**	**Enacted on**	**'23. 04. 28.**
Rev.	**1**	**Document No.**	**-**
Managed by	**Information Security Bureau**		
Reviewed by	**Head of Information Security Bureau**		
Approved by	**CEO**		

Purpose

The purpose of this policy is to protect POSCO FUTURE M's information assets safely and effectively and to set out the compliance requirement that officers/employees shall comply with in order to protect the personal information of customers who use POSCO FUTURE M's services, officers/employees, and contractors.

Scope of Application

This policy applies to POSCO FUTURE M and its employees. All affiliates, invested corporations, and employees of POSCO FUTURE M, as well as partner and contract companies that do business with POSCO FUTURE M, are encouraged to comply with this policy or a similar policy at the same level as this policy.

Code of Conduct

1. **We strive to secure and maintain our global competitiveness by complying with international standards for information security and relevant domestic and foreign laws and by protecting information assets such as core technologies and HR, which are the source of our competitive edge.**
2. **Officers/employees shall recognize that they are the main agents for information security and continuously participate in education and training sessions to improve security levels.**
3. **Officers/employees make information security part of their daily routine and establish related activities as a corporate culture.**
4. **The purpose of collecting personal information shall be specified at the time in the context, and the data controller shall process personal information only to the necessary to achieve such purpose may take place to reach.**
5. **We shall use personal information within the scope of the purpose for which it was**

collected and select methods to minimize the privacy infringement of data subjects.

Action Plans

1. **Information Security Management System**

   - We shall ensure the stable operation of information systems and establish and operate an information security management system to minimize the industrial losses that security accidents may cause.

   - We shall establish and operate procedures to control security risks and monitor and review information security activities.

   - We shall establish methods and standards to identify and evaluate risks to key information assets and regularly conduct risk assessments.

   - We shall provide regular training to all officers/employees and establish a regular management and inspection system to ensure the effectiveness of information security.

2. **Personal Information Protection Measures**

   - We shall prepare protective measures for the processing stage, including collection, storage, use, provision, and destruction of personal information, to protect privacy, freedom, and rights of details of the subject throughout the above stages.

   - We shall manage personal information safely through appropriate technical, administrative, and physical protection measures under the degree of risk and possibility of infringement of the subject rights.

   - We shall generally disclose matters related to the processing of personal information, such as the personal information processing policy. We shall also prepare reasonable procedures to ensure that the rights of information principals, such as the right to request access to their information, are guaranteed.

   - The department in charge of personal information shall provide training on personal information protection to raise awareness of personal information handlers, including officers/employees, and to prevent personal information from being misused, abused, and leaked.

3. **Role of the Information Security and Privacy Officer**

   - The information security and privacy officer shall oversee the information security and privacy policy, and the above officer also establish and manage an information security

management system.

- The competent department shall monitor the implementation of information security and privacy policies and address security vulnerabilities.

4. Report and Discipline

- Officers/Employees shall immediately report security incidents to the officer or department head in charge of security.

- The company shall establish a standard of criteria and operation for information security and privacy violations. The company may discipline officers/employees based on such measures.

5. Related Internal Standards

- Regulations: Information security regulations, Privacy regulations, etc.

- Policy: Information Systems Security Policy, (Korea) National Core Technology Management Policy, Drawing Management Standards, Physical Access Control Management Policy, Document Management Policy, Integrated Security Monitoring Policy, Information Security Policy for POSCO, Operational Technology(OT) Security Management Policy, etc.