# Bylaws Regarding Security Management of Service Providers

Established Oct.15, 2010

1. Purpose

The purpose of these bylaws is to prevent the leakage of confidential data such as the service results or the internal data provided to external service providers due to carelessness or hacking.

2. Application Scope

A. Applies when consigning service providers such as the information business of the University, information security consulting, research and development (R&D), etc. to private businesses, research institutes, etc.
B. Applies when the University requests outsourced services to private companies through contract for specific tasks such as the maintenance work, etc. in order to increase task efficiency or when it is necessary.
C. For matters not specified in these bylaws, refer to the University's Information Protection Regulation and Bylaws, as well as relevant federal statutes and regulations of the Republic of Korea.

3. Responsibilities and Rights

A. The head of the ordering agency for the service business shall take measures to ensure that the Information Security Officer is responsible for the security management of the personnel, equipment, data, etc. for the overall performance of the service business.
B. The Information Security Manager shall oversee security affairs regarding various matters such as the Service Provider's participants, equipment, security management of data and the system, establishment and enforcement of security measures for the network, etc.
C. The security management responsibilities related to the service business belong to the representative of Service Provider, and the representative may appoint a manager who will perform the security tasks for the overall service business.
D. The manager of Service Provider shall supervise the overall security management of the subcontractor regarding business and security affairs of the personnel, equipment, and data related to the service business.

4. When bidding service

A. Important outsourcing service business shall be classified to the appropriate level of confidentiality from the beginning phase, and be requested for service as such. The use of ambiguous expressions such as 'care required', 'security required' are prohibited.
B. The Service Requesting Organization (hereinafter referred to as "the SRO") shall, among the data and equipment expected to be invested, classify the ratings of those that require security in accordance with the relevant statutes and self-regulation, and submit the necessary security requirement standard to the department in contract prior to the bid announcement.

C. The Department in Contract (hereinafter referred to as “the DC”) shall notify in advance the information such as the obligations of maintaining confidentiality regarding the service business, the penalties of violation, etc. in time of the bid announcement.
D. If the SRO requests submission of proposal, it must prepare a list of assessment items and evaluation criteria for security management plans such as documents, facilities, equipment, etc.
E. The SRO and the DC shall review whether the security management plan for the overall service business presented in the bid proposal by the Service Provider is valid and reflect this in the selection of business.

5. When making a contract on service:

A. If external security is required for the service business itself or regarding the data and equipment invested, an agreement on confidentiality may be additionally made in order to ensure confidentiality and to clearly define the scope of security and the responsibilities.
B. The agreement on confidentiality must specify the matters as to include: the scope of confidential information, security compliance, liability in case of violation, intellectual property rights issue, return of data, and etc.
C. The contract must specify that the participants of service business cannot be replaced by the Service Provider at their own discretion, and that Service Provider must immediately report to the ordering agency in case there is any change in the participants’ personal information (including overseas travel) and obtain an approval.
D. The task guideline (or task directions) must describe in detail the overall security matters such as security inspection/education on the security management method/personnel for data, equipment, facilities, etc. in order to clearly communicate the requirements of the ordering agency to the business.

6. When performing service

A. The security management of the participating personnel must comply with the following:
    ① A Declaration of Information Security containing each individual’s signature and signs must be collected from all participants of the service business (Attachment #1)
    ② Security training shall be conducted on all participants prior to their performance in service business on the obligation of confidentiality and the penalties in case of violation in accordance with the legal statute or regulation of the ordering agency.
    ③ In order to reinforce security awareness, the Service Provider must periodically conduct its own security education and submit the report on the information-protection education result (Attachment #2) to the ordering organization. Service Provider must also attend any security education that the ordering agency requires.
B. The security management of data must comply with the following:
    ① The confidential information provided to the Service Provider such as the network map, IP status, service business products and personal information shall be written on the ‘data management book’, be signed by both the giver (Information Security Manager of the concerned agency) and the receiver (security manager of Service Provider) before the transfer from the giver to the receiver.
    ② All data related to the service business and all products produced during the business process must be saved in the file server of the Ordering Agency or be stored and managed in the PC designated by the Information Security Manager

③ All data related to service business must not be saved on the online file storage services or personal emails, and when data transmission through emails becomes necessary, the data shall only be transmitted through its own emails following the encryption of the attached data. However, highly classified confidential data must never be sent or received through emails.

④ If the performance of business is to be done in the office provided by the Ordering Agency, the provided confidential data must be returned when the worker leaves the office, and the general documents other than confidential documents can be stored inside a locker with a combination lock if there happens to be one in the office provided by the Ordering Agency.

⑤ All products and the records produced while performing service business must never be provided, lent, or viewed to/by any person who is unauthorized by the Information Security Manager. The Service Provider must mark the name of the person who printed it out and date of printing on the paper when printing out confidential information.

C. The security management of the office and the equipment must comply with the following:

① The service business must be performed at a place which has a combination lock, can be controlled, and is provided by the Ordering Agency, or at an office where the equivalent environment is established through consultation with the Ordering Agency.

② A security inspection must be conducted on the Service Provider's office or the place of service performance at least once a week, and regarding the result of inspection, the Service Provider must comply with the feedbacks or demands of improvement given by the Information Security Manager of the Ordering Agency.

③ When performing service business in the Ordering Agency 's office, the laptops and related devices must be checked for virus infection or unauthorized usage/transfer every time a participating employee brings in or takes out laptops or related devices. Must check:

- Whether the device has a Vaccine or PC Security Program installed
- Whether the device is infected with malicious codes or has been subjected to an unauthorized usage/transfer.

④ An unauthorized use of data storage device such as USB is prohibited, but if it becomes necessary to store products, it must only be used under the supervision of the Information Security Manager of the Ordering Agency.

⑤ The Service Provider must set the CMOS password, the Window login password, and the screen saver (10-minute interval) password, etc. on the laptops and PC to which contains at least 8 letters *and* numbers.

D. The security management must comply with the following when accessing internal or external networks:

① When the use of the Ordering Agency's network becomes necessary while performing the service business, the user ID for the participants of business must be applied in accordance with the external personnel ID application (Attachment #3), and the applied IDs must be

registered as a group. Each ID must be given an access right to the information system. The access right must be revoked or the ID must be deleted once the access right given per each ID becomes unnecessary.

② When the use of the Ordering Agency's network becomes necessary while performing service business, the password given to the participants must be separately recorded and managed by the Information Security Officer of the Ordering Agency, and he or she must access the participants' accounts from time to time and check up on the stored data and the work history.

③ When the use of the Ordering Agency's network becomes necessary while performing the service business, the Information Security Officer of the Ordering Agency must order the equipment & server administrator to check the access records to the internal server and the network equipment every day and to report any abnormalities to the Information Security Manager.

④ When the use of the Ordering Agency's network becomes necessary while performing the service business, the laptop PC used by the Service Provider must be prohibited from having an internet access. However, if the internet access becomes necessary for the performance of business, the Service Provider's Manager in Charge must request for it himself, and if the Ordering Agency's Information Security Manager agrees that it is necessary, the internet access must only be granted after designating the laptop to have an internet access, and setting the firewalls to allow access to only the necessary websites.

⑤ The network of the Ordering Agency and the Service Provider must completely block access to any online file-sharing websites such as P2P using a firewall or alike.

7. At the end of service

A. The final products or materials that are produced after the completion of business which require external security shall be made and managed as confidential, and the unnecessary data shall be deleted and discarded.

B. All materials related to the service such as every data, equipment, documents, and intermediate or final products that were ever provided to the Service Provider shall be retrieved in entirety, and the Service Provider is prohibited from keeping any copies of such.

C. Electronic records saved in electronic devices such as laptops and data storage devices shall be secured in accordance with Article 6 of the 'Basic Guidelines for Information Protection of Educational Institutions' of the Ministry of Education, Science and Technology (MEST).

D. After the retrieval and disposal of service-business-related materials, POSTECH must demand and obtain a letter of confirmation from the Service Provider indicating that it does not possess any service-business-related-materials such as copies, and with the name of its representative written and signed.

[Attachment #1]

Declaration of Information Security (for external personnel)

I declare that I will comply with the following terms when performing my duties with POSTECH from (Month), (Day), (20XX) to (Month), (Day), (20XX).

1. I recognize the significance of the information I obtained while performing my duties for POSTCH, and I acknowledge that any related work are confidential for the University's security.

2. I will comply with the following with regards to working for POSTECH.

   A. I will not disclose POSTECH's classified information regarding the operation or any other information in general.

   B. I will not exploit or release any of the information I gained through my job performance at my own discretion.

   C. I will use POSTECH's infrastructure resources (emails, phones, fax, etc.) for only job purposes.

   D. I will not disclose any information that may compromise POSTECH's interests.

   E. I will not perform any work other than what is permitted, and will comply with all current laws and regulations regarding security.

3. I will not disclose to the third parties any and all confidential information I acquired while performing my job, not only during my service (e.g. during the contract period) but even after my service performance has ended (e.g. expiration or termination of contract). I will also return all relevant information at the end of the service, and proceed with the eviction procedure after confirming with the manager in charge.

4. I acknowledge that the POSTECH has the possession rights to all products created through my service and I agree to POSTECH's ongoing supervision and the regular/irregular checks (including email monitoring) to prevent unauthorized leakage of information.

5. I will not use any illegal software in my use of the POSTECH system, and if any damage is done to the POSTECH's system due to my use of the illegal software (including the virus spread), I will be subject to all civil and criminal liabilities.

6. If any harm or loss is done to POSTECH due to the damage or destruction of physical or intangible assets such as electronic equipment, software, or data during the course of my service to POSTECH, I will be liable to the compensation.

7. If I violate any of the declarations above, I will be subjected to the severe consequences in accordance with the relevant statutes and pledge to subject myself to all civil and criminal liabilities accordingly.

Month, Day, 20XX

Affiliation of the pledger:

Name: (Signature)

POSTECH

[Attachment #2]

Information Security Education Result Report (for Service Providers)

1. Purpose

The results of the Information Security Education autonomously conducted during the service business, and in accordance with the information security regulation of the University, shall be submitted to the Ordering Agency.

2. Subjects

All personnel participating in the service business

3. Matters

The curriculum and the time schedule are to be determined through consultation with the ordering department of the service business with the support from the University’s Information Security Department.

4. Detailed Education Results

| Name of Trainee, Affiliation/Job Tittle | Phone: | E-mail: | Note: |
|---|---|---|---|

POSTECH

[Attachment 3]

External Personnel ID Application

Approved by Director of Department

Applicant Affiliation

Name (Seal or Signature)

Date of Application Month, Day, 20XX

Application Period Month, Day, 20XX

Purpose ☐ New Registration ☐ Changes in Entitlements ☐ Inactivation ☐ Re-use ☐ Delete ID

System

Name 1. 4. 7.

2. 5. 8.

3. 7. 9.

ID Name

Default Password

Reason

and/or

Contents

1. You must change your password when you login for the first time
2. The password must be composed of 8 or more letters of both alphabets and numbers, and the special characters such as $,\,',!,& cannot be used.

Information Security

Person in Charge Name of Department

Name (Seal or Signature)

Processed Date Month, Day, 20XX

System

Person in Charge Name of Department

Name (Seal or Signature)

Processed Date Month, Day, 20XX

POSTECH