Detailed Regulations on Personal Information Protection

Established December 1, 2008
Amended November 28, 2012
Amended February 19, 2018

Article 1 (Purpose) The purpose of these detailed regulations is to set forth matters needed to protect personal information and implement activities thereof within Pohang University of Technology and Science (hereinafter referred to as University) in accordance with the Regulations on Security of the University and related legislation.

Article 2 (Subject and Scope of Application) These detailed regulations shall apply to personal information and persons who handle personal information which are collected, saved, used, transmitted or discarded via the University's network or other means besides the network.

Article 3 (Definition) The definitions of terms used in these detailed regulations are as follows:

1. "Personal information" refers to information of a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified (including information by which the individual in question may not be identified but can be identified by a simple combination with other information).
2. "Personal information manager" refers to a person at the University who collects, keeps, processes, uses, provides or discards the personal information of members of the University.
3. "Subject of information" refers to a person who can be identified with the managed information and therefore the subject of the information concerned.
4. "Personal information file" refers to an aggregate of personal information which is systematically arranged or organized according to a predetermined rule so that personal information can be readily searched.
5. "Management" refers to collecting, creating, recording, saving, possessing, processing, editing, searching, printing, correcting, restoring, using, providing, disclosing, and discarding personal information, and other acts similar thereto.
6. (Deleted February 19. 2018)
7. "Image data processing equipment" refers to equipment permanently installed in a predetermined area to film images, etc. of a person or object, or to transmit such images via a wired or wireless network.
8. (Deleted February 19. 2018)
9. "Entrance control system" refers to a device which automatically controls entering and exiting an area which requires security.

Article 4 (Duties and Responsibilities) ① In accordance with the Regulations on Security, the Personal Information Protection Officer shall organize a Personal Information Protection Department and Personal Information Protection Staff to efficiently perform the personal information protection duties of the University.

② The Personal Information Protection Department shall perform the following as a unit organization performing matters related to personal information protection of the University after receiving orders from the Personal Information Protection Officer:

1. Execute personal information protection plans and set budgets
2. Manage related regulations
3. Protect and manage personal information files
4. Hold classes on personal information protection
5. Handle services for external personal information protection
6. Other matters related to protecting personal information

③ The Personal Information Protection Staff in charge of protecting personal information shall include a Personal Information Protection Controller, Personal Information Protection Working-level Staff, Fellow

Personal Information Protection Controller, Fellow Personal Information Protection Staff and Personal Information Manager, and shall act as follows:

1. The Personal Information Protection Controller, who is the Director of the Personal Information Protection Department, shall manage and oversee all matters pertaining to protecting personal information at the University, and report important matters related to personal information protection to the Personal Information Protection Officer, etc.
2. The Personal Information Protection Working-level Staff, who receives orders from the Personal Information Protection Controller, shall be in charge of working-level jobs pertaining to protecting personal information and execute established plans for personal information protection, etc.
3. The Fellow Personal Information Protection Controller, as the Director of a unit organization, shall manage, oversee, etc. working-level jobs of personal information protection within the department he/she is affiliated with after receiving orders or supervision from the Personal Information Protection Officer.
4. The Fellow Personal Information Protection Staff in charge of working-level jobs of personal information under the supervision of the Fellow Personal Information Protection Controller shall handle working-level jobs in unit organizations by receiving orders and supervision from the Fellow Personal Information Protection Controller.
5. The Personal Information Manager shall perform and be responsible for the following activities related to protecting personal information at the University:
   a. Participate in personal information protection activities
   b. Comply with and execute policies on personal information protection
   c. Execute standards for technical and managerial protection measures of personal information
   d. Check, etc. for illegal and unjust violations of personal information within the University
   e. Implement other matters related to protection of personal information

Article 5 (Principles for Protecting Personal Information) (Deleted February 19, 2018)

Article 6 (Collection and Use of Personal Information) (Deleted February 19, 2018)

Article 7 (Providing Personal Information) (Deleted February 19, 2018)

Article 8 (Restrictions on Using and Providing Personal Information) (Deleted February 19, 2018)

Article 9 (Restrictions on Managing Unique Identification Information) (Deleted February 19, 2018)

Article 10 (Destruction of Personal Information) (Deleted February 19, 2018)

Article 11 (Restrictions on Management of Personal Information due to Consignment) (Deleted February 19, 2018)

Article 12 (Protection of Personal Information) The Personal Information Protection Officer shall devise protection measures stated in the following subparagraphs to prevent personal information from being lost, stolen, leaked, forged or damaged:

1. Restrictions of physical access
2. Protection when copying and printing
3. Manage and confirm access rights of Personal Information Manager
4. Encryption of personal information
5. Access control
6. Prevention of forging access records
7. Installation and operation of security programs

Article 13 (Personal Information File Register) (Deleted February 19, 2018)

Article 14 (Inspection of Personal Information) (Deleted February 19, 2018)

Article 15 (Correction or Deletion of Personal Information) (Deleted February 19, 2018)

Article 16 (Suspension of Managing Personal Information) (Deleted February 19, 2018)

Article 17 (Report of Personal Information Violation) (Deleted February 19, 2018)

Article 18 (Education on Personal Information Protection) The Personal Information Protection Officer shall regularly hold educational classes for personal information managers and subjects of information to protect personal information kept by the University.

Article 19 (Treatment of Entrance Records) Except for those stipulated in the Detailed Rules on General Security, the entrance records, recorded and managed by the entrance control system operated for the

University's security, shall be in accordance with these detailed regulations as the location information of individuals.

Article 20 (Ensuring Rights of Data Subject) The Personal Information Controller shall take appropriate measures in accordance with Chapter 5 of the Personal Information Protection Act, Chapter 6 of the Enforcement Decree of the Personal Information Protection Act, and reasonable internal process accordingly, and shall notify the reason and result of processing if a data subject (or a deputy) requests inspection, correction, deletion, suspension, etc. of the personal information. Provided, that the same shall not apply where there are special regulations in statute.

Article 21 (Internal Management Plan) ① A Personal Information Protection Officer must establish and implement an yearly internal management plan in order to protect personal information and ensure rights of data subject.

② An internal management plan must include the following:

1. Matters concerning whether the Personal Information Protection Officer has been designated
2. Matters concerning the role and responsibility of the Personal Information Protection Officer and the Personal Information Manager
3. Matters concerning necessary measures to ensure safety
4. Matters concerning the education of the Personal Information Manager
5. Other matters necessary for personal information protection

③ If there is any significant change in the items of Paragraph 2, the Personal Information Protection Officer must modify and implement the internal management plan immediately, and the revision history must be managed.

Article 22 (Inspection of Personal Information Protection Status) ① The Personal Information Protection Officer may conduct a status inspection of the following items in order to investigate the appropriateness and security management status of the general personal information protection work of the University:

1. Matters concerning the personal information and management of the personal information files processed by the Personal Information Controller, and installation and operation of image information processing equipment
2. Matters concerning the technical, operational, and physical measures to ensure safety of personal information
3. Matters concerning the data subject's request of inspection, correction, deletion, suspension of personal information, and the current status of measures
4. Other matters necessary for investigation of safety and appropriateness of the University's personal information processing and protection

② The Personal Information Protection Staff must cooperate with the status inspection.

Article 23 (Sanctions) ① In the case of violation of statutes and regulations related to the protection of personal information, if the University receives penalties for property such as a fine, the relevant department that bears the reason for the liability shall bear the penalty.

② The Personal Information Protection Officer may shut-down the internet service such as website, etc. if necessary in the case the personal information is leaked or exposed from the personal information processing system.

Addenda

1. These detailed regulations shall be amended and implemented as of November 28, 2012.
2. Items processed before the implementation of these detailed regulations shall be seen as being processed by these detailed regulations.

Addendum

These detailed regulations shall be amended and implemented as of February 19, 2018.

(Attachment: Form 1) Other use of personal information and provisions to third party register (Deleted February 19, 2018)

(Attachment: Form 2) Personal information file register (Deleted February 19, 2018)

(Attachment: Form 3) Personal information (inspection, correction/deletion, management suspension) request form (Deleted February 19, 2018)