Detailed Rules on Information Security

Established November 28, 2012
Amended February 18, 2013

Chapter 1 General Provisions

Article 1 (Purpose) The purpose of these Detailed Rules is to set forth detailed matters needed for information security activities of Pohang University of Science and Technology (hereinafter referred to as the "University") and efficient implementation of information security tasks in accordance with the Regulations on Security of the University.

Article 2 (Roles and Responsibilities) ① The information security officer must put in place an information security administrative department and information security administrative staff to efficiently perform information security tasks of the University.

② The information security administrative department shall perform each of the following roles as the department overseeing information security tasks of the University:

1. Implement information security plan and establish a budget
2. Manage regulations related to information security
3. Operate and manage the information security system
4. Perform information security risk assessment and conduct information security audit
5. Educate on information security and provide training thereon
6. Be the administrative window for external information security duties
7. All other matters related to information security

③ The information security administrative staff in charge of information security administration shall include information security manager, information security staff, information security division manager and information security division staff, and they shall perform each of the following roles:

1. The head of the information security administrative department shall be the information security manager and perform roles, such as managing and supervising administrative jobs for information security of the University and reporting major issues related to information security to the information security officer.
2. Information security staff shall handle administrative jobs of information security after receiving orders from the head of the information security administrative department, and perform roles such as implementing established information security plans.
3. The head of the unit organization shall be the information security division manager and perform roles such as managing and supervising administrative jobs of information security within its department after receiving direction and supervision from the information security officer.
4. Information security division staff shall handle administrative jobs of information security after receiving orders from the head of the unit organization, and perform administrative jobs of information security at the department where the staff works under the direction

and supervision of the information security division manager.

Article 3 (Definition) The terms used herein shall have the following meanings:

1. “Information assets” refers to information itself in a narrow sense but includes all equipment generating, processing and storing such information in a wide sense.
2. “Risk assessment” refers to calculating the degree of risk by measuring the size of the risk depending on the importance level of information assets and vulnerability level in terms of confidentiality, integrity and availability of information assets.
3. “Confidentiality” refers to the characteristics where unauthorized persons cannot use the information or where information is not revealed to unauthorized persons.
4. “Integrity” refers to the characteristics where information cannot be modified or destroyed by an unauthorized method.
5. “Availability” refers to the characteristics where an information asset is continuously accessed and used at the request of an authorized person.
6. “Risk Assessment Results Report” refers to the results evaluated according to risk levels based on the vulnerability analysis results.
7. “Vulnerability” refers to the state where there is no direct harm but there is risk of damage to information assets from outdated or inadequately applied worm/virus patches, weak password or network access settings, etc.
8. “Statement of Applicability” refers to a document stating control objects and control items that can be applied to the information protection management system of the University based on the risk assessment, risk handling procedure, and results.
9. “Risk Management Plan” refers to a report describing detailed risk management methods based on the Statement of Applicability.
10. “System” refers to a collection of regularly interacting organized hardware and software, including server, network, PC, DB, etc., performing predetermined information processing functions.
11. “System operator” refers to an operation staff appointed to operate and manage the system.
12. "Application program” refers to a program that configures a program or application software (application) produced by a member of the University or an external organization.
13. "Application system” refers to a collection of application software created for a particular job or purpose and a collection of hardware related thereto.
14. “Application system operator” refers to an operation staff appointed to operate and manage the application system.
15. “Infringement Accident” refers to cases such as data tampering, loss or malfunction of the information system or information network by offensive actions such as malware infections, hacking, service interruption, etc.
16. “POSTECH Computer Emergency Response Team (POSTECH-CERT)” refers to an organization searching causes of infringement accidents and performing response measures by going through analysis and response procedure when an infringement accident occurs within the University.
17. “Security audit” refers to the act of collecting and analyzing evidence in various ways and reporting the results of the analysis to confirm compliance of necessary security standards and procedures for information protection to be carried out.
18. “Audit evidence” refers to information saved by recording every measure taken in the

process of managing records to check whether record management has been carried out according to appropriate policies or standards.

19. “Improper matters” refer to cases implemented differently from as defined in Information Protection Policies and relevant security regulations and thus, refer to a problem that can increase security risk.

Chapter 2 Information Asset Management

Article 4 (Classification and Registration) ① Information security fellow manager shall classify information assets of the unit organization according to the Information Asset Codes and Classification System (Attachment 1) and fill out and keep the Information Asset Register (Attachment 3).

② Information security fellow manager shall record changes of the information assets such as new, replaced or destroyed ones at the Information Asset Register, and notify such changes to the information security manager within seven days.

③ Information asset classification criteria and Information Asset Register may be added or deleted depending on the types and forms of the information assets owned by the University. Such changes shall be notified to the unit organization when it occurs.

Article 5 (Importance Evaluation and Classification) ① Information security fellow manager shall fill out the Information Asset Register according to the importance evaluation and classification of information assets (Attachment 2) for information assets of the unit organization.

② Importance evaluation criteria for information assets includes confidentiality, integrity and availability, each of which are assessed from levels 1 to 3, and the importance of information assets are calculated annually.

③ Levels of importance of information assets are divided into five steps (VL, L, M, H and VH) depending on the results of the sum of importance assessment values.

Article 6 (Information Assets Management) ① The information security manager shall check the appropriateness of identification and classification of information assets submitted by a unit organization, and collectively manage the Information Asset Register.

② The information security manager shall verify the adequacy of importance evaluation of information assets submitted by a unit organization, and regularly perform vulnerability analysis and risk assessment in association with the importance evaluation.

③ Information security manager shall notify the unit organization of the analysis results after performing risk assessment to properly manage information assets of the University.

Chapter 3 Risk Assessment and Management

Article 7 (Vulnerability Assessment) ① Information security manager shall perform vulnerability assessment for information assets with high importance evaluation level in the Information Asset Register of the University.

② The information security manager shall implement vulnerability assessment for 6 fields: operating system, server, network, mock hacking, physical vulnerability and application program.

③ As a rule, vulnerability assessment for information assets shall be carried out regularly. It can be separately performed when a crucial change has occurred to the environment of the University.

④ The information security manager shall report to the information security officer after writing a Vulnerability Assessment Results Report including the following based on the results of the assessment for each information asset:

1. Information asset list
2. Importance evaluation table of information assets
3. Vulnerability assessment results

Article 8 (Risk Assessment) The information security manager shall perform risk assessment including each of the following based on the vulnerability assessment results, and report to the information security officer after composing a Risk Assessment Results Report:

1. Contents of risk assessment checklist
2. Assessment criteria for potential risk per field
3. Assessment criteria for exposure risk per field
4. Risk assessment results for each field

Article 9 (Risk Management Procedure) Information security manager shall perform the following risk managing procedures in accordance with the Risk Assessment Results Report:

1. Write a Statement of Applicability after determining acceptable risk level and identifying risks to be managed based on the Risk Assessment Results Report.
2. Compose a Risk Managing Plan in accordance with the Statement of Applicability and report to the information security officer.
3. Notify the vulnerability assessment results and the risk assessment results based on the Risk Managing Plan to the concerned unit organization.

Article 10 (Follow-up Management) The information security manager shall verify whether risk management is adequately carried out at the unit organization according to the Risk Managing Plan and report the result to the information security officer.

Chapter 4 System Security Management

Article 11 (Introduction and Installation) ① Information security fellow manager must report detailed information concerning equipment installation to the information security manager when introducing a system, and must request a security vulnerability check if it applies to any one of the following:

1. A system introduced to provide service to all members of the University
2. A system installed within the central computer room
3. Other cases determined to be necessary by the information security manager

② The information security manager must perform and notify the analysis results of the security vulnerability check, and examine the security setting environment.

③ The system operator must configure the following basic security settings when the

equipment is installed:

1. As a rule, system operation shall be performed in a console, but in case remote access is required, only the concerned IP address shall be permitted.
2. Block all IP addresses except for the terminal of the system operator or areas with security settings.
3. Block all ports except for the ones needed for the service.
4. When requesting system operation to an external organization, only the concerned IP addresses and service ports shall be permitted and a warning banner against its use for any other purpose shall be created. The concerned IP addresses and service ports shall be immediately deleted when the permitted usage period ends.

Article 12 (Operation and Management) ① As a rule, the system shall be managed by creating an account for managing the system. Root account shall be used only when necessary, and important security patches and upgrades related to security shall be frequently applied.

② The following log information must be saved for at least three months and not be arbitrarily changed to ensure evidence traceability when an infringement accident occurs:

1. Log related to system access (e.g., user account, time/date of log on/off)
2. All attempts to access data or resources
3. Log related to performing important system commands such as changing passwords
4. System event log

③ System log information must not be provided without an official request or a cooperation requested by the law, apart from when used for the job.

④ System operator must back up important data in case system recovery is impossible due to a security accident.

⑤ When the original usage of the equipment is changed, such change must be notified to the information security manager.

Article 13 (Withdrawal and Disposal) ① The information security fellow manager shall remove and separately store media such as a hard disk in which data is stored or request crushing thereof to the information security manager before withdrawing or disposing of the equipment.

② The fellow information security manager shall notify the information security manager via an email, a phone call, etc. of the withdrawal or disposal of the equipment.

Article 13-1 (Disuse of Information System's Storage Medium) ① When disusing (e.g., changing, returning, transferring or destroying) an electronic information storage medium such as a hard disk, user and system operator must take security measures so that the data recorded in the storage medium is not leaked to the outside after getting approval from the information security fellow manager.

② When the user of the information system has changed, the saved data shall be deleted by total format at least three times for the information system used in processing confidential materials and at least one time for all other information systems.

③ Detailed procedure for disusing a storage medium of an information system shall be implemented after separately consulting the asset managing department.

④ Detailed matters related to disusing an electronic information storage medium shall comply with the Ministry of Education and Science Technology's Guidelines on Disusing Process for Information System's Storage Medium (Established February 18, 2013).

Article 14 (Security Guidelines) The information security manager shall provide Security

Guidelines needed for managing and operating the system to the information security fellow manager, and application of the detailed security items shall comply therewith.

Chapter 5 Application System Security Management

Article 15 (Separation of Development Environment) As a rule, application system shall be divided into development system and operation system. In case separation is difficult, the development environment shall be configured so that it does not affect the security of the operation environment.

Article 16 (Security Function Design) ① When configuring an application program, the following security functions shall be designed considering known security vulnerabilities in the program itself or user environment from the developing stage:

1. Separate the manager module and the general user module.
2. As a rule, a user account shall be assigned per developer. Sensitive information such as a password shall not be shown on the user screen in plain text.
3. A user account of a developer generated in the application program shall have access authority and access control.
4. In case of an important application program, a user log for activities of the manager and user shall be created so that it can be used as evidence when an infringement accident occurs.

② The Software Development Security Guide set by the Minister of the Ministry of the Interior and Safety shall be complied with to secure the safety and security of the application program, and security vulnerabilities of, for example, source codes, etc., shall be checked and eliminated.

Article 17 (Operation of an Application System) ① A security vulnerability check shall be performed for an application system configured internally or by outsourcing before it is operated.

② A security vulnerability check may be requested if necessary. The information security manager shall immediately perform such security vulnerability check, notify the analysis result, and examine the security setting environment.

Article 18 (Monitoring of an Application System) ① An application system operator must continuously monitor the safety and reliability of application programs and the operation environment so that infringement accidents do not occur.

② When an infringement accident occurs, pre-actions such as promptly stopping the operation of the application system or separating the network shall be performed and then reported to the information security manager.

③ The information security manager shall notify the reasons of the infringement accident and results according to Chapter 6 Infringement Accident Response.

Article 19 (Outsourcing of Application System Development) ① When outsourcing the development of an application system, design requirements for security functions and security compliance matters concerning developers shall be stated in a Service Proposal or an Agreement.

② Risk elements for programming security of application systems shall be managed and

security control shall be performed so that the developed application programs are not leaked.
③ Security pledges shall be received from external developers participating in the application system configuration.
④ All other matters shall comply with the Detailed Rules on General Security.

메모 [PL1]: "일반보안관리세칙"="일반보안세칙(Detailed Rules on General Security)"과 동일한 것으로 간주

Chapter 6 Infringement Accident Response

Article 20 (Types of Infringement Accident) Types of infringement accidents are as follows:

1. When a part or the entire service of the information system, network, etc. is stopped due to Denial-of-Service attack (DoS), worm/virus, etc.
2. When the information system such as main services of the University is hacked and the website is modified or destroyed
3. When information is leaked by hacking a system wherein research data or confidential information of the University are saved
4. When information assets of the University attempt to attack the outside or are used as a routing point.
5. When continuous attacks from the outside are detected
6. When other information security infringement accidents occurred

Article 21 (Risk Level) Infringement Accidents shall be classified into different levels in accordance with the Infringement Accident Risk Level Table (Attachment 5) depending on the damages and its effect on the job.

Article 22 (Reporting Process) The Infringement Accident Report (Attachment 4) shall be written and submitted to the information security manager when an infringement accident occurs. Types of report are as follows:

1. When a user detects an infringement accident within the University
2. When an infringement accident is filed by an external organization
3. Other cases when an infringement accident is discovered using the security equipment

Article 23 (Infringement Accident Response) The information security manager shall respond as follows depending on the infringement accident risk level when an infringement accident is reported:

1. In case of Level 1 infringement accident, isolate the concerned system network (block IP/MAC address) and perform emergency response measures such as finding and analyzing the attack route, vulnerable points, etc., through POSTECH-CERT.
2. For Level 2 infringement accidents, isolate the concerned system network (block IP/MAC address) and notify the results after analyzing the causes and performing vulnerability check.
3. When a Level 3 infringement accident occurs, guide how the user can personally perform a check-up after isolating the concerned system network (blocking IP/MAC address).

Article 24 (Follow-up Measures) The information security manager must implement the following follow-up measures after completing the infringement accident response:

1. Record the infringement accident response results in the Infringement Accident Report
2. Notify the reporter on measures to prevent a recurrence of the same infringement accident and make an announcement to members of the University if necessary.

Article 25 (Restriction Process) ① Restrictive measures may be taken for security when information assets of the University are breached by unauthorized persons inside or outside the University.

② Restrictive measures may include restrictions on using the University's information assets or service restrictions.

③ Restriction contents must be immediately notified to the concerned person or relevant person when a restriction occurs. In case of an emergency, actions can be made first and later notified.

④ When a disciplinary action higher than limiting usage of the University's information assets or restricting services is necessary, it shall be processed in accordance with the University's relevant regulations.

Article 26 (Organization Composition) ① The information security officer shall have POSTECH-CERT to respond to infringement accidents such as hacking of the University's information system and information network according to Article 6 Clause 4 of the Regulations on Security.

② POSTECH-CERT shall consist of information security officer as the head, administrative personnel such as information security manager and information security staff, and technical personnel such as PLUS, an information security club, etc.

③ POSTECH-CERT shall perform each of the following roles:

1. Infringement Accident prevention activities: self-inspection, mock hacking, spreading education
2. Respond to and analyze real infringement accidents, damage recovery techniques
3. Share information with CERT of other organizations and support cooperation systems
4. Act as a single window for responding to infringement accidents such as cyber control

Article 27 (Organization Operation) The operation of POSTECH-CERT shall be stipulated separately.

Chapter 7 Information Security Audit

Article 28 (Types of Audit) ① Information security audit shall be divided into a periodically performed regular audit and an irregularly performed special audit.

② A special audit shall be performed when issues such as the following occur:

1. When a serious information infringement accident is expected or has occurred
2. When the information security officer determines a special audit is necessary

Article 29 (Personnel Composition) ① Information security audit personnel shall perform duties under the direction of the information security officer.

② As a rule, information security audit personnel shall be the staff of the information security administrative Department and, if necessary, internal and external professional security personnel may be included.

Article 30 (Audit Implementation) An information security manager shall establish a basic information security audit plan wherein the subject of audit, items, schedule, audit personnel, etc., are defined, and perform security audit as follows after reporting the plan to the

information security officer:

1. Secure necessary security audit evidence through interview of the person in charge, system settings, system log, vulnerability diagnostics, risk assessment analysis, etc., for each audit item when performing an information security audit
2. Cautiously perform the audit to minimize the risk of stopping the work process when auditing a currently operating system
3. Receive correction plans for improper items discovered in the information security audit from the information security fellow manager and perform follow-up actions related to such correction

Article 31 (Reporting Result) ① Results of the information security audit shall be reported to the information security officer. If a major security accident is discovered during the security audit, it should be promptly corrected and then reported to the information security officer.

② The Information Security Audit Report shall include items such as below:

1. Objective/scope of information security audit
2. Duration of information security audit
3. Method of performing the information security audit
4. Audit checklist and results
5. Improper matters and correction plans

Article 32 (Follow-up Measures) ① The information security manager shall notify the subject of audit and audit department matters to be improved according to the results of the security audit.

② The subject of audit and audit department shall establish and carry out improvement methods for improper matters discovered during the information security audit and notify the results to the information security officer.

③ The information security officer shall regularly inspect the implementation process for security improvements that should be solved in the mid- to long-term and, if necessary, support the improvement methods until the improper matter is completely solved.

Chapter 8 Information Security Training

Article 33 (Security Training) ① The information security officer must establish an information protection training plan and request the competent department related to training so that continuous training can be carried out.

② Information security manager must regularly or irregularly train personnel involved in information protection jobs in accordance with the implementation standard of the competent department related to training.

③ If necessary, the information security manager may consign training to an outside professional information protection training institute after discussions with the competent department related to training.

④ Among irregular training stated in paragraph 2, newly employed personnel or transferred personnel must receive security training within 5 days of employment and prospective personnel permitted to handle confidential materials must be approved after receiving the training.

Addenda

1. The Detailed Rules 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. The Detailed Rules on the Classification and Management of Information Assets, Detailed Rules on Infringement Accident Response, Detailed Rules on System Security Management, Detailed Rules on Application System Security Management, Detailed Rules on Risk Assessment and Management and Detailed Rules on Information Protection Audit shall be abrogated and integrated thereto as of the establishment date of the present Detailed Rules.

Addenda

1. The Detailed Rules shall be established and take effect on February 18, 2013.
2. Matters implemented prior to the effective date of the Detailed Rules herein shall be deemed to have been implemented by these Detailed Rules.

(Attachment 1) Information Asset Codes and Classification System

Information Asset Codes and Classification System

Category	Type	Code	Details
Information Assets	Hardware	HW-SV-0001 (Server)	A device which provides a service to a client via a network. Basically, a device with an operating system and system software and it includes super computers, workstations, storage systems, etc.
		HW-NW-0001 (Network)	A device which enables data exchange by connecting at least two computers with a cable, etc. It includes communication equipment such as routers, switches, AP, etc.
		HW-SS-0001 (Security System)	As a device to protect from various threats, it includes intrusion detection systems, firewall systems, threat management systems, etc.
		HW-PC-0001 (PC & Peripheral)	Personal computers having an operating system and peripherals (e.g. printer, scanner, etc.).
	Software	SW-0001	Various types of application programs used in computer programs and used to solve problems. It includes system managing program, diagnosing program, communication program, utility, applications, source program, and object program.
	Data	DA-0001	Information in the form of letters, numbers, sounds, pictures, etc., that can be processed by a computer. It includes data in operation, data saved on-line, off-line data, back-up data, monitoring record, database data and transmission data via communication medium.
	Human Resources	HR-0001	Referring to human labor as a production resource, it includes users, managers, maintenance persons, customers, contractors, external personnel, etc.
	Document	DOC-0001	Shows a certain opinion, concept or ideas in writing or signs. It includes system documents, user manuals and operation and training guides.
Physical/Environmental Assets		PH-0001	Tangible assets visible to the eyes. It includes computer communication facilities, magnetic media, support equipment, buildings and supplementary installations, heating, lighting and convenient facilities.
Active Assets		ACT-001	As assets created during activities, it includes image,

		fame and operation of the organization.

(Attachment 2) Importance Evaluation Criteria and Classification for Information Assets

Importance Evaluation Criteria and Classification for Information Assets

1. Importance Evaluation Criteria for Information Assets

Evaluation Criteria	Evaluation Level	Details
Confidentiality	High (3)	When a major loss is experienced throughout the entire University if the concerned information asset is leaked without authorization
	Medium (2)	When partial loss is experienced by the University if the concerned information asset is leaked to the outside
	Low (1)	When no loss is experienced by the University or it does not matter that the concerned information asset is disclosed to the outside
Integrity	High (3)	When a major loss is experienced throughout the entire University if the concerned information asset is tampered with
	Medium (2)	When partial loss is experienced by the University if the concerned information asset is tampered with
	Low (1)	When there is hardly any effect in performing the job even if the concerned information asset is tampered with
Availability	High (3)	When major loss is experienced throughout the entire University if it is impossible to use the concerned information asset
	Medium (2)	When partial loss is experienced by the University if it is impossible to use the concerned information asset
	Low (1)	When there is hardly any effect on performing the job even if it is impossible to use the concerned information asset

2. Importance Level for Information Assets

Importance Level for Information Assets	Security Requirements Evaluation Index
VH (Very High)	9 points
H (High)	7-8 points
M (Medium)	6 points
L (Low)	4-5 points
VL (Very Low)	3 points

(Attachment 3) Information Asset Register

Information Asset Register

Information Asset Code	Hardware			Software			Data & Document				Additional Information							Importance Evaluation				
	System Name	IP Address	Quantity	Operating System	Name of Application	Quantity	Data & Document Name	Storage Method	Storage Medium	Retention Period	Model Name	Manufacturer	Main Use	Installation Location	Managing Department	Manager	Operator	Confidentiality	Integrity	Availability	SUM	Level
HW-NW-0001	Server farm switch	3.99	1	12.0 (3)XE2							Catalyst 6509	CISCO	Main	Computer Room	Information System	Sang-moo Park	Gil-dong Hong	3	3	3	9	VH

※ Input only relevant items in accordance with Article 4 (Classification and Registration)

메모 [h2]: 5조가 아닌 4조로 수정 합니다. 확인 부탁드립니다.

(Attachment 4) Infringement Accident Report

Infringement Accident Report

❑ Basic Information of Infringement Accident (to be filled out by Reporter)

- Name:
- Department:
- Contact no. (e-mail, phone no.):
- IP address and usage:
- OS type and version:
- Time and date of infringement accident discovery:
- How the infringement accident was discovered:

- Damages of the infringement accident:

❑ Response Measures Taken (to be filled out by the person in charge at Computer Emergency Response Team)

- Responder:
- Time/Date:
- Attacker information:
- Damage detail:

- Confirmation and measures taken:

- Future measures to be taken:

(Attachment 5) Infringement Accident Risk Level Table

Infringement Accident Risk Level Table

Risk Level	Damages	Effect on the Job
Level 1	1. Complete or major destruction of the central computer room 2. Operation suspension of all or most of the systems 3. Disconnection of communication lines 4. Operation suspension of most network equipment which affect services related to the jobs of the University 5. Disconnection of power supply	1. Overall hindrance to the jobs of the University
Level 2	1. Partial destruction of the central computer room 2. Partial operation stop of the system 3. Partial disconnection of communication line 4. Partial operation suspension of a network equipment which affect services of the University	1. Partial hindrance to the jobs of the University 2. When jobs of the University or departments are greatly affected because groupware, etc., stopped operation
Level 3	1. Temporary hindrance to the information system but there is no physical damage thereto 2. Some unstable communication lines (abnormal traffic) 3. Temporary hindrance of network assets registered in the information asset list but there is no physical damage thereto 4. In case of the following infringement accidents: - When continuous acts of collecting vulnerabilities (scanning) are detected - When continuous illegal access attempts are discovered - When transmission of abnormal packets has increased - When a quickly spreading worm/virus from the outside is found	1. Temporary delay and unstable state of University work 2. When University work is interrupted due to temporary delay and unstable groupware, etc.