Regulations on Security

Established November 28, 2012

Article 1 (Purpose) The purpose of these regulations are to protect all tangible and intangible information assets of Pohang University of Science and Technology (hereinafter referred to as the University) and to regulate processing and activities of security.

Article 2 (Applicable Subjects and Scope) ① These regulations shall be applicable to all members using and managing tangible and intangible information assets of the University and external personnel contracted for the University's needs.

② The range of the application shall be all tangible and intangible information assets of the University, which require managerial, physical and technical security, and the subsidiary facilities. However, a separate corporation using the University network must establish its own security regulations and follow the University's Regulations on Security if security incidents occur.

Article 3 (Obligation and Responsibility) All members and related external personnel using and managing tangible and intangible information assets of the University must comply with the University's Regulations on Security and related legislation, and shall have the obligation and responsibility to protect the University's information assets within their provided rights to use and manage the assets.

Article 4 (Definition) The terms used in these regulations shall have the following meanings:

1. "Information assets" refer to information owned by the University such as electronic information and data, hardware, software, physical environment, human assets and documents, intellectual property, and information related to technology and academic research.
2. "Information security" or "information protection" refers to all activities to devise a managerial, physical and technological means to prevent leakage, forgery and tampering, damage etc. of information collected, processed, saved, searched, transmitted and received via the information system and information network, including cyber security.
3. "Information system" refers to hardware and software needed for collecting, processing, saving, searching, transmitting and receiving information, including terminals such as a server or a personal computer, an auxiliary memory medium, a network device, an application program, etc.
4. "External personnel" refers to all personnel beside members of the University, and consists of outsourcing personnel, external research participation personnel, personnel in consigned shops, and other external personnel depending on their use of the University's assets.
5. "Security incident" refers to an incident where the University's information asset has been viewed, leaked, damaged or changed without permission.
6. "Danger evaluation" refers to the act of calculating the level of danger after measuring the size of the danger depending on the importance of information assets and the weakness in confidentiality, integrity, and availability of information assets.
7. Other terms shall follow common definitions.

Article 5 (Chief Security Officer) ① The Provost & Executive Vice President shall be the Chief Security Officer (hereinafter referred to as CSO) who manages all information security activities, and shall also be the chairperson of the Security Committee.

② The CSO shall perform the following activities:

1. Setting security strategy plans
2. Policies related to security
3. Establishing and enforcing the security budget
4. Organizing and operating the University's security organization
5. Other security activities of the University

③ The CSO shall create a security organization as in Attachment 1 in order to efficiently and systematically perform security activities of the University, and shall designate fellow officers in charge of security.

Article 6 (Fellow Officers in Charge of Security) ① Fellow officers in charge of security shall include a Personal Information Protection Officer, a Research Security Officer, and an Information Security Officer.

② The Personal Information Protection Officer shall be a Vice President representing the position of each group unit, and shall perform the following activities:

1. Creating and enforcing personal information protection plans
2. Establishing and amending regulations related to personal information protection
3. Administering and managing overall matters related to personal information protection
4. Submitting items in the personal information protection field to the Security Committee for consideration
5. Other activities defined by presidential decree

③ The Research Security Officer shall be a Vice President who directs research-related jobs, and shall perform the following activities:

1. Creating and enforcing research security policies and basic plans
2. Establishing and amending regulations related to research security
3. Administering and managing overall matters related to research security
4. Submitting items in the research security field to the Security Committee for consideration
5. Other activities defined by presidential decree

④ The Information Security Officer shall be a Vice President who directs information security jobs, and shall perform the following activities:

1. Creating and enforcing information security policies and basic plans
2. Establishing and amending regulations related to information security
3. Administering and managing overall matters related to information security
4. Submitting items in the information security field to the Security Committee for consideration
5. Other activities defined by presidential decree

Article 7 (Security Committee) ① A Security Committee (hereinafter referred to as Committee) shall be established under the CSO to deliberate on major items related to security, and shall be organized as follows:

1. With the CSO as the chairperson and the Head of Information Security working-level department as the secretary, the Committee shall be composed of 10 or so position holders, and the members of the Committee shall be as stated in the Attachment.
2. The term of membership for each committee member, including the chairperson, shall be the duration of incumbency.
3. The Committee shall be assembled by notifying items and contents for discussions via an official document by a working-level department which has items to discuss seven days in advance.

② The Committee shall deliberate on the following:

1. Security strategy and policy establishment
2. Main issues related to security regulations
3. Evaluation and handling of a security violator
4. Analysis of security evaluation, and items that require adjustment and discussions in security performance
5. Other items required by the chairperson

③ A decision shall require a majority vote of the attendees who make up the majority of all the incumbent members, and a tie shall mean a vote down.

Article 8 (Working-level Security Meeting) ① To effectively execute, adjust and agree on the working-level meeting, a Working-level Security Meeting (hereinafter referred to as Meeting) shall be comprised as follows:

1. The Meeting shall be composed of the heads of representative working-level departments of each security job, and the secretary shall be the person in charge from the working-level security department that called the Meeting.

2. The Meeting shall be called by notifying items and contents for discussion via an official document by a working-level department which has items to discuss seven days in advance.

② The Meeting shall discuss the following:

1. Working-level items related to security scope
2. Items related to establishing and executing the security budget
3. Security-related regulations
4. Discussion on a management plan for hardware, software, physical security, etc. when outsourcing
5. Other attendant items of the above.

Article 9 (Working-level Security Department) ① A Working-level security department shall be established to act as a security-related working-level department and to adjust and support the security activities of a unit group.

② The Working-level security department shall be under fellow officers in charge of security, and shall perform jobs with independence and continuity.

③ The Working-level security department shall perform the following:

1. Executing security plans and establishing a budget
2. Managing security-related regulations
3. Operating and managing security system
4. Danger evaluation and security inspection activities
5. Executing security education and training
6. Working-level window for external security
7. Other attendant items related to security

Article 10 (Establishment and Implementation of the Regulation) The implementation of the Regulations on Security and details needed for security activities shall be stipulated separately.

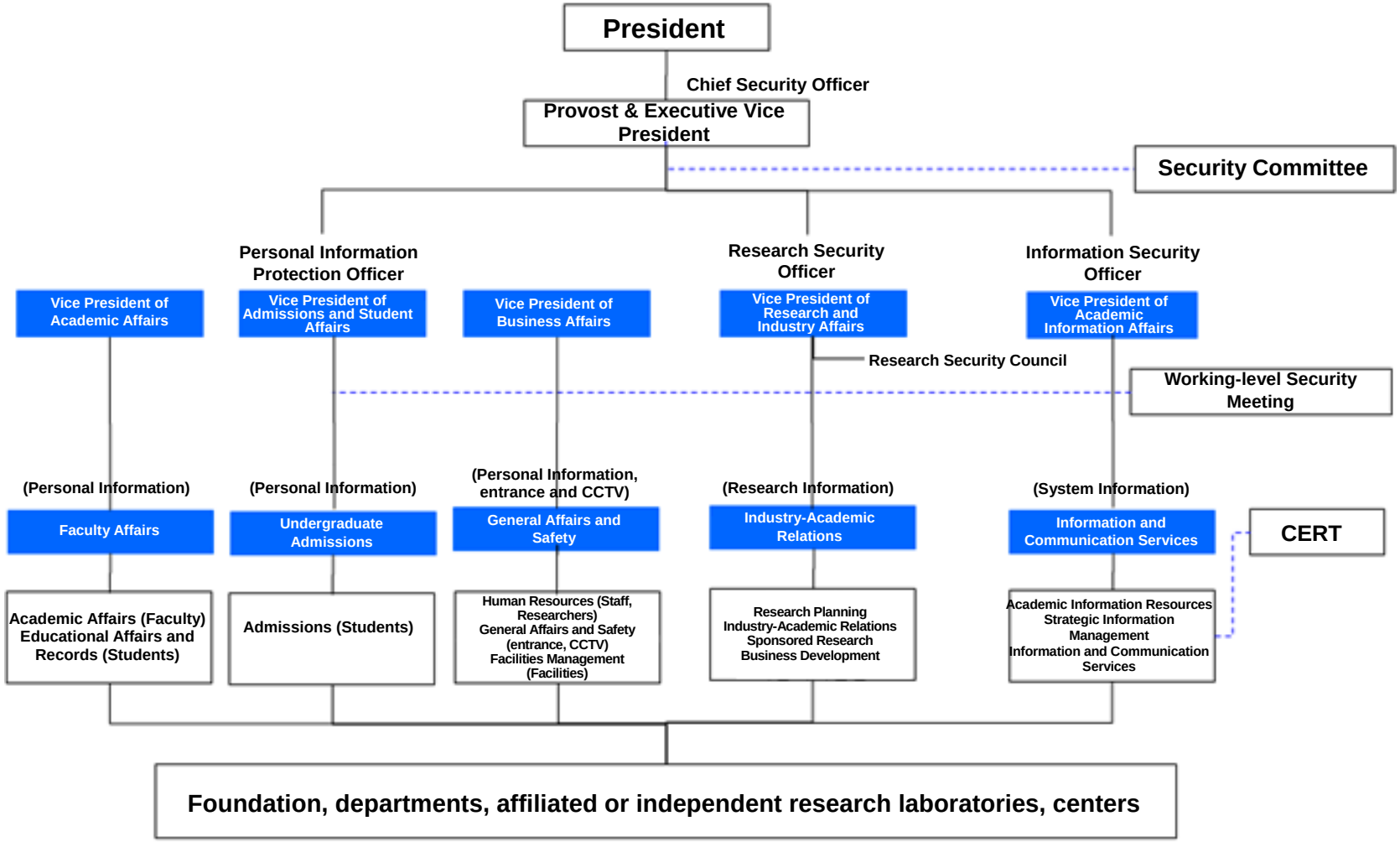
Article 11 (Restriction Process) Restrictions may be placed if the University's information assets have been violated by unauthorized internal or external users, and the details thereof shall be specified separately.

Addenda

1. The present regulation shall be established and take effect as of November 28, 2012.
2. The Information Protection Regulation established and enforced prior to the present regulation shall be abolished on the establishment date of the present regulation as is integrated thereto.

(Attachment 1) Structure of Security Organization

University Security Organization



(Attachment 2) Security Committee

Security Committee

No.	Classification	Position	Comment
1	Chairperson	Provost & Executive Vice President	
2	Member	Vice President of Planning	
3	Member	Vice President of Academic Affairs	Personal Information Protection Officer
4	Member	Vice President of Admissions and Student Affairs	Personal Information Protection Officer
5	Member	Vice President of Research Affairs	Research Security Officer
6	Member	Vice President of Academic Information Affairs	Information Security Officer
7	Member	Vice President of External Relations and Communications	
8	Member	Vice President of Business Affairs	Personal Information Protection Officer
9	Secretary	Head of Working-level security department	