Personal Information Protection

Document No.: SWS-C-001

Effective Date: January 1, 2025

Table of Contents

1. General Provisions
2. Personal Information Protection Organization
3. Guarantee of Data Subject Rights
4. Secure Management of Personal Information
5. Security Incidents
6. Security Audits and Training

1. General Provisions

A. Purpose of the Personal Information Protection

The purpose of these regulations is to comply with applicable information security laws and regulations, including the Personal Information Protection Act, the Act on Promotion of Information and Communications Network Utilization and Information Protection, and the Act on the Protection of Information and Communications Infrastructure. These regulations aim to define detailed measures necessary to effectively protect customers' personal information from misuse, damage, falsification, and leakage.

B. Scope of Application

These regulations apply to all employees of SWECO Inc. and to any third parties who access the company's information assets under contractual relationships.

C. Definitions of Terms

The definitions of terms used in these regulations are as follows:

1) "Personal Information" refers to information relating to a living individual that falls under any of the following categories:
   - Information that can identify an individual, such as name, resident registration number, video images, etc.
   - Information that may not identify an individual on its own but can easily be combined with other information to do so. Whether the information can be "easily combined" shall be reasonably assessed considering the possibility of acquiring such other information, and the time, cost, and technology required to identify the individual.
   - Information that, by pseudonymizing the two categories mentioned above in accordance with Subsection 1-1, cannot identify a specific individual without the use or combination of additional information to restore it to its original state (hereinafter referred to as "pseudonymized information").

   1-1) "Pseudonymization" refers to the processing of personal information in such a way that specific individuals cannot be identified without the use of additional information, by deleting parts of the information or replacing them entirely or partially.

2) "Processing of Personal Information" refers to actions such as collection, generation, linkage, association, recording, storage, retention, processing, editing, retrieval, output, correction, recovery, use, provision, disclosure, disposal, or any similar activities involving personal information.

3) "Data Subject" means an individual who can be identified by the processed information and is the subject of that information.

4) "Chief Privacy Officer (CPO)" refers to the person who has overall responsibility for the processing of personal information within the organization, as defined in Article 32(2) of the Enforcement Decree.

5) "Personal Information File" means a set of personal information that is systematically arranged or organized according to specific rules, making it easily searchable.

D. Principles of Personal Information Protection

All employees of SWECO Inc. must comply with the following principles of personal information protection:

1) Personal information processors shall clearly define the purpose of processing and collect only the minimum personal information necessary for that purpose, in a lawful and legitimate manner.

2) Personal information shall be processed lawfully within the scope necessary for the stated purpose, and shall not be used for any other purpose beyond that scope.

3) Personal information processors shall ensure the accuracy, completeness, and currency of personal information within the necessary scope of the processing purpose.

4) Personal information shall be managed securely, taking into account the possibility and level of risk of rights infringement to the data subject, depending on the method and type of processing.

5) The privacy policy and other matters related to the processing of personal information shall be made publicly available, and the rights of data subjects (such as the right to access) must be guaranteed.

6) Personal information shall be processed in a manner that minimizes intrusion into the data subject's private life.

7) Where the purpose of collecting personal information can be achieved through anonymization or pseudonymization, anonymized data shall be used.
If anonymization is insufficient to achieve the intended purpose, pseudonymized data may be used instead.

8) Employees shall strive to earn the trust of data subjects by complying with and implementing responsibilities and obligations prescribed under the Personal Information Protection Act and other relevant laws and regulations.

2. Personal Information Protection Organization

A. Duties of the Chief Privacy Officer

The Chief Security Officer (CSO) shall oversee all matters related to the protection of customer personal information and shall perform the following functions:

- Establish policies for the protection of customer personal information.
- Implement internal management systems to prevent the leakage of customer personal information.
- Take prompt and proactive remedial actions in the event of personal information breaches or related incidents
- Conduct company-wide training programs on personal information protection.
- Plan and conduct regular monitoring and simulation training related to the protection of customer personal information.
- Address other matters deemed necessary to ensure the protection of personal information.

B. Duties of Personal Information Controllers

- All personal information controllers must comply with the Personal Information Protection Act, its Enforcement Decree, Enforcement Rules, and the principles of personal information protection.
- Upon recognizing any personal information breach, the controllers must promptly report the incident to their department head and the Chief Privacy Officer.
- All controllers must complete relevant training organized by the Chief Privacy Officer and sign a confidentiality agreement related to information security and privacy protection.

3. Guarantee of Data Subject Rights

A. Rights of the Data Subject

The data subject shall have the following rights with respect to the processing of their personal information:

- The right to be informed about the processing of their personal information.
- The right to determine and consent to the processing of their personal information, including the scope and purpose of such consent.

- The right to confirm whether personal information is being processed and to request access to such information (including the issuance of copies).
- The right to request the suspension, correction, deletion, or destruction of their personal information.
- The right to seek prompt and fair remedies for any damages incurred as a result of the processing of their personal information.

B. Access to Personal Information

A data subject may request access to their personal information processed by a personal information controller.

C. Correction and Deletion of Personal Information

1) A data subject who has accessed their personal information may request the personal information controller to correct or delete such information.
However, if the information is specified by other applicable laws or regulations as subject to collection, the data subject may not request its deletion.

2) Upon receiving a request from the data subject under Paragraph 1, the personal information controller shall, unless otherwise specified by special procedures under relevant laws, promptly review the request and take necessary actions such as correction or deletion, and notify the data subject of the outcome.

D. Destruction of Personal Information

1) When personal information becomes unnecessary—due to expiration of the retention period, achievement of the purpose of processing, or other reasons—the personal information controller shall promptly destroy such information.
However, this does not apply if preservation is required under other applicable laws or regulations.

2) When destroying personal information pursuant to Paragraph 1, the personal information controller shall ensure that the information is rendered irrecoverable and irreproducible.

4. Secure Management of Personal Information

A. Obligation to Take Safety Measures

Personal information controllers shall take technical, administrative, and physical measures necessary to ensure the security of personal information—such as establishing internal management plans and retaining access logs—in accordance with the Presidential Decree, to

prevent loss, theft, leakage, falsification, alteration, or damage of personal information.

B. Security Guidelines

1) All employees shall sign and submit an Information Security Pledge upon joining or leaving the company, and when signing annual employment contracts.

2) When outsourcing tasks to third parties or allowing access to the company's information assets, the relevant parties must also sign a Confidentiality and Information Security Agreement, agreeing to comply with all related policies and regulations.

3) All company facilities shall be managed according to their designated security levels, classified as General Areas, Protected Areas, and Restricted Areas.

4) No employee or third party is allowed to extract the company's information assets from company premises without authorization.

5) Network traffic monitoring must be continuously performed, and any abnormal signs must be reported immediately to the Chief Privacy Officer (CPO) or other relevant authorities for prompt action.

6) Personal information must be used only for pre-authorized purposes, and its entire lifecycle—from collection and distribution to storage and disposal—must be strictly managed to prevent improper exposure, misuse, or unauthorized leakage.

5. Security Incidents

A. Personal Information Breach

A personal information breach refers to any incident in which a personal information controller loses control over a data subject's personal information or allows unauthorized access, not caused by applicable laws or the controller's voluntary intent. Such breaches include, but are not limited to, the following cases:

- Loss or theft of documents, portable storage devices, laptop computers, or other media containing personal information.
- Unauthorized access to databases or other personal information processing systems by individuals who do not have proper access rights.
- Delivery of files, paper documents, or other storage media containing personal information to unauthorized persons due to intentional or negligent actions of the personal information controller.

- Any other case in which personal information is disclosed or transferred to an unauthorized individual.

B. Notification of Personal Information Breach

1) When a personal information controller becomes aware of a personal information breach, they must immediately report it to the Chief Privacy Officer (CPO). The CPO shall promptly take necessary actions and implement measures to minimize potential damage.

2) Upon becoming aware of the breach, and unless there is a justifiable reason, the personal information controller must notify the affected data subjects within 5 days of the incident, providing the following information.
However, if immediate measures are necessary to block access paths, address system vulnerabilities, or delete leaked data to prevent further exposure or spread, the notification may be sent within 5 days after such emergency measures have been completed:
   - The types or categories of personal information leaked
   - The time of the breach and how it occurred
   - Guidance for data subjects on how to minimize possible damages
   - The controller's response actions and procedures for damage relief
   - Contact information for the responsible department that handles inquiries or complaints in the event of damages

3) If it is not possible to confirm all of the items listed in Paragraph 2 at the time of notification, the controller may initially inform the data subject of the following and provide full details as soon as they are confirmed:
   - That a breach involving the data subject's personal information has occurred
   - Any of the items in Paragraph 2 that have been confirmed at the time of notification

4) If the personal information controller fails to notify the data subject within 5 days from the actual occurrence of the breach due to failure to detect the incident, they shall be required to prove the exact point in time when the breach was discovered.

6. Security Audits and Training

A. Information System Monitoring

1) The Chief Privacy Officer (CPO) shall regularly review the personal information management system and actual operational practices to identify and remediate vulnerabilities.

2) If any vulnerabilities or violations of security policies are identified during the monitoring process, appropriate remedial measures must be taken without delay.

B. Personal Information Protection Training

The Chief Privacy Officer shall plan and implement training programs necessary to prevent incidents such as the leakage of customer personal information.

Supplementary Provisions

A. Effective Date

These regulations shall take effect on January 1, 2025.