Detailed Rules on General Security

Established November 28, 2012

Chapter 1 General Provisions

Article 1 (Purpose) The purpose of these regulations is to establish detailed matters necessary for the general security management of Pohang University of Science and Technology (hereinafter referred to as the "University") in accordance with the Regulations on Security of the University as well as the Regulations on Security and the Detailed Rules on the Enforcement of the Regulation on Security set forth by the government.

Chapter 2 Personnel Security

Article 2 (Definition) The terms shall have the following meanings:

1. "Confidential information" refers to classified government information, the leakage of which may cause harmful consequences to the assurance of national security according to relevant statutes of the government, or secret information that concerns the existence of the University and is classified under the Detailed Rules herein.
2. "External personnel" refers to all personnel other than members of the University, and can be categorized into outsourced service personnel, external research participation personnel, personnel hired by consigned stores and other external personnel depending on their use of the University's information assets.
3. "Contract staff members" refer to those other than permanent employees who are hired out of the University's necessity for a certain period.

Article 3 (Basic Security Duties of Members of the University) Members of the University must comply with each of the following security standards upon their employment as members of the University until they are removed from office or retired:

1. A person hired as a member of the University must submit to the competent department related to human resources the Information Protection Pledge (the attached Form 1) in which compliance with Regulations on Security and relevant statutes of the University are stipulated.
2. A person working as a member of the University must support security check activities and regularly receive trainings on security and response procedures for security accidents, etc.
3. A person removed from office or retired from the University must observe legal and moral duties suggested by the University's information protection activities.
4. Personnel security concerning researchers performing research projects among members of the University shall be separately established in the Detailed Rules on Research Security Management.

Article 4 (Background Check) ① A person subject to a background check shall be as follows:

1. Prospective University staff members
2. Prospective personnel authorized to handle confidential information
3. Other persons recognized as required for security reasons

② Background checks shall be performed by the competent department related to human resources, and the department shall perform a background check when requested in accordance with relevant legislation of the University.

③ The background check report must be managed along with personnel records of the relevant person.

Article 5 (Management of Contract Staff Members) ① In principle, background check of persons engaged in special fields among contract staff members (e.g., persons performing confidential tasks, persons working in restricted areas, and security guards) and other persons requiring a background check shall be performed before appointment.

② In principle, confidential information shall not be authorized to be handled by contract staff members. If an approval to handle confidential information is required, authorization may be granted after a review at a Working-Level Security Meeting.

③ Responsibility of supervising contract staff members shall lie in the person who holds the power to appoint and dismiss, the head of relevant unit organization, and the person in charge of the relevant job.

Article 6 (Security Measures Concerning the Appointment of Foreign Nationals) ① When signing an employment contract with a foreign national for business consultation or other purposes, a background check must be requested 30 days prior to the date of appointment and the appointment of a foreign national with suspicious background shall be determined after a review at a Working-Level Security Meeting.

② When signing an employment contract with a foreign national to be hired by a unit organization, the Chief Security Officer shall supervise to ensure that the contract includes security precautions, such as liability for damages caused by the disclosure of confidential information obtained during the employment or after the contract period, and setting of the employee's job limit.

③ When a foreign employee retires, the Chief Security Officer shall prepare an Information Protection Pledge form, which sets forth the prohibition on the disclosure and/or personal use of such important materials as confidential information obtained during employment at the University, and determine whether any types of such materials were removed from the University without due notice.

Article 7 (Authorization of Confidential Information and Revocation Thereof) A person handling confidential information defined in the Detailed Rules on Document Security shall comply with each of the following process for safe-keeping of confidential information:

1. The President, the Chief Security Officer, the Information Security Manager and other persons performing information security tasks shall be the subject to security clearance.
2. The statement of reasons of security clearance, the Information Protection Pledge, four copies of identity statement, two certified copies of the family register and six copies of photos (2 cm x 2.5 cm) shall be submitted when requesting security clearance.
3. If a person who has been authorized to handle confidential information is assigned to a different position or retires, the person must immediately return his or her security clearance card to the competent department related to human resources.
4. When an authorized person has lost his or her security clearance card, the person must submit an explanatory statement of the loss to the competent department related to human resources without delay and request re-issuance along with a written pledge stating that the person shall take full responsibility for any repercussions related to the loss.

Article 8 (Security Management Concerning External Personnel) Unit organization of the University must carry out each of the following personnel security activities with regards to external personnel contracted out of necessity:

1. When signing a contract with external personnel, the contract must include matters concerning security and/or internal control, emergency measures, ownership, security education requirements, security violation conditions and the Information Protection Pledge, in addition to general contract matters. Other necessary security requirements must be added depending on the type of other external personnel or outsourcing contracts.

2. Appropriate access control and security management must be carried out in accordance with the Detailed Rules on Information Security and the Guidelines on the Management of Accounts and Passwords when external personnel need access to internal information assets of the University.
3. If external personnel are stationed at the University to perform a project, a separate work area shall be provided, in principle, to the external personnel to prevent any information leakage.
4. External personnel must attend regular security training sessions held by the University and security check activities of the University.

Chapter 3 Document Security

Article 9 (Definition) The terms used herein shall have the following meanings:

1. "Confidential document" refers to a classified government document that may cause harmful consequences to the assurance of national security according to relevant statues or a classified document designated as such by the University.
2. "Internal Use Only" refers to a document that does not constitute confidential information yet still requires special protection for the purpose of conducting the business of the University.
3. "Electronic document" refers to a document which is not in general paper form, but is electronically composed, transmitted, received or saved by a device capable of data processing, such as a computer.

Article 10 (Classification Criteria) ① All documents of the University as defined in the Detailed Rules on the Classification and Management of Information Assets shall be classified to the following security levels:

1. Public Use
2. Internal Use Only
3. Confidential
4. Strictly Confidential

② "Public Use" document refers to a document that may not have any effect on privacy issues or the conduct of research and business activities of the University even if it is leaked or damaged.

③ "Internal Use Only" document refers to a document of which leakage is restricted, and which can affect the conduct of research and business activities and/or the public image of the University if it is leaked or damaged. The internal use only document includes the following:

1. Mid- to long-term management plan, policy making and management documents of the University before public disclosure
2. Research projects or research records classified as Temporary Restriction (Level B) or higher among confidential research projects
3. Academic information including student grades, etc. and personal information of University's staff members
4. Minutes of committee meetings or other work-related meetings before public disclosure
5. Various documents related to project-equivalent works
6. Documents designated by the Chief Security Officer, etc.

④ "Confidential" document refers to a document of which leakage is restricted, and a document whose leakage or damage may seriously compromise the management of the University, or a classified government document defined under the relevant statutes. The confidential document includes the following:

1. Level II or lower confidential documents as defined in the relevant statutes
2. Document manuals containing nationally valuable information or research presentation plans requiring reports

3. Documents designated as confidential by the President or the Security Committee, etc.

⑤ Access to “Strictly Confidential” document is highly restricted. It refers to a document whose leakage or damage can severely affect the existence of the University or a document that requires strictly confidential treatment under University’s policies.

Article 11 (Basic Document Security) The management of security documents classified according to Article 10 must be in accordance with each of the following security standards:

메모 **[Office1]:** 10조에서 보안 등급을 정의 내리므로, 11조에서 10조로 수정합니다.

1. Internal use only document must be prohibited access by outsiders and leakage to the outside in accordance with the process prescribed in Article 13, and be regularly checked to prevent falsification. In the case of transmission, it must be encrypted and managed by the relevant person in charge.
2. Confidential document must be managed only by the authorized personnel according to the process as prescribed in Article 14. If the retention period of a document expires, the document must be safely destroyed.
3. Any internal and external access to strictly confidential documents shall be strictly prohibited. They shall be encrypted, and file transmission, including via e-mail, shall not be permitted. The original file shall not be stored in a computer nor in a portable storage device. The strictly confidential document must be managed in such a manner that only the management of the University can view it.

Article 12 (Protection of Internal Use Only Documents) The internal use only document shall be deemed to be confidential information. Internal use only document management register shall be kept and managed as follows:

1. The unit organization creating, saving and using internal use only documents shall keep an internal use only document incoming/outgoing register, apart from general documents, and assign disparate receiving and sending identification numbers.
2. In the case of publishing an internal use only document, it shall be published with cooperation of the Chief Information Protection Officer in accordance with the case of publishing confidential documents.
3. Internal use only documents with expired protection period shall be processed as follows:
   A. Cross out the title page of the internal use only document when re-classifying it into a general document, and save the document according to the document storage and preservation method.
   B. Documents determined to be destroyed shall be deemed to be confidential documents and, thus, incinerated.
   C. An internal use only document without a title page stating the protection period shall be processed after an inquiry to where it was produced. If such information is not available, the document shall be re-classified as a general document or destroyed after getting an internal approval from the head of the relevant unit organization.
4. An internal use only documents shall be deemed to be confidential and, thus, stored in a confidential information storage box, not to be stored together with general documents.
5. The current status of the possession of internal use only documents shall be notified to the head of a department dedicated to information protection during a regular security audit, and the submission form shall follow the Report on the Current Status of the Possession of Confidential Documents.
6. When creating an internal use only document, the protection period shall be stated and classified as follows:

Internal Use Only	1.0 cm
MM. DD, YYYY. General Document, Destruction	0.5 cm

<---------- 5 cm ---------->

A. Circle “General Document” for internal use only documents that are no longer effective as such after its protection period and can be re-classified as a general document.
B. Circle “Destruction” for internal use only documents that must continue to be classified as internal use only even after the protection period but will be destroyed since they no longer need to be stored.

Article 13 (Protection of Confidential Information) Protection of confidential information shall be performed as follows:

1. The handling, classifying and re-classifying of confidential information shall follow relevant statutes.
2. The competent department for document regulations shall be in charge of managing incoming and outgoing confidential documents, and persons with security clearance shall be assigned to the task among those who work at the competent department.
3. The competent department for Regulations on Documentation shall be in charge of storing confidential information and, in principle, shall perform centralized storage and management.
4. In principle, a confidential information storage container shall be a steel-made, double-layered cabinet and must have a double combination lock.
5. The head of the working-level department for confidential information storage shall be the principle person responsible for storing confidential information, and the person in charge of security shall be the secondary responsible person. Provided that, if the storage of confidential information is distributed at multiple locations, the department head responsible for the storing unit shall be the principal responsible person and must appoint a separate secondary responsible person.
6. Transferring confidential information shall be completed by two main lines below the final line of the Confidential Information Management Register and by filling out the following transference information:

Transference of Confidential Information
Urgent Confidential Case
has been duly transferred as above.
MM. DD, YYYY

Sent by	Position	Name	(Seal)
Received by	Position	Name	(Seal)
Confirmed by	Chief Information Protection Officer	Name	(Seal)

7. All persons wishing to view confidential information must fill out relevant information in the Confidential Information Viewing Register and sign or seal on it before viewing the document. The same process applies for the approval of a confidential document.
8. The Chief Security Officer must establish safe confidential document transfer and destruction plan to thoroughly maintain and manage the security of confidential information during emergency.
9. The Chief Security Officer must investigate the current status of personnel authorized to handle confidential information and confidential information in possession as of the last day of June and December every year, and notify the Officer in charge of security affairs at the Ministry of Education

using a separate relevant form by July 10 of that year and January 10 of the following year.

10. The format of the title page of a confidential document shall comply with that specified under relevant statutes.

Chapter 4 Facility Security

Section 1 Security for General Facilities

Article 14 (Definition) The terms used herein shall have the following meanings:

1. "Data processing room" refers to an area where various types of information assets and supplementary equipment are exclusively operated, and may include a control room and a machinery room.
2. "Entrance control system" refers to a device that automatically controls entry to and exit from an area that requires security.

Article 15 (Responsibility for Facility Security) The head of the competent department for facility security shall be in charge of overall facility security of the University, and the head of the department or affiliated center concerned shall be in charge of each unit organization.

Article 16 (Designation of Protected Areas) ① Protected Areas of the University shall be categorized as follows:

1. Restricted region: Entire area of the University and affiliated centers
2. Restricted area: The President's office, offices of persons with assigned positions, research laboratories, operating rooms, boiler rooms, broadcasting studios, data processing rooms, substations, and research centers related to advanced industries
3. Controlled area: areas of extremely high security importance where access by unauthorized persons is prohibited.

② For designated protected areas, relevant information must be recorded and kept in the Protected Area Register in accordance with a separate relevant format.

Article 17 (Management of Protected Areas) ① Persons other than relevant personnel and authorized persons must be prohibited from entering controlled areas, and an entrance roster must be recorded and kept in accordance with a separate, relevant format.

② The following sign must be placed at the top center of the entrance of restricted and controlled areas. However, the sign may be omitted for the President's office, offices of persons with assigned positions, research laboratories, etc.

Restricted Area	Controlled Area

15 × 30cm

③ The following sign stating the person in charge must be positioned at an appropriate place in the protected areas.

Person in charge	
Primary	
Secondary	

100 mm

150 mm

Article 18 (Managing Responsibility for Protected Areas) ① The persons in charge of managing

protected areas are as follows:

1. Restricted region
   A. The President's office, offices of persons with assigned positions: secretary
   B. Research laboratories: Principal professor of each research laboratory
   C. Administrative office: the head of the department concerned
   D. Operating rooms, boiler rooms, data processing rooms, substations, underground common areas: the head of a department responsible for managing such facility
   E. Research centers related to advanced industries: the head of an affiliated center responsible for managing such facility
2. Controlled area: the head of a department managing such facility

② The person in charge of managing protected areas must designate a secondary responsible person among the personnel in the same department.

③ The person in charge of managing protected areas must ensure thorough management of protected areas by performing self-inspection at least once a month to identify management issues and vulnerable points, and establish measures accordingly.

Article 19 (Access Restriction) ① Access to facilities within protected areas shall be permitted only to authorized persons with a smart card.

② Entrance to facilities for work purposes by those who do not have regular Access ID cards, such as external personnel's temporary access, shall be permitted only if accompanied by persons who are authorized to access the facilities.

③ External personnel authorized for temporary entrance must wear a temporary entrance pass when entering protected areas.

④ A person whose smart card has been lost or stolen must report such matter immediately to the competent department in charge of managing and operating the smart card system and have it re-issued.

⑤ The competent department responsible for managing and operating the smart card system must maintain information of a person's entry to and exit from protection areas for at least 3 months.

⑥ An unauthorized person's illegal access to or attempt to access an protection area must be reported upon detection to the person in charge at the competent department for facility security or the security guard.

Article 20 (Security for Central Data Processing Room) ① In principle, access to the Central Data Processing Room shall be limited to authorized University members who have been issued entrance cards. If other persons need access due to works related to the Central Data Processing Room, they must access after obtaining an approval from the head of the competent department for facility security.

② The entrance control system must be installed and operated to keep a record on persons entering and exiting, and to control and manage the Central Data Processing Room.

③ Excessive ornament on the outside of the Central Data Processing Room shall be avoided, and external and internal signs indicating the functions and purpose of the facilities (data processing rooms, machinery rooms, etc.) shall be minimized.

④ The Central Data Processing Room must be equipped with facilities to prevent disasters.

Article 21 (Protection of Offices and Laboratories) The last person to leave an office or a research laboratory must check each of the following:

1. Whether cabinets, desks, entrance doors, etc. have been locked
2. Whether office appliances (computers, printers, photocopiers, etc.) and electric heaters have been turned off
3. Whether the lights have been turned off

4. Whether the security record has been filled out
5. All other security measures

Section 2 Security for Entrance Control System

Article 22 (Definition) The terms used herein shall have the following meanings:

1. "Entrance control system" refers to a control device installed at the entrance of a building, and is categorized into an RF entrance controller and a fingerprint reader. It permits or rejects entrance after checking the identity of a person via the smart card.
2. "Smart card" refers to an identity card (including a mobile card) of the University member produced for the purpose of permitting entrance, checking attendance, electronic payment, etc.
3. "Department in possession of entrance control system" refers to a department where the entrance control system is installed.
4. "Department in charge of general management of entrance control system" refers to the department that oversees general matters concerning the entrance control system.

Article 23 (Roles and Responsibilities) ① The head of department for general safety management shall be the Chief Entrance Control System Officer and shall perform each of the following roles as the person responsible for controlling entrance to the University:

1. Manage the current status of the installation and operation of the entrance control system
2. Establish requirements and procedures for managing the commissioned entrance control system
3. Manage general security matters of companies to which the entrance control system has been commissioned
4. Issue smart cards for the entrance control system and run training programs/sessions for proper use thereof
5. Other tasks necessary to protect entrants

② The head of department in possession of entrance control system shall be the person responsible for operating the entrance control system. Duties and responsibilities include instructing and supervising the person in charge of system management at the department in possession of entrance control system concerning his or her tasks related to the protection of entrance information, analyzing access logs from the entrance control system, and preventing accidents caused by improper use.

③ The person in charge of system management at the department in possession of entrance control system shall be the person handling entrance information for work purposes. He/she must devise necessary measures to ensure the safety of such entrance information so that it is not lost, stolen, leaked, falsified or damaged.

Article 24 (Prior Notification) The unit organization (department or academic department) wishing to install the entrance control system must notify the Chief Entrance Control System Officer of its installation plan after prior discussion.

Article 25 (Notice Installation) ① The head of department in possession of entrance control system may put up a notice at the entrance stating that the entire building is an entrance control system-installed area in case multiple entrance control systems are installed within the building.

② When installing an entrance control system, the head of department in possession of entrance control system must carry out necessary actions such as installing a notice stating the following information so that it can be easily recognized by the subject of information:

1. Usage guide and method
2. Entrance scope and time

3. Contact information of the department in charge and the person in charge

Article 26 (Collection Restriction) ① When collecting entrance information via the entrance control system, the system must not be arbitrarily manipulated exceeding the scope of the installation purpose.

② When collecting entrance information via the entrance control system, the information must not be copied or taken outside.

A**rticle 27 (Keeping an Entrance Control System Possession Register)** The head of department in possession of entrance control system shall fill out the Entrance Control System Possession Register (attached Form 2) so that the subject of the information may view it when a change occurs to the entrance control system.

Article 28 (Processing Limit) The head of the department in possession of entrance control system must restrict the viewing or supply of entrance information to the minimum extent that falls within the purpose of possessing entrance information. Provided that, the concerned entrance information may be viewed or supplied for a purpose other than that of possession if it applies to any of the following:

1. When the subject of information agrees
2. When information is viewed by or supplied to the subject of information
3. When there is a special regulation(s) set forth in the relevant statutes
4. When information is provided for safety purposes, such as crime prevention, facility safety, and fire prevention
5. When it is needed in the proceedings of a court trial
6. Other cases when acknowledged as necessary at a Working-Level Security Meeting

Article 29 (Viewing and Providing Entrance Information) ① A person wishing to view or receive entrance information must fill out the Entrance Information Viewing Application Form (attached Form 4) and submit it to the head of department in possession of entrance control system.

② For an organization wishing to view or receive entrance information, the organization must submit to the head of department in possession of entrance control system an official written request specifying the purpose of viewing and the range of entrance information.

③ When the head of department in possession of entrance control system allows an organization to view or receive entrance information, a record must be kept and managed in the Entrance Information Viewing/Providing Register (attached Form 3).

Article 30 (Commissioning of Installation and Management of Entrance Control System) ① The head of department in possession of entrance control system may commission installation and management of the entrance control system to a professional entity which meets the following requirements after discussing with the Chief Entrance Control System Officer:

1. Possesses professional equipment and technology necessary for protecting entrance information
2. Possesses professional personnel to perform commissioned work

② The head of department in possession of entrance control system who intends to commission the installation and management of an entrance control system must decide detailed matters necessary to protection of entrance information, such as the range of work to be commissioned, access restriction to entrance information, etc., and keep a record in relevant documents such as a commissioning agreement, etc.

③ In the case the work is commissioned, the name of the commissioned entity, the person in charge and contact information must be included in the notice.

Article 31 (Retention and Storage Period) ① In principle, documentation on the entrance information shall be limited to protection areas of the University in accordance with the relevant statutes.

② Entrance information collected by the entrance control system shall be stored up to 30 days from the

day of collection.

Article 32 (Confidentiality Obligation) A person who processes or used to process entrance information must not use it for unjustified purposes, such as leaking entrance information learned while on duty, processing it without duly granted authority or providing it for a third party's use.

Section 3 CCTV Security

Article 33 (Definitions) The terms used herein shall have the following meanings:

1. "CCTV" refers to a system that collects image information with a filming device installed at a predetermined space and transmits such information only to particular recipients via closed wired or wireless transmission lines.
2. "Image information" refers to information that can confirm the identity of the concerned individual with the image filmed by the CCTV.
3. "Processing" refers to the handling of image information other than collection, such as inputting, saving, transmitting, editing, deleting, playing of image information collected by the CCTV and other similar actions.
4. "Subject of Information" refers to a person who can be identified with image information and who is the subject of the concerned image information.
5. "Department in possession of image information" refers to a department that possesses image information.
6. "Department in charge of general management of image information" refers to the department that oversees general affairs concerning the protection of image information.

Article 34 (Application Scope) ① CCTV installed and operated at the University to serve public interest, such as crime prevention, securing of evidence, facility safety and fire prevention, and protection of image information collected and processed shall be in compliance with the present internal regulations as specified herein, except for cases in which a special regulation(s) exists under relevant statutes.

② In the cases of installing a fake camera in place of CCTV installed and operated by the University, the present internal regulations shall apply regardless of whether real image information is handled.

Article 35 (Roles and Responsibilities) ① The head of the department in charge of general management of image information shall be the person responsible for the CCTV and shall perform the following roles as the person responsible for protecting image information of the University:

1. Manage the current status of the installation and operation of CCTV
2. Establish requirements and procedures for managing commissioned CCTV
3. Manage the general security of the company to which CCTV has been commissioned
4. Provide education programs/session on image information protection
5. Other tasks necessary to protect image information

② The head of department in possession of image information shall be the person responsible for operating the CCTV. Duties and responsibilities include instructing and supervising the person in charge of handling image information concerning his or her tasks related to the protection of image information, analyzing access logs from the image information system, and preventing accidents caused by improper use.

③ The person in charge of operating CCTV shall be the person handling entrance information for work purposes and must devise measures necessary to ensure the safety of such image information so that it is not lost, stolen, leaked, falsified or damaged.

Article 36 (Restrictions on Installation/Operation of Image Information Processing Equipment) ①

Image information processing equipment must not be installed/operated at public places in the University except for the following cases:

1. When it is specifically allowed by the relevant statutes
2. When it is necessary for crime prevention and investigation purposes
3. When it is necessary for facility safety and fire prevention purposes

Article 37 (Prior Notification) The department (or academic department) wishing to install CCTV must notify the head of the department in charge of general management of image information of its installation plan after prior discussion.

Article 38 (Installation of Notice) ① The head of department in possession of image information may put up a notice at the entrance stating that the entire building is a CCTV-installed area in case multiple CCTVs are installed within the building.

② When installing CCTV, the head of department in possession of image information shall carry out necessary actions such as installing a notice stating the following information so that it can be easily recognized by the subject of information:

1. Purpose and location of installation
2. Filming range and time
3. Department in charge and contact information
4. Person in charge and contact information

Article 39 (Commissioning of CCTV Installation and Management) ① The head of department in possession of image information may commission CCTV installation and management to a professional entity which meets the following requirements:

1. Has professional equipment and technology necessary for protecting image information
2. Has professional personnel to perform commissioned work

② The head of department in possession of image information who intends to commission CCTV installation and management must decide the details necessary to protect image information, such as the range of work to be commissioned and access restriction to image information, and keep a record of such matters in relevant documents including a commissioning agreement.

③ When the work is commissioned, the name of the commissioned organization, the person in charge, and contact information must be stated in the notice.

Article 40 (Restriction of Collection) ① When collecting image information via CCTV, the camera must not be arbitrarily manipulated exceeding the scope of the installation purpose.

② When collecting image information via CCTV, the sound recording function must not be used.

Article 41 (Keeping an Image Information Register) The head of the department in possession of image information shall fill out the Image Information Register (attached Form 2) when generating image information so that the subject of the information may view.

Article 42 (Processing Limit) The head of the department in possession of image information must ensure that such information is not used for purposes other than that of possession as well as that only authorized persons are allowed to view or receive such information. Provided that, the concerned image information may be viewed or supplied for a purpose other than that of possession if it applies to any of the following:

1. When the subject of information agrees
2. When information is viewed or provided to the subject of information
3. When there is a special regulation(s) set forth in the relevant statutes
4. When information is needed for the purpose of media reports, such as newspapers and broadcasting, and provided in a way that particular individuals cannot be identified
5. When it is need to investigate crime, prosecute a case or sustain a public prosecution

6. When it is needed in the proceedings of a court trial
7. Other cases including when it is acknowledged as necessary at a Working-Level Security Meeting

Article 43 (Viewing, Providing, and Deleting Image Information) ① An organization wishing to view or receive image information must submit to the head of department in possession of image information an official written request specifying the purpose of viewing and the range of image information that is to be viewed.

② The subject of information who wishes to view or delete image information may submit the Image Information Viewing/Deletion Application Form (attached Form 7) to the head of the department in possession of image information. Provided that, such request may be rejected for any one of the following cases:

1. When the image information has been destroyed or deleted because its retention period has expired
2. When it significantly obstructs criminal investigations, sustainment of public prosecutions or trial proceedings
3. When there exist significant technical difficulties in deleting only the image information of a particular subject of information
4. When it raises substantial privacy concerns for taking necessary measures to make a request pursuant to paragraph 1
5. When there exist other justifiable public reasons to reject a request for viewing, etc.

③ When the head of department in possession of image information allows image information to be viewed or deleted in response to a request made pursuant to paragraphs 1 and 2, a record must be kept and managed in the Image Information Register (attached Form 6).

Article 44 (Retention and Deletion) In principle, image information collected by CCTV shall be deleted within 30 days of collection. Provided that, except for cases where the retention period is stipulated in the relevant statues or where there is a special purpose(s).

Article 45 (Confidentiality Obligation) A person who processes or used to process image information must not use it for unjustified purposes, such as leaking image information learned while on duty, processing it without duly granted authority, or providing it for a third party's use.

Addenda

1. These detailed rules herein shall be established and take effect on November 28, 2012.
2. Matters implemented prior to the effective date of the detailed rules herein shall be deemed to have been implemented by these detailed rules.
3. Detailed Rules on Personnel Security, Detailed Rules of Document Security and Detailed Rules on Facility Security prior to the establishment and effective date of the present detailed rules shall be abrogated and integrated thereto as of the establishment date of the present detailed rules.

(Attachment 1) Information Protection Pledge

Information Security Pledge

Name:
Resident Registration No.:

I hereby pledge to have full knowledge of the Regulations on Security and relevant detailed rules of POSTECH (hereinafter referred to as the University), and to faithfully comply therewith.

1. Information Protection Compliance Items during Employment
   ① I shall use the information obtained from the University or all information obtained in relation to works concerning the University only for business reasons serving the establishment purpose of the University.
   ② I shall not violate an agreement or duties whereby exclusive information of a former employer, another external organization or an individual is to be kept confidential even when working as a member of the University. I shall not use their exclusive information without a written letter of delegation from the former employer, other company or the individual when working for the University.
   ③ I shall do my best to carefully use and store media on which information is recorded such as various documents, photographs, magnetic tapes, computation equipment, etc. so that undue falsification, copying, damage, missing, destruction, leakage of a confidential information, etc., can be prevented.
   ④ I shall not leak important operational matters, information, research results, etc., of the University obtained while on duty or during various research processes, meetings, seminars, etc.
   ⑤ I shall not access information or facilities unauthorized to access while on duty. Nor shall I use data storage/processing facilities possessed by the University to serve its establishment for anything other than work purposes. In addition, I shall not store personal information within such facility.
   ⑥ I shall not use information assets provided by the University for purposes other than business objectives of the University. Nor shall I leak the information assets of the University to the outside without the University's permission.
   ⑦ I shall comply with the Information Protection Regulations and Detailed Rules thereof for generating, using and destroying documents related to business of the University.
   ⑧ I agree and pledge to comply with the regulations set forth in the University's Information Protection Regulations and Detailed Rules thereof for all other matters.

2. Information Protection Compliance upon Retirement
   ① I shall immediately return all information assets belonging to the University upon retirement.
   ② I pledge not to possess or have saved University's confidential information or information assets anywhere by any method.
   ③ I shall not reveal any important confidential information of the University (including data related to its operation, research results, etc.) obtained during employment to any other external personnel inside or outside the University who are not involved in the transfer of duties and responsibilities even after retirement.
   ④ I shall not reveal or use confidential information on the University for other external personnel for three years after retirement.
   ⑤ I shall not only actively cooperate with the University's efforts to protect confidential information but

also faithfully observe legal and moral obligations pertaining thereto.

I hereby pledge that I shall have thorough knowledge of the above and faithfully comply therewith and shall bear all responsibilities according to relevant statutes and regulations of the University in case I have violated the above.

Date: Name: (seal)

Chairperson of Security Committee of Pohang University of Science and Technology

(Attachment) Entrance Control System Possession Register

Entrance Control System Possession Register (Existing/Changed)

(1) Department Name	
(2) Installed Location	
(3) Function	
(4) No. of Installed Systems	
(5) Installation (Change) Date	
(6) Commissioned Entity	
(7) Scope	
(8) Operating Time	
(9) Notice Location	
(10) Purpose of Installation	
(11) Storage Media	
(12) Retention Period	
(13) Deletion Method	

(Attachment 3) Entrance Information Viewing/Providing Register

Entrance Information Viewing/Providing Register

(1) Entrance Information Name	
(2) Viewing/Providing Organization	
(3) Viewing/Providing Date	
(4) Viewing/Providing Cycle	
(5) Viewing/Providing Format	
(6) Viewing/Providing Period	
(7) Viewing/Providing Purpose	
(8) Viewing/Providing Rationale	
(9) Viewing/Providing Request Date	
(10) Notes	

(Attachment 4) Entrance Information Viewing Application Form

Entrance Information Viewing Application Form

(1) Applicant	Name		Telephone No.	
	Date of Birth		Department	
	E-mail			
(2) Viewing Details	Installed Location			
	Requested Date			
	Content			
(3) Department in Possession of Entrance Information (To be filled out by person in charge)	Department			
	Name of Person in Charge			
	Signature of Person in Charge			

Month Date Year

Applicant: (Signature or seal)

(Attachment 5) Image Information Register

Image Information Register

(1) Department in Possession of Image Information			
(2) Installed Location			
(3) Function	Voice Recording	Zoom-in	Rotation
	(Yes/No)	(Yes/No)	(Yes/No)
(4) No. of Installed Devices			
(5) Installation Date			
(6) Commissioned Entity			
(7) Filming Range			
(8) Filming Time			
(9) Notice Location			
(10) Purpose of Installation			
(11) Storage Media			
(12) Retention Period			
(13) Deletion Method			

(Attachment 6) Image Information Management Register

Image Information Management Register

No.	Classification	Date	File Name /Type	Person in Charge	Purpose/ Reason	Requester	Reason for Use/Supply	Use/Supply Format	Period
1	□ Used □ Supplied □ Viewed □ Destroyed								
2	□ Used □ Supplied □ Viewed □ Destroyed								
3	□ Used □ Supplied □ Viewed □ Destroyed								
4	□ Used □ Supplied □ Viewed □ Destroyed								
5	□ Used □ Supplied □ Viewed □ Destroyed								
6	□ Used □ Supplied □ Viewed □ Destroyed								
7	□ Used □ Supplied □ Viewed								

	□ Destroyed								

(Attachment 7) Image Information Viewing/Deletion Request Form

Image Information (Viewing [ ] , Deletion [ ]) Request Form

Applicant	Name		Telephone No.	
	Date of Birth		Relation to the Subject of Information	
	Address/ E-mail			
Subject of Information	Name		Telephone No.	
	Date of Birth			
	Address/ E-mail			
Request Detail (Please be specific; otherwise, request may not be processed)	Information Record Period of Requested Image	Date: From (Time :) To (Time :)		
	Installed Location of Image Information Processing Equipment			
	Purpose/ Reason for Request			
I hereby request confirmation of the existence of personal image information and viewing thereof pursuant to Article 52 of the Standard Guidelines on Personal Information Protection.				
Date: Applicant: (Signature or Seal)				
Department in Possession of Image Information	Department Name			
	Name and Signature of	(Signature or Seal)		

	Person in Charge	