



## Information Security Standard Measures for ASU's Computer Systems

Version 0.1  
November 2008

## Table of Contents

1 DOCUMENT CLASSIFICATION: UNIVERSITY CONFIDENTIAL .....	3
2 DOCUMENT REVISION .....	3
3 DEFINITION OF TERMS .....	4
4 STANDARD.....	4
5 ENFORCEMENT.....	4

## 1 DOCUMENT CLASSIFICATION: UNIVERSITY CONFIDENTIAL

Physical and Administrative Controls	Reproduction	Distribution	Destruction/Disposal
Each employee is responsible for controlling usage and access on a need-to-know basis. This policy also applies to contractors.	Limited copies may be made only to employees or contractors who have signed a non-disclosure agreement.	Internal: Use University envelope whenever possible. External: Use sealed envelope.	Use document destruction bins. Shred or erase magnetically recorded documents if unable to recycle.

## 2 DOCUMENT REVISION

Date	Revision	Revised By	Basis for Revision & Description

### Document Change/Correction Request

Your feedback is valuable. Anyone who uses this document is invited to use this form to submit requests for changes or corrections to this document. Please complete all of the sections and mail to:

#### Document Identification

**Document title**  
**Date of Document**  
**Master File Location**

#### Requester Identification

Name	
Department	
Phone Number	( ) -
Email Address	

#### Request

The following Change is requested:

**Please describe the change and reason(s) why the change is requested.**

Correction:

**Section \_\_, page \_\_ contains the following erroneous information:**

**This information should be changed to:**

**Attach additional sheets if necessary to fully describe the change or correction.**

### 3 DEFINITION OF TERMS

- **Access control** is to restrict objects to which a subject is allowed to have access.
- **Secure area** is the inside of a server room in which computers and communication equipment are located and where the measures against information security violations caused by outside hackers and disasters are implemented physically and environmentally.
- **Contractor** refers to a person who undertakes all or part of the processing tasks on information systems such as planning, development, maintenance, and operation.
- **Delivery personnel** refers to a person whose purpose is to receive or pass items to employees working in a secure area and who does not need to enter the secure area. Such exchanges of items can occur in courier services and delivery of office equipment, etc.
- **Outsourcing** is to order all or part of the processing tasks of information systems such as planning, development, maintenance, and operation to the personnel outside the government agency.
- **Availability** is the status in which a person who is allowed to access information can access the information and the related assets without being interrupted when he or she needs to do so.
- **Integrity** is the state in which information is not damaged, altered, or deleted.
- **Equipment, etc.** refers to information equipment and software.
- **Confidentiality** is the state in which only a person who is allowed access can access the information.
- **Shared identification code** is an identification code that is shared by multiple subjects. In principle, a single identification code is granted to a single subject; however, it can be shared by multiple subjects if there are any restrictions on the information system or in consideration of how they are used. Such an identification code is called a shared identification code.
- **Storage media** is media on which information is recorded or described. Storage media includes paper or other tangible objects that contain information perceptible by the human senses through writing, documents and other letters and figures (hereinafter referred to as “written documents”) and records created through methods imperceptible by the human senses, such as through electronic methods, magnetic methods or others, that are provided for information processing by computers (hereinafter referred to as “electronic storage media”). Electronic storage media includes embedded electronic storage media that are built in computers and communication equipment and external electronic storage media such as an external hard disk, CE-R, DVD, MO, USB memory, and flash memory.
- **Administration** is to manage the information for authentication (including identification code and authentication information) and the granting of information for permission of access control.
- **Announced security hole** is a security hole that can be known to everyone and includes one announced by software or hardware manufacturers and vendors and one announced by security-related organizations such as CERT Coordination Center.

- **Service** is a set of functions that is composed of a single or multiple functions provided to the connected computer by an application running on a server.
- **Least privilege** is a function to limit the spectrum where administrative rights can be exercised to the minimum extent necessary for the administrative task.
- **Identification** is to identify the subject that accesses an information system.
- **Identification code** is a code that an information system recognizes to identify the subject. A User ID is a typical identification code.
- **Subject** refers to a person who accesses the information systems or other information systems and a device. A subject is supposed to be human in principle; however, other information systems and devices can be subjects when multiple information systems and devices work in coordination.
- **Authentication** is to verify whether the subject that presents an identification code is legitimate or the one that is granted the identification code. The information system recognizes the subject as legitimate if the identification code and authentication information are presented in a correct way and authentication is successful. Though being “authenticated” means to be proved officially or by a third party, “authentication” in these standards for Measures does not always mean such proof.
- **Authentication information** is information that a subject presents to an information system in order to become authenticated. A password is typical authentication information.
- **Authentication information storage device** is a device that stores authentication information so that a legitimate subject can own or hold it. In the case that an authentication method based on ownership is used, the information system recognizes the subject as legitimate if it has this. A magnetic strip card and IC card are typical authentication information storage devices.
- **Information system** is a computer system that provides information processing and communications.
- **Information security policies** are policy of the University and the operation procedures that provide step-by-step instructions on how to execute the measures formulated in the standards of University in specific information systems and tasks.
- **Information transfer** is to transmit electronically recorded information and to transport electronic storage media and written documents that contain information outside the government agency.
- **Legal employee** refers to an employee who is designated to execute administrative tasks by appointment and or title.
- **Software** refers to the procedures and orders to operate a computer that are written in a form that computers can understand. An operating system and applications running on the operating system can be viewed as software in a broad sense.
- **Terminal** is a computer that an employee directly operates (including an operating system and connected peripheral devices) such as a PC and a PDA.

- **Communication line** is a mechanism by which multiple computers are connected to send or receive information in a prescribed communication protocol. A communication line that is established by connecting a line and communication equipment is called a physical communication line, and a communication line that is formulated over the physical communication line and can exchange information in a prescribed communication protocol is called a logical communication line.
- **Communication equipment** is a device that is located to connect the lines and used to control the information exchanged by computers via a line. Repeater hubs, switching hubs, routers, and firewalls are included.
- **Computers** are computers in general and include operating systems, servers including connected peripheral devices, and terminals.
- **Marking** is information to indicate restrictions on how to handle the information (meaning measures to secure appropriate handling of information such as “do not copy,” “internal use only,” “do not re-distribute,” “encryption required,” and “destroy after reading,” etc.).
- **Multiple factors authentication / composite authentication** is an authentication method in which multiple factors of knowledge, ownership, and or biological information are used to authenticate.
- **Outside the University entity** refers to outside the organization or building managed by the University that legal employees belong to.
- **Communication line outside the University** is a logical communication line that computers that are not managed by the University are connected with and is used for communications between such computers regardless of what physical communication lines (wired/wireless, real/virtual, managed by the University/other organizations) or communication equipment are used.
- **Information systems not supplied by the university(unsupplied information system)** is the information systems that are not the ones supplied by the University that legal employees belong to. These may include private PCs and the information systems provided to loan employees working in the relevant University by the original organization.
- **Information processing using information systems not supplied by the University** refers to the information processing required to execute the administrative tasks using unsupplied information systems. This includes not only using the devices directly but also using the services provided by the devices. A service here means one such as an e-mail service for private use. Transferring business e-mail messages required to execute the administrative tasks to a privately used e-mail service and vice versa are examples.
- **Malware** is software in general that brings a result unwanted for computer users, such as computer viruses and spyware.
- **Malware definition file** is the data that antivirus software, etc. uses to determine malware.
- **Labeling, etc.** is to put information into a state in which all persons who handle it can have a common understanding of its classification. The classification must be shown for each item of information in principle. However, this includes any measures to make a common understanding of classification of the information. For specific information systems, it is also deemed as labeling, if the policy, etc. clearly states classification of

information stored in the information system and the policy is notified to all persons who use the information system.

- **Mobile PC** is a terminal that is movable as needed for business purposes regardless of terminal shape. A laptop PC that is used at a specific place is not a mobile PC.
- **Exceptional measures** refers to when an employee takes alternative measures required in order to continue executing his/her administrative tasks appropriately, or, if there is a rational reason for doing so, reports and obtains permission not to meet compliance requirements in the case that complying with the relevant information security policies is difficult.
- **Login** is an action in which a subject requests authentication. Because login is followed by authentication, the validity of the subject is unknown at the login stage.
- **Logon** is the status in which the subject that has requested authentication by login is validated by the information system.
- **University entities** refers to ASU's departments and colleges, including the Presidents Office, the Provost, Legal Counsel, Finance, Administrative Areas, Colleges and Dean Areas, and all other University entities not mentioned in this document.

## 4 GENERAL

ASU must take responsibility for its own information security. It is necessary to formulate a unified framework to provide guidance on such measures and raise the level of information security based on the "Attorney General Audit Report # 08-04."

This document provides the standards for the measures that ASU should take to achieve information security and to further raise the level of information security in the unified framework.

### 4.1 Revising the Standards for Measures

This document should be reviewed periodically and revised as necessary to maintain its applicability in the future.

### 4.2 Complying with Laws and Regulations

How information and information systems are handled is discussed in Laws and Regulations (hereinafter referred to as "relevant laws and regulations"), Section XX. Relevant laws and regulations must be conformed to when information security measures are taken. Because these relevant laws and regulations should be conformed to regardless of the information security measures formulated, this document does not specifically address them. Furthermore, existing ABOR decisions on information security measures must be conformed to as well.

### 4.3 How to use Standards for Measures

#### 4.3.1 *Relationship of these Standards for Measures and Standards of University Entity*

This document provides the Standards for Measures that each University should take to implement information security and further raise their level of information security. Additionally, each University entity should review their current information security policy to achieve heightened information security than provided for in this document.

Each University entity should also determine what to define in its own Standards in view of its characteristics and update it accordingly by referring to this document directly and incorporating the relevant contents of these Standards for Measures with or without modifications (structure, expressions.)

## 4.4 Scope

These Standards for Measures should be applied as follows:

- A. These Standards for Measures are formulated for the purpose of protecting “information.” “Information” in these Standards for Measures refers to information that is stored in information systems, stored in electronic storage media outside the information systems, and written or printed on documents for information systems. Unfinished documents are also included within this scope. Information written or printed on the documents can be electronically recorded information that is described in the documents (containing information input into the information systems or information output from the information systems) and specifications of information systems.
- B. These Standards for Measures should be applied to employees who handle information and information systems. In these Standards for Measures, “employees” refers to University entity employees and those under a departmental structure of their respective University entities who handle information and information systems governed by the respective University.

### 4.4.1 Structure

This document is composed of three levels – Chapter, Section and Item. Information security measures are organized into the following chapters:

- Building the Organization and System
  - Measures for Information
  - Measures based on the Clarified Requirements of Information Security
  - Measures for Components of Information Systems
  - Measures for Individual Considerations
- A. **Building the Organization and System** describes organizational issues such as systems, evaluation procedures, breaches, and exceptional measures and also clarifies operational authority and responsibilities of employees to ensure the entire organization takes information security measures.
  - B. **Measures for Information** defines compliance requirements at each stage of the information lifecycle – creation, use, storage, transfer, provision, and deletion – and indicates the measures that employees must take when performing tasks to protect information.
  - C. **Measures based on Clarified Information Security Requirements** explains security functions such as access control and defines compliance requirements to prevent threats such as security holes, malware, and denial of service attacks.
  - D. **Measures for Components of Information Systems** defines compliance requirements and describes measures to take for information systems in view of the individual characteristics and lifecycle of information systems such as computers and communication lines.
  - E. **Measures for Individual Consideration** define compliance requirements for individual consideration that need specific attention in terms of information security such as procurement, development, and information processing outside the University.

#### **4.4.2 Itemized Measures**

This document sets compliance requirements for measures each University should take by individual item.

#### **4.4.3 Setting Security Level**

The information security measures that should be taken depend on the importance of the information assets to protect or threats that exist. The measures must be strong enough for the characteristics of information systems and tasks. These Standards for Measures set the strength level for each measure to meet compliance requirements and are formulated as follows:

A. **High Risk Compliance Requirements** are measures that “*must*” be taken for especially important

Information (Currently this consist of FERPA, HIPAA, etc.,) and the information systems that handle such information as required by University entities

B. **Confidential Requirements** are measures that “*should*” be taken for especially confidential information (Currently this consist of Intellectual Property, University non-public information, and also information deemed by the university that is not for general public knowledge).

By following the above compliance requirements, each University entity should take measures that satisfy or exceed the Basic Requirements. Each University entity should also evaluate the risks in view of the characteristics of information systems and tasks in order to select an appropriate level for each compliance requirement.

#### **4.4.4 Evaluation Procedures**

Each University entity should confirm that the following requirements are met based on these Standards for Measures by conducting information security auditing periodically or as necessary.

- The standards of University entities conform to these Standards for Measures (confirming compliance in design)
- Actual operations conform to the standards of University entities (confirming compliance in operation)
- The standards of University entities are appropriate and efficient for the risks or are not unfeasible (confirming the adequacy in design)
- Actual operations are appropriate and efficient for the risks (confirming the adequacy of operations).

The main purpose of information security auditing at each University entity is to confirm compliance in design and operation. In principle, each University entity should take responsibility for implementing its own information security measures. However, in order to promote information security measures for all University entities, each entity must report to the ASU University Information Security Office how well the measures are implemented and the results of their audit. The University Information Security Office will inspect and evaluate how well the information security policy for each University entity is formulated and how well the measures are implemented based on the evaluation metrics related to these Standards for Measures.

## 5 BUILDING THE ORGANIZATION AND SYSTEM

### 5.1 Compliance Requirements

- B. Designation of Security Committee
  - The ISO designated two information security committees – the University Technology Council (UTC) and the Technology Advisory Group (TAG)
  - The ISO designated a Chair and Co-Chair within TAG.
  - Committees are responsible for creating, reviewing and approving security standards across the University. The ISO will approve the standards.
  
- A. Designation of Information Security Auditor/Assessor
  - The ISO should designate the information security auditor/assessor.
  - The ISO will direct the auditor/assessor's activities.
  
- B. Designation of HIPAA Information Security Officer unit representation

### 5.2 Assignment of Roles

- A. In the context of the implementation of the information security measures, the same person must not undertake the following roles.
  - The applicant for approval or permission and the approval or permission (hereinafter referred to as “approval authority, etc.”)
  - The auditee and the auditor
  
- B. Approval or permission by supervisors
  - The employee must apply for approval with the approval authority, etc. to make a decision of approval or permission (hereinafter referred to as “approval, etc.”) in the light of their official authority. When approval is obtained from the supervisor of approval authority, etc., it is not required to obtain approval from the approval authority, etc.
  - In the case that the employee is granted approval, etc. in the preceding case, he or she must take necessary measures in accordance with requirements or approval authority, etc.

### 5.3 Violation and Exceptional Measures

- A. Handling the violations
  - In the case that a breach is found within a University entity's information security policy, employees must report to the ISO who is responsible for the policy.
  - The ISO will instruct the violator or pertinent persons to take necessary measures to maintain information security in the case of being informed of or finding any serious breach of an information security policy.
  
- B. Exceptional Measures
  - The information security committee must designate the person who judges whether the request for applying any exceptional measure should be allowed or denied (hereinafter referred to as “the judge”) and define the judgment procedure.
  - The employee must request for the approval for exceptional measures to the judge by following the formulated procedures. However, the employee can make this request after the fact in the case that the exceptional measures is immediately needed for executing his or her tasks and the immediate taking of alternative measures that are not provided for in the information security policy or

violation of the policy is unavoidable. The employee must clarify the following information:

- Requester information (name, department, contact)
  - Portion of information security policy that the exceptional measure is requested for (compliance, policy, etc.)
  - Period for applying the exceptional measures
  - Description of the exceptional measures (an alternative measure, etc.)
  - Reporting procedure for terminating the exceptional measures
  - Reason for requesting the exceptional measure
- The judge must review the request for applying an exceptional measure made by the employee in accordance with the formulated judgment procedure and approve or disapprove the request. When the judge makes a final decision, he or she must formulate a request process record including the following information and present it to the ISO.
    - Name of the Judge (name, title, department, contact)
    - Requester information (name, department, contact)
    - Portion of information security policy that exception measure is requested for (Authorization, Compliance, etc.)
    - Period for applying the exceptional measure
    - Description of the exceptional measures (alternative measure, etc.)
    - Reporting procedure for terminating the exceptional measure
    - Reason for requesting the exceptional measure
    - Approved or disapproved
    - Reason for approval or disapproval
    - Portion of information security policy or compliance that exceptional measure is approved for
    - Period of the approved exceptional measure
    - Description of the exceptional measures (an alternative measure, etc.)
    - Reporting for terminating the exceptional measure
  - The employee must report to the judge who is responsible for the exceptional measure when he or she terminates the approved exceptional measure. However, this reporting is not required if the judge decides so.
  - The judge must check whether the requestor has reported terminating the approved exceptional measure on its expiration and instruct the requestor to report it and take necessary measures. However, this reporting is not required if the judge decides so.
  - The ISO must formulate the ledger of request process records for exceptional measures and provide this to the information security auditors at their request for reference purposes.

## **5.4 Operation**

### ***5.4.1 Education of Information Security Measures***

#### **Educating about Information Security Measures**

##### High Risk Compliance Requirements

- The ISO must educate employees about information security policies and regulation.
- The ISO must examine educational contents on information security policy and regulation for the employees and formulate educational materials.
- The ISO must develop and plan to educate employees on information security measures and organize its implementation system so that employees can participate in at least one education program per year.
- The ISO must plan and develop the contents and system for education on information security measures and organize the implementation system so that any employee who starts working or transfers to another department can participate in an educational program.
- The ISO must establish the system to manage the achievement of participation of the employees on information security measures.
- The information security officers must inform the University entity of the achievement of participation of each employee on information security measures.
- The University entity must advise the employee who has not participated in any educational program for information security measures. In the case that the employee does not take his or her advice, the University entity must report this to the ISO.
- The ISO must report the achievement of participation of each employee on information security measures to the information security committee once a year.

#### Confidential Requirements

- The ISO must plan the contents for training employees on information security measures and organize the system regarding information security rules.

#### **Participating in Educational Programs on Information Security Measures**

##### High Risk Compliance Requirements

- The employee must participate in at least one educational program per year on information security measures in accordance with the plan to educate employees on information security measures.
- The employee must ask the ISO how they can participate in an educational program on information security measures at his or her new workplace when they start working or transfer to another department.
- The employee must report to the ISO in the case that he or she cannot participate in an educational program on information security measures for any reason that he or she is not responsible for.

##### Confidential Requirements

- The employee should participate in a training program on information security measures if participating in such a training program is formulated in the policy.

### **5.4.2 Failure Handling**

#### **Advance Preparation for Possible Failure**

##### High Risk Compliance Requirements

- The ISO must establish the system to prevent damage from increasing and recover from the failure (including incidents and failures, hereinafter referred to as "failure") in the case of any failures that can breach information security.
- The University entity must establish the failure report procedure that the employee uses to report to the ISO and notify the procedure to all employees.

- The ISO must establish the failure handling procedure.
- For information systems considered especially important for the tasks, the ISO must prepare the emergency network with information including emergency contacts and means of communication for the responsible information system security officer, the responsible information system security administrator and message contents.

#### Confidential Requirements

- The ISO should establish a point of contact to receive information about failure from outside the University and announce the access to the contact to parties outside the University.

### **Reporting and Taking Emergency Measures on Failures**

#### High Risk Compliance Requirements

- In the case that the employee is aware that a failure has occurred, he or she must notify the relevant party and report to the ISO in accordance with the reporting procedure formulated by the Information Security Office.
- The employee must confirm whether the failure handling procedure exists and follow the procedure if possible.
- In the case that any failure has occurred and no relevant failure handling procedure exists or it is unknown whether such a procedure exists, the employee should try to prevent the damage from increasing until he or she is instructed how to handle it. The employee should follow instructions when he or she receives them.

### **Cause Investigation and to Prevent the Recurrence of Failure**

#### High Risk Compliance Requirements

- In the case that any failure has occurred, the University entity and Information Security Team should investigate the cause of failure and prevent the recurrence, then report to the ISO in writing.
- In the case that the ISO receives a report of failure from a University entity, he or she must examine the failure report and take necessary measures to prevent a recurrence.

## **5.5 Evaluation**

### **5.5.1 Self-Assessment of Information Security Measures**

#### **Formulating an Annual Plan for Self-Assessment**

##### High Risk Compliance Requirements

- The ISO must formulate an annual plan for self-assessment.

#### **Preparing for the Self-Assessment**

##### High Risk Compliance Requirements

- The ISO must establish the self-assessment form and procedure for each University entity.

#### **Conducting the Self-Assessment**

#### High Risk Compliance Requirements

- The University entity must instruct employees to conduct self-assessments in accordance with the annual self-assessment plan formulated by the ISO.
- Employees must conduct self-assessments using the self-assessment form and procedure instructed by the ISO.

#### **Evaluating the Result of Self-Assessment**

##### High Risk Compliance Requirements

- The ISO must confirm that the University entity has conducted self-assessments and has evaluated the results.

#### **Making improvements Based on the Self-Assessment**

##### High Risk Compliance Requirements

- The University entity must make any improvements that they believe possible within the scope of his or her authority based on the results of self-assessment, then report their findings to the ISO.
- The ISO must evaluate the results of the self-assessment as a whole and instruct University entities to make improvements as needed.

### **5.5.2 Information Security Audits**

#### **Formulating the Audit Plans**

##### High Risk Compliance Requirements

- The information security auditors must formulate the annual plan for information security audit and gain approval from the ISO.

#### **Instructing the Information Security Audit**

##### High Risk Compliance Requirements

- The ISO should instruct information security auditors to conduct an audit in accordance with the annual plan for information security audit.
- The ISO should instruct information security auditors to conduct audits that are not defined in the annual plan for information security audit as needed to respond to changes in information security conditions.

#### **Formulating the Detailed Audit Plans**

##### High Risk Compliance Requirements

- The information security auditors must formulate individual audit plans to conduct audits in accordance with the annual plan for information security audit and the instructions for auditing to respond to changes in information security conditions.

#### **Preparation for the Information Security Audit**

##### High Risk Compliance Requirements

- The information security auditors must select and appoint a person necessary for the audit work as an information security auditor from among those who are independent from the auditee.
- The information security auditors must partly outsource the audit work to a supplier outside the University entity as needed; all outsourcing should be approved by the ISO.

### **Conducting the Information Security Audit**

#### High Risk Compliance Requirements

- The information security auditor must conduct audits under the direction of the information security auditors based on the audit plan.
- The information security auditor must confirm that the standards of the University entity comply with these Standards for Measures.
- The information security auditor must confirm that the procedure complies with the standards of University.
- The information security auditor must confirm that the actual operations by the auditee are in compliance with the information security rules by confirming the adequacy of the self-assessment, etc.
- The information security auditor must document audit working papers.
- The information security auditors must formulate the audit report based on the audit working papers and submit it to the ISO.

### **Reaction Based on the Results of the Information Security Audit**

#### High Risk Compliance Requirements

- The ISO must instruct other departments to investigate whether similar problems exist and solve them if he or she believes that it is highly likely that the departments other than the auditee pose similar challenges or problems and quick investigation is required based on the audit report.
- The University entity must develop the improvement plan for the problems in which resolution is requested and report this to the ISO.
- The ISO must evaluate the validity of existing information security policies and compliance and order a review as needed based on the results of the audit.

## **5.6 Review**

### ***5.6.1 Reviewing Information Security Measures***

#### **Reviewing the Information Security Measures**

#### High Risk Compliance Requirements

- The ISO must consider whether reviewing the policy and compliance is required as need arises and if it is required, then he or she must review them.
- In the case that the University entity finds any issues or problems in the information security policy and compliance, he or she should consult the ISO.
- The ISO should take necessary measures when consulted with regard to any issues or problems.

## **6 MEASURES OF INFORMATION**

### **6.1 Data Classification (See ASU Data Classification Standard)**

#### ***6.1.1 Classifying the Data***

##### **Classifying the Information**

###### High Risk Compliance Requirements

- The Information Security Committee should establish standards for designating and labeling classification and marking in terms of confidentiality, integrity, and availability of electronic records and confidentiality of written documents for the information used in the tasks.

##### **Classifying the Information on Creation or Obtainment and Considering Marking**

###### High Risk Compliance Requirements

- If an employee creates information, he or she must classify it based on its confidentiality, integrity, and availability and consider whether marking is required.
- If an employee obtains and starts to manage information created by someone outside the University entity, he or she must classify it based on its confidentiality, integrity, and availability and consider whether marking is required.

##### **Labeling Classification and Marking**

###### High Risk Compliance Requirements

- Employees should label the classification of information in a way that can be understood by the person(s) allowed to view it and also label the marking as needed.

##### **Application of the Existing Classification and Marking**

###### High Risk Compliance Requirements

- Employees must apply existing classification and marking in the case that he or she quotes any existing information in new information.

##### **Changing Classification and Marking**

###### High Risk Compliance Requirements

- If an employee thinks that any information requires re-classification, he or she must consult the ISO. If it is required, then the consulted person must re-classify the relevant information appropriately.
- If an employee thinks that any information requires review of marking, he or she must consult the ISO. If it is required, then the consulted person must re-mark the relevant information appropriately.

#### ***6.1.2 Usage of Information***

##### **Prohibiting Usage for Non-Business Purposes**

### High risk Compliance Requirements

- Employees should not use any information for purposes other than executing his or her tasks.

### **Handling Information Based on Classification and Marking**

#### High Risk Compliance Requirements

- Employees must handle information appropriately in accordance with the classification labeled on the information. If the marking is also labeled beside the classification, the instructions for marking should be followed.

### **Handling Classified Information**

#### Confidential Requirements

- Employees should not take classified information outside the University for purposes other than executing his or her tasks.
- Employees must not leave classified information unattended.
- Employees must not make copies of confidential information more often than necessary.
- Employees must not distribute confidential information more often than necessary.

#### High Risk Compliance Requirements

- For High Risk information, employees should clearly indicate the period during which it should be treated as high risk. If an employee thinks changing it to a lower classification is required during this period, he or she must take the steps required for re-classification.
- The employee should give a serial number on the written document in which High Risk information is printed and clarify where it is kept.

## **6.1.3 Maintenance of Information**

### **Maintaining the Information Based on Classification**

#### High Risk Compliance Requirements

- Employees should provide appropriate access control on classified information stored within electronic storage media.
- Employees should manage electronic storage media appropriately in accordance with the classification of the information stored.
- For written documents containing information that is input into or output from information systems, employees should manage the written document containing confidential information or important specifications.
- Employees should consider if encryption is required when he or she stores confidential information within electronic storage media. If it is required, he or she should encrypt it.
- Employees should consider whether performing an electronic signature is required if he or she stores critical information within electronic storage media. If it is required, then he or she should perform an electronic signature.
- For electronic records or important specifications that are either critical or vital information, employees must consider whether making a backup or copy is required. If it is required, then he or she must make a backup or copy.
- For back-ups or copies of electronic records or important specifications that are
- Either critical vital information, employees must consider whether contingency planning is required. If so, then he or she must take appropriate measures to prevent all disaster.

## **Information Retention Period**

### High Risk Compliance Requirements

- Employees must keep information stored within electronic storage media until the retention period expires if such a period is set and delete it without delay if the period does not require extension.

## **6.1.4 Transfer of Information**

### **Gaining Approval and Notification of Information Transfer**

#### High Risk Compliance Requirements

- Employees must gain approval from their manager and/or the ISO if he or she transfers confidential High Risk information, integrity information, availability information, or important specifications.
- Employees must notify their manager or the ISO if he or she transfers electronic records of information as well as availability information or written documents including confidentiality information. However, this notification is not required for information transfer for which the manager and/or ISO deems unnecessary.

### **Selecting Between Transmitting and Transporting the Information**

#### Confidential Requirements

- Employees should select to transmit or transport electronic records of confidential information in consideration of safety and notify their manager and/or the ISO. However, this notification is not required for transfer of electronic records of confidentiality of public information and integrity as well as availability for which the manager and/or ISO deems unnecessary.

### **Selecting the Transfer Means**

#### Confidential Requirements

- Employees should select the means to transfer confidential information or important specifications in consideration of safety and notify their manager and/or the ISO.

### **Protecting Printed Information**

#### Confidential Requirements

- If an employee transports a written document including confidential information or important specifications, he or she must take appropriate security measures in accordance with the classification of information, etc.

### **Protecting the Electronic Records**

#### Confidential Requirements

- If an employee transfers electronic records of confidential information, he or she must consider whether protection by password is required. If it is required, then he or she must set a 13 alpha-numeric, special character password.

- If an employee transfers electronic records of confidential information, he or she must consider whether encrypting the information is required. If it is required, then he or she must encrypt it utilizing AES.
- If an employee transfers electronic records of confidential information, he or she must consider whether performing an electronic signature is required. If it is required, then he or she must perform an electronic signature to the information.
- If an employee transfers electronic records of confidential information, he or she must consider whether back-ups are required. If they are required, then he or she must make a backup of the information.
- If an employee transfers electronic records of vital information, he or she must consider whether any measures are required, such as transferring the same electronic records on different routes so as to prepare for a possible hindrance due to lost or missing data or delays in transfer to the destination. If it is required, then he or she must take necessary measures.

#### High Risk Compliance Requirements

- If an employee transfers electronic records of confidential information, he or she must encrypt it in a way that provides the encryption strength required, split it into pieces, and transfer it using different routes.

## **7 Measures Based on Clarifying Information Security**

### **7.1 Information Security Function**

#### **7.1.1 Authentication Function**

##### **Introducing Authentication Functions**

#### Confidential Requirements

- The ISO must consider whether authentication is required for every information system. The information system that handles classified information requires authentication.
- The ISO must provide functions for identification and authentication for the information systems for which authentication is required.
- If authentication information must be kept secret, the information system administrator must keep the authentication information unknown to others for the information systems for which authentication is required.
  - The authentication information must be encrypted if it is stored.
  - The authentication information must be encrypted if it is communicated.
  - If the authentication information cannot be encrypted if it is stored or communicated, the user must be notified that it is not encrypted when he or she sets, changes, or provides (enters) authentication information.
- For information systems where authentication is required, the ISO must establish a function to prompt users to change authentication information periodically if he or she requires such changes to users along with either of the following functions:
  - A function to check whether users change the authentication information periodically
  - A function to refuse continued use of the information system if users do not change the authentication information periodically
- For information systems for which authentication is required, the ISO should establish a function to stop authentication using the relevant authentication information or authentication information storage device or to stop use of information systems using a corresponding identification code if he or she recognizes that the authentication

- information or authentication information storage device is used or can be used by another party.
- For information systems for which authentication is required, the ISO should establish the following functions:
    - A function to let users set their own authentication information
    - A function to keep the authentication information set by users in a state that other parties cannot know easily
  - For information systems where authentication is required, the information system administrator must meet all the applicable requirements if he or she uses an authentication method other than that based on knowledge, ownership, or biological information, after examining whether the following are applicable or not in defining the requirements.
    - Any subject other than the legitimate subject must not be accepted (prevention of incorrect permission).
    - The legitimate subject must not be denied for any reasons for which it is not responsible (prevention of false denial).
    - The legitimate subject must not be able to grant (including issuance, renewal, and change hereinafter the same in this section) or lend its authentication information to other parties easily (prevention of substitution).
    - The authentication information must not be easily duplicated (prevention of duplication).
    - There must be means to invalidate logons individually at the discretion of the information system security administrator (assurance of invalidation).
    - The authentication must be available whenever necessary without any interruption (assurance of availability).
    - In the case that any information or device needs to be provided from outside to add new subjects, such information or devices can be sufficiently provided during the life of the information system (assurance of continuity).
    - The authentication information must be able to be re-issued to the legitimate subject in a secure manner if the authentication information granted to it cannot be used (assurance of re-issuance).
  - The information system administrator must not use relevant biological information for purposes other than those agreed to by the user if he or she uses authentication methods based on biological information. He or she should be careful not to invade the privacy of the user when using the relevant biological information.

#### High Risk Compliance Requirements

- For information systems where authentication is required, the information system administrator should establish a function to perform multiple authentication methods.
- For information systems where authentication is required, the information system administrator must establish a function to notify users of their last login. The following functions should be established:
  - A function to let the users set their own authentication information
  - A function to keep the authentication information set by the users in a state in which other parties cannot easily know it.
- For information systems where authentication is required, the information system administrator must meet all applicable requirements if he or she uses an authentication method other than that based on knowledge, ownership, or biological information after examining whether the following are applicable in defining the requirements:
  - Any subject other than the legitimate subject must not be accepted (prevention of incorrect permission).
  - The legitimate subject must not be denied for any reasons for which it is not responsible (prevention of false denial).

- The legitimate subject must not be able to grant (including issuance, renewal, and change; hereinafter the same in this section) or lend its authentication information to other parties easily (prevention of substitution).
- The authentication information must not be easily duplicated (prevention of duplication).
- There should be means to invalidate logons individually at the discretion of the information system administrator (assurance of invalidation).
- The authentication must be available whenever necessary without any interruption (assurance of availability).
- In the case that any information or device needs to be provided from outside to add new subjects, such information or devices can be sufficiently provided during the life of the information system (assurance of continuity).
- The authentication information must be able to be re-issued to the legitimate subject in a secure manner if the authentication information granted to it cannot be used (assurance of re-issuance).
- The information system administrator must not use relevant biological information for purposes other than those agreed to by the user if he or she uses authentication methods based on biological information. He or she must be careful not to invade the privacy of the user when using relevant biological information.

#### High Risk Compliance Requirements

- For information systems where authentication is required, the information system administrator must establish a function to perform multiple authentication methods.
- For information systems where authentication is required, the ISO must establish a function to notify users of their last login.
- For information systems where authentication is required, the ISO must establish a function to detect or prevent any attempts at illegitimate logon.
- For information systems for which authentication is required, the information system administrator must establish a function to display a notification about the use of the information system before user login to the information system.
- For information systems for which authentication is required and in the case that the user requires periodic changes in authentication information, the ISO must establish a function to prevent the users from re-using the same authentication information as previously used.
- For information systems for which authentication is required and in the case that the identification code with administrative rights is shared, the ISO must establish a function to require that users logon using an individual identification code before they login using the shared identification code.

#### **Identification Code Handling**

##### Confidential Requirements

- Employees should not use the information system using an identification code other than the identification code granted to him or her.
- Employees must not grant or lend the identification code granted to him or her to other parties.
- Employees must not leave the identification code that has been granted to him or her in a state in which it can be known by parties who do not need to know it.
- Employees must notify the information system security administrator if he or she does not need to use their identification code any longer. However, this reporting is not always required if the ISO has stated that individual reporting is not required.

#### **Authentication Information Handling**

### Confidential Requirements

- If authentication information is used or can be used by others, employees must report this to the ASU Help Desk or the information system security administrator immediately.
- If the ASU Help Desk or the information system security administrator receives a report that authentication information has been used or can be used by others, he or she must take necessary measures.
- If an employee uses authentication methods based on his or her personal authentication credentials, he or she must meet the following:
  - The employee must keep his or her authentication information unknown to others in handling.
  - The employee must not share his or her authentication information with others.
  - The employee must try to remember his or her authentication information.
  - The employee must select authentication information that cannot be easily guessed.
- If an employee is instructed to change their authentication information periodically by other security standards, he or she must do so.
- If an employee uses authentication methods based on ownership, he or she must meet the following requirements:
  - The employee must take security measures so that the authentication information storage device is not used in an unintended manner.
  - The employee must not grant or lend his or her authentication information storage device to others.
  - The employee must not lose the authentication information storage device. If it is lost, he or she must report this to the ASU Help Desk or the information system security administrator.
- If an employee does not need to use the authentication information storage device any longer, he or she must return this to his or her manager or the information system security administrator.

## **7.1.2 Access Control Function**

### **Introducing the Access Control Functions**

#### Confidential Requirements

- The ISO should consider whether access control is required for every information system. He or she should determine if an information system that handles classified information requires access control.
- For the information systems where access control is required, the ISO should establish a function to provide access control.

#### High Risk Compliance Requirements

- For information systems where access control is required, the ISO must add a function to provide access control based on the attributes other than those of the user and the group the user belongs to.
- For information systems where access control is required, the ISO must establish a function for Mandatory Access Control (MAC).

### **Configuring Access Control**

#### Confidential Requirements

- Employees must configure necessary access control using the functions installed on the information system in accordance with the classification and marking of the information stored in the information system.

### 7.1.3 Administration Function

#### Introducing the Administration Functions

##### Confidential Requirements

- The ISO should consider whether administration is required for every information system. He or she should decide if an information system that handles classified information requires administration.
- For information systems where administration is required, the ISO must establish a function to provide this administration.

##### High Risk Compliance Requirements

- For information systems where administration is required, the ISO must establish a function of the least privilege.
- For information systems where administration is required, the ISO must establish a function to re-issue authentication information automatically.
- For information systems where administration is required, the ISO must establish a dual locking function.

#### Granting and Managing Identification Code and Authentication Information

##### Confidential Requirements

- For information systems where administration is required, the ISO must decide to approve or disapprove the use of the shared identification code for each information system.
- For information systems where administration is required, the ISO must clearly establish the procedures for administration including the following:
  - A procedure to validate the applicant is the legitimate subject if a subject makes a request for administration
  - The initial distribution procedure and the change manager procedure of authentication information
  - The setting procedure and the change control procedure for access control information
- For information systems where administration is required, the ISO must provide training for the person responsible for the administration.
- The administrator must issue identification codes and authentication information only to the subject that has gained approval to use the information system.
- If the administrator issues an identification code, he or she must notify the users whether the code is shared or not.
- The administrator must grant (including issuance, renewal, and change; hereinafter the same in this section) the identification code with administrative rights only when such identification codes are required to execute business or business responsibilities.
- The administrator must invalidate the identification code of an employee if the employee does not need to use it any longer. He or she must check whether unnecessary identification codes exist if he or she adds or deletes an identification code due to personnel changes, etc.
- Employees must return the authentication information storage device provided to their administrator when he or she no longer needs to use it.

- The administrator must configure access control only within the minimum necessary scope considering business responsibilities and needs. He or she must check whether inappropriate access control settings exist in if he or she adds or deletes an identification code due to personnel changes, etc.

#### High Risk Compliance Requirements

- The administrator must grant a single identification code to employees for a single information system.
- The administrator must keep a record of employees that have been granted identification codes. If the administrator destroys the record, he or she must gain approval from the ISO in advance.
- The administrator must not grant an identification code that has already been granted to another person.

### **Applying Alternative Measures for Identification Code and Authentication Information**

#### Confidential Requirements

- For information systems where administration is required and the information system security administrator receives a request for approval from an employee to use an alternative measure because the employee cannot use their identification code, he or she must confirm that the applicant is a legitimate user and consider whether the alternative measure is required. If it is required, he or she must provide it.
- For information systems where administration is required and the ISO or the information system security administrator receives a report of unauthorized use of an identification code, he or she must invalidate system use with that identification code.

### **7.1.4 Audit Trail Management Function**

#### **Introducing the Audit Trail Management Functions**

#### Confidential Requirements

- The ISO should consider whether audit trails are required for each information system.
- For information systems where audit trails are required, the ISO must establish a function to collect the audit trails.
- For information systems where audit trails are required, the ISO must define information items for each event in order to collect the audit trails and the retention period of the audit trails.
- For information systems where audit trails are required, the ISO must define a strategy to deal with cases where the audit trails cannot be obtained or may be unobtainable and establish a function to handle the situation for the information system as needed.
- For information systems where audit trails are required, the ISO must provide access control to prevent the obtained audit trails from being deleted, falsified, or accessed illegally.

#### High Risk Compliance Requirements

- For information systems where audit trails are required, the ISO must establish a function to aid automatic checking, analyzing, and reporting of the audit trails for the information system.
- The ISO must establish a function on the information system to notify any events that indicate possible information security infringement to the monitoring personnel, etc. immediately if such events are found in the obtained audit trails.

## **Obtaining and Keeping the Audit Trails**

### Confidential Requirements

- For information systems where audit trails are required, the information system administrator must record the audit trails using the function established for the information system by the ISO.

## **Studying, Analyzing and Reporting the Obtained Audit Trails**

### High Risk Compliance Requirements

- For information systems where audit trails are required, the ISO or information system security administrator must study and analyze the obtained audit trails periodically or as needed, then take necessary information security measures or report to the ISO.

## **Notifying the Users about Audit Trail Management**

### Confidential Requirements

- For information systems where audit trails are required, the ISO or the information system security officer must explain that the audit trails can be obtained, maintained, checked, and analyzed to the information system security administrator and users in advance.

## **7.1.5 Assurance Function**

### **Introducing the Assurance Functions**

#### Confidential Requirements

- The ISO must consider whether assurance measures are required for information systems that handle classified information.
- For information systems where assurance measures are required, the ISO must establish the assurance functions.

## **7.1.6 Encryption**

### **Development of Systems for Encryption**

#### Confidential Requirements

- The ISO must define the algorithm and implementation system for encryption for the University.
- If a University entity selects an algorithm, they must examine required security and reliability and select an algorithm contained in the encryption list recommended by industry best practices if possible.
- For the encryption key (excluding written documents; hereinafter the same) or to perform an electronic signature, the ISO must define production procedures, the expiration date, disposal procedures, renewal procedures of the key, and procedures to deal with problems if the key is exposed (hereinafter referred to as "management procedures, etc. of the key").

#### High Risk Compliance Requirements

- The ISO must define a method used for creating a backup of the key used to decrypt the encrypted information or a method to escrow the key (hereinafter referred to as “backup method, etc. of the key”).

### **Introducing the Functions for Encryption**

#### Confidential Requirements

- The ISO must consider whether encryption functions are required for information systems that handle confidential information (except written documents; (hereinafter the same in this section).
- For information systems where encryption is required, the ISO must establish a function to provide encryption.
- The ISO should consider whether performing an electronic signature is required for the information systems that handle critical information.

#### High Risk Compliance Requirements

- For information systems that require encryption, the ISO must configure the cryptographic module as a component of application so that it can be replaced.
- For information systems that require encryption or an electronic signature, the ISO must allow for the selection of AES key length.

### **Management of Encryptions and Electronic Signatures**

#### Confidential Requirements

- For information systems that require an electronic signature, the ISO must provide the information or a measure to validate the electronic signature to the signature examiner.

#### High Risk Compliance Requirements

- If the ISO decides that an encryption or an electronic signature is required, he or she must collect information about the compromise risks of the algorithm selected for the information system as needed.

## **7.2 Threats to Information Security**

### **Building the Information Systems**

#### Confidential Requirements

- For applications, computers and communication equipment (except computers and communication equipment without announced security hole information; hereinafter the same in this section), the ISO must collect and document device information required to respond to security holes.
- The ISO must take measures to respond to the announced security holes relating to software used in computers or communication equipment when such computers or communication equipment are built or start operating.

#### High Risk Compliance Requirements

- For information systems that handle vital information, the ISO must install computers and communication equipment in a redundant configuration so that the services can continue to be provided without disruption when action is taken in response to security holes.
- The ISO must take available measures for computers and communication equipment even in the event that there is no information about the announced security holes.

## **Operating the Information Systems**

### Confidential Requirements

- The ISO must update the documents that include device information required to respond to the security holes in the case that the configuration of application, computers and communication equipment has been changed.
- The information system security administrator must obtain information about the announced security holes relating to software used on the computers and communication equipment that he or she is responsible for as needed. He or she must provide the following information for security holes:
  - Need of response
  - Response procedure
  - Temporary workaround procedure if no response procedure exists
  - Effects of response or temporary workaround procedures on the information systems
  - Response implementation schedule
  - Need of response testing
  - Response testing procedure
  - Response testing plan
- The information system security administrator must take measures against security holes based on risk.
- The information system security administrator must record items including date, work description, and worker for the measure against security holes that have been taken.
- The information system security administrator must obtain a file to use to solve the problem of security holes such as a patch or updated software version, etc. (hereinafter referred to as “security update file”) in a reliable manner. He or she must also validate the integrity of the security update file in the case that any validation procedure is provided (i.e. MD5 hash).
- The information system security administrator must investigate and analyze measures for security holes and software configurations periodically and respond when he or she finds any computers or communication equipment in an inappropriate state.
- The ISO must share the obtained information about the security holes and measures with other University entities as needed.

### **7.2.1 System Builds**

#### **Building the Information Systems**

##### Confidential Requirements

- The ISO must take measures to prevent the information systems (limited to information systems with computers, communication equipment or communication lines connected to communication lines extending out of the University facility such as Internet-related lines; hereinafter the same in this section) from being used as a system build.
- The ISO must build the information system so that the impact would be minimized in the case that the information system is used as a system build.

##### High Risk Compliance Requirements

- The ISO must define the monitoring procedure to monitor whether the information system is being used as a stepping-stone and the retention period of the monitoring records.

### **Operating the Information Systems**

#### Confidential Requirements

- The information system security administrator must monitor the information system in accordance with the monitoring procedure and keep the monitoring record.

## **7.3 System Requirements of Information Systems**

### **7.3.1 System Requirements of Information Systems**

#### **Planning and Designing the Information Systems**

##### Confidential Requirements

- The ISO must require the person who is responsible for information systems to establish the system to maintain security throughout its lifecycle.
- The ISO must decide the security requirements of the information systems.
- The ISO must define the measures in purchasing (including leasing) equipment, etc., developing software, configuring information security functions, protecting against information security threats, and handling measures for components of information systems in order to meet the security requirements of information systems.
- If the ISO recognizes any important security requirements for the information system to be built, a security target (ST) evaluation and confirmation to the third-party organization for the relevant information system should be requested. However, if the information system is updated or the specification changes in the process of development and changes in important security requirements are found to be only minor in the reviewed security target, such evaluation and confirmation are not always required.
- The ISO must define the installation procedure and environmental requirements in terms of information security when the information system is built and goes into the operation phase.

##### High Risk Compliance Requirements

- If the ISO recognizes any important security requirements for the information system to be built, he or she must define the required security function for the device and software products to be procured based on the security function designed to meet the requirement system.

#### **Building, Operating and Monitoring Information Systems**

##### Confidential Requirements

- The information systems administrator must use the information security measures that have been formulated based on the security requirements to build, operate, and monitor information systems.

#### **Moving and Disposing of Information Systems**

##### Confidential Requirements

- If the information system administrator moves or disposes of an information system(s), he or she must consider whether deleting or saving the information or disposing or reusing the information systems is required and take appropriate measures in either case.

## **Reviewing Information Systems**

### Confidential Requirements

- The ISO must consider, as appropriate, whether reviewing the information security measures for information systems is required. If it is required, then he or she must carry out the review and take appropriate measures.

## **7.4 Computers**

### **7.4.1 Basic measure for Computers**

#### **Installing Computers**

##### Confidential Requirements

- The ISO must establish the rule(s) to maintain computer security.
- The ISO must establish the document to identify the responsible employees and users of every computer.
- For computers that handle vital information, the ISO must consider and ensure the system capabilities to provide the performance required from the relevant computer in the future.
- The ISO must consider whether any information security function is necessary for the computer or not.
- The ISO must set the relevant function(s) for computers where an information security function is required.
- The ISO must take measures to protect computers against announced security holes that exist in the operating system and applications running on the computer (with the exception of those without announced security hole information).
- The ISO must take measures to protect computers (with the exception of those computers that do not have antivirus software, etc.) against malware.
- The ISO must establish the documents used for computers.
- For information systems that handle classified information, the information system administrator must locate the computer in a secure area. However, this is not required for mobile PCs in the case that he or she gains approval from the ISO.

##### High Risk Compliance Requirements

- For the computers that handle vital information, the information system administrator must install the computers that are required to provide services in a redundant configuration.

#### **Operating Computers**

##### Confidential Requirements

- The information system administrator must manage operation of computers based on the rule to maintain security.
- The ISO must review the rule to maintain computer security appropriately. If there are any changes to the relevant rule, he or she must record it.
- Employees must not use computers for purposes other than executing his or her tasks.

- In the case that the information system administrator has changed the responsible employees and/or computer users, he or she must update the document to identify the new responsible employees and/or computer users. He or she must also record such changes.
- The information system administrator must take measures to protect computers against announced security holes to maintain an appropriate computer security level.
- The information system administrator must take measures to protect computers against malware to maintain an appropriate computer security level.
- If the information system administrator has changed a computer's configuration, he or she must update the documents used for those computers with the changes made. He or she must also record such changes.

#### High Risk Compliance Requirements

- The information system administrator must periodically examine the state of each item of software used on the computers within his or her control and make improvements if any computers are found to be in an inappropriate state.

## **7.5 Application Software**

### ***7.5.1 Common Measures for Applications provided via Communication Line***

#### **Installing the applications**

##### Confidential Requirements

- The ISO must define the rule(s) to maintain security of the services to be provided via a communication line.
- Applications must not run transport encryption within applications; this should always be performed in infrastructure.

#### **Operating the applications**

##### Confidential Requirements

- The information system administrator must operate and manage systems daily and periodically based on the rule related to the maintenance of security of the services.
- The employee must not use the services that are provided via a communication line for non-business purposes.

### ***7.5.2 Email***

#### **Introducing E-mail Service**

##### Confidential Requirements

- The information system email administrator should configure e-mail servers so that unsolicited bulk e-mail cannot be relayed.

#### High Risk Compliance Requirements

- The information system e-mail administrator should establish a function to authenticate employees when e-mail clients send or receive messages to or from the e-mail server.

### **Operating E-mail Service**

#### Confidential Requirements

- If an employee sends or receives e-mail messages containing business information, he or she must use the e-mail service provided by the e-mail server that is operated or outsourced by the University that he or she belongs to. However, this is not always required if he or she has gained approval for information processing in unsupplied information systems.
- Employees must display any e-mail message he or she receives as text in the e-mail client.

### **7.5.3 Web**

#### **Introducing the Web**

##### High Risk Compliance Requirement

- If users enter strings, etc. in the services provided using Web servers, the information system administrator should sanitize input data.
- The information system administrator must build the information systems so that Web servers do not send any information that could be utilized in attacks to Web clients.
- For information systems that handle high risk information, the information system administrator must identify the information to protect against sniffing and consider if encryption is required. If it is required, then he or she must encrypt the information for the services provided using Web servers.

##### Confidential Requirements

- For information systems that handle confidential information, the information system administrator must identify the information to be stored on Web servers and confirm that the relevant servers do not contain any confidential information.
- The information system administrator must use the digital certification to ensure the validity of Web servers.

#### **Operating the Web**

##### High Risk Compliance Requirements

- If an employee downloads software to a computer on which a Web client is running, he or she must confirm the source of the software using an electronic signature.

##### Confidential Requirements

- The information system administrator must limit the Web pages from outside the University that employees can browse and review the limit periodically.

## **7.6 Data Communication**

### **7.6.1 Common Measures for Communication Lines**

## Building Communication Lines

### Confidential Requirements

- The ISO must establish the rule related to the maintenance of security of communication lines and communication equipment (Section XX).
- If the information system administrator builds a communication line, he or she must consider the risks in doing so.
- For information systems that handle vital information, the information system administrator must consider and ensure the system capabilities to provide performance required for the relevant communication lines and communication equipment for the future.
- The ISO must establish the documents to be used for the communication lines and communication equipment.
- For all communication lines and equipment, Network Operation Management must establish the documents to specify the persons who manage them.
- Network Operation Management must define the software necessary for communication equipment to be operated. However, this is not required in the case of communication equipment for which it is difficult to change software.
- Network Operations Management should group the computers that are connected to the communication line and separate them on that communication line.
- Network Operation Management should consider the communication requirements among the grouped computers, use the communication equipment and provide access and route control in accordance with communication requirements.
- For information systems that handle confidential information, the required encryption of confidential information sent or received using the communication line must be considered. If it is required, then he or she must encrypt it.
- For information systems that handle classified information, Network Operation Management should consider the security of physical lines used for the communication line and select appropriate ones.
- Network Operation Management must ensure security of the connections that are used in the services for remote maintenance or diagnosis work for the communication equipment.
- Network Operation Management should take measures to protect communication equipment against announced security holes in the communication changes on the security of the communication line and take appropriate measures.
- If the security of an information system is difficult to ensure, Network Operation Management must change the communication line from the shared configuration to an independent and closed configuration.
- Employees must not connect computers and communication equipment that are not approved by Network Operation Management to the communication line.
- Network Operation Management should take measures to protect communication equipment against announced security holes to maintain an appropriate security level for the communication equipment.
- Network Operation Management should synchronize the time of the communication equipment with the standard time of the information systems.

### High Risk Requirements

- Network Operation Management must periodically examine the conditions of all software necessary for the operation of communication equipment that he or she is responsible for. When equipment under inappropriate conditions is found, then he or she must work to improve the relevant inappropriate conditions. However, this is not required for communication equipment of which it is difficult to change software.

## Disposing of Communication Lines

### Confidential Requirements

- If Network Operation Management disposes of communication equipment, he or she must delete all information stored within the electronic storage media of the communication equipment.

## **8 MEASURES FOR INDIVIDUAL CONSIDERATION**

### **8.1 Information Security Measures for Procurement and Development**

#### ***8.1.1 Purchasing the equipment, etc.***

##### **Scope**

This applies to purchases (including leases; hereinafter the same) of equipment, etc.

##### **Establishing the Mechanism to Ensure University-Wide Information Security**

### Confidential Requirements

- The ISO must formulate the selection criteria for the equipment, etc.
- The ISO must formulate the confirmation and test procedure for the equipment, etc. in terms of information security measures.

##### **Procedures for Purchasing the Equipment, etc.**

### Confidential Requirements

- If a University entity selects equipment, etc., they should consider whether the equipment, etc. meets their selection criteria and utilize the results to make a selection.
- If the equipment, etc. is delivered, the University entity must confirm that the delivered equipment, etc. meets the selection criteria for the equipment, etc. and add the confirmation to the inspection.
- The University entity should consider whether information security maintenance and check-ups are required after the equipment, etc. is delivered. If it is required, the University entity must clarify the maintenance and check-up requirements and sign an agreement with the manufacturer of the equipment, etc. or other service provider.
- If there are required specifications for security functions to satisfy the security requirements and the purchase is made by a comprehensive evaluation of bidders, the ISO must select the equipment, etc. based on whether it is certified according to the Industry Information Security Evaluation and Certification Scheme.

#### ***8.1.2 Outsourcing***

##### **Scope**

This applies to information processing tasks based on outsourced job functions and on requirements that stipulate leases, contracts, and other agreements, including the following:

- Software development (programming, system development, etc.)
- Information processing (statistics, tabulation, data entry, media conversion, etc.)
- Leasing
- Examination and research (examination, research, investigation, etc.)

## **Establishing the Mechanism to Ensure Information Security Common Across all University Entities.**

### Confidential Requirements

- The ISO must establish the criteria to determine the scope of information systems that can be outsourced and the scope of information assets that may be accessed by contractors.
- The ISO must establish the selection procedure and selection criteria.

### High Risk Compliance Requirements

- The ISO must establish the procedure to evaluate the information security level of a contractor(s) based on international standards (URL) to select a contractor more stringently.

## **Clarifying the Information Security Measures to be Implemented by Contractors**

### Confidential Requirements

- The University entity with assistance from the ISO must clarify the information security measures that a contractor(s) must implement in outsourced work and notify the candidate contractors in advance.
- The University entity with assistance from the ISO must formulate the response procedure in the event that information security is violated in contracted work and notify the candidate contractors in advance.
- The University entity with assistance from the ISO must establish a procedure to check how well information security measures are implemented by the contractor(s) and the response procedure in the event of poor implementation, and notify them to the candidate contractors in advance.

## **Selecting an Outside Contractor**

### Confidential Requirements

- The University entity with assistance from the ISO must select a contractor based on the selection procedure and selection criteria .

### High Risk Compliance Requirements

- The University entity with assistance from the ISO must check the information security level of candidate contractors in accordance with the procedure to evaluate the information security level of the contractor based on international standards and utilize it to make a selection.

## **Contracts Pertaining to Outsourced Work**

### Confidential Requirements

- The University entity with assistance from the ISO must sign an outsourcing agreement with contractors that stipulates implementation of information security measures in the contracted work, nondisclosure (including prohibiting use of information for non-business purposes), response procedures in the event of information security breaches,

procedures to check implementation of information security measures, and response procedures in the event of poor implementation of information security measures. The University entity should include the following the agreement as needed:

- Steps to make the contractor(s) undergo an information security audit
- Steps to make the contractor(s) secure a service level
- The University entity with assistance from the ISO must clarify the responsibilities of both parties for the outsourcing agreement, build consensus, and request the contractor(s) present a confirmation note, etc. on how information security measures will be implemented and managed. The University entity should also include the following description in the confirmation note, etc. as needed:
  - Specification of the person(s) who engages in the outsourced work
  - Detailed work that the person(s) does in order to implement information security measures
- The University entity with assistance from the ISO must judge whether to renew the outsourcing agreement based on the selection procedure and selection criteria on a case-by-case basis but must not take the decision to renew lightly.
- The University entity with assistance from the ISO must consider whether to change the services that are provided by the contractor(s) (including maintaining and improving the basic policy for information security, operation procedures, and management procedures) based on the selection procedure and selection criteria.
- The University entity with assistance from the ISO must prohibit the contractor from subcontracting all or part of the outsourced work to a third party. However, this is not always required if the University entity with assistance from the ISO receives explanations from the contractor and decides that the explanation ensures that information security measures will be taken to protect against the potential dangers from subcontracting.

## **Procedures in Implementing the Outsourcing**

### Confidential Requirements

- If an employee provides classified information or important specifications to a contractor, he or she must provide only the minimum necessary information and take the following measures:
  - If the employee provides information to a contractor, he or she must provide it in a safe delivery method and record the provision of the information.
  - If the provided information becomes unnecessary for a contractor due to the termination of the outsourcing, etc., the employee must have the contractor return, dispose of, or delete the information without fail.
- If information security is violated in contracted work, the University entity with assistance from the ISO must have the contractor(s) take necessary measures in accordance with the defined response procedure.
- The University entity with assistance from the ISO must check how information security measures are implemented by a contractor in accordance with the defined procedure.

## **Procedures to Terminate the Outsourcing**

### Confidential Requirements

- The University entity with assistance from the ISO must confirm the information security measures implemented in the outsourced work when he or she terminates the outsourcing and adds the confirmation to the inspection.

### **8.1.3 Software Development**

#### **Establishing the Software Development System**

##### Confidential Requirements

- The ISO should require that the person responsible for information systems establish the system for software development designed to comply with information security measures (to meet compliance requirements of High Risk, and Confidential data elements).
- If the ISO outsources software development, he or she must select necessary information security measures (or compliance requirements of High Risk, and Confidential data elements that should be implemented by a contractor and ensure that such implementation is assured by the contractor(s).

#### **Starting Software Development**

##### Confidential Requirements

- The ISO must define the procedure and environment for each phase of software development in terms of information security.
- The ISO must consider whether separating the information system that is used for software development and testing from the operating system is required in terms of information security. If it is required, then he or she must separate them.

#### **Designing the Software**

##### Confidential Requirements

- The ISO should consider whether security functions are required. If required, then ISO must design the function appropriately and clearly describe it in the design document based on the analysis of measured dangers connected with the information assets to be used in the operation of the software to be developed and the classification of information that is handled by the software.
- The ISO should consider whether a function to manage the security functions for operation of the software to be developed is required. If required, then ISO must design the management function appropriately and clearly describe it in the design document.
- The ISO should define the scope and procedure of review to confirm the validity of information security in software design and review it accordingly.
- The ISO should consider whether a function to confirm the validity of information security in the data processed or input-output by the software to be developed is required. If required, then ISO must design the function appropriately and clearly describe it in the design document.
- If there are any important security requirements for the software to be developed, the ISO must request a security target (ST) evaluation and confirmation by the third-party organization for the purposes of designing security functions to meet them. However, in the event that he or she undergoes the ST evaluation and confirmation for the information system that contains the relevant software, updates the software, or the specification changes in the process of development and the changes in important security requirements are found to be only minor in the reviewed ST, such evaluation and confirmation are not always required.

#### **Developing the Software**

##### Basic Compliance Requirements

- The ISO should protect against unnecessary access and make a backup of the source code that is formulated by the software developer.
- The ISO must define the rule(s) for coding in terms of information security.
- The ISO must integrate security processes within university Software Development Lifecycle.

#### Enhanced Compliance Requirements

- The ISO must define the scope and procedure of review to confirm the validity of the formulated source code and review it accordingly.

#### **Testing the Software**

##### Basic Compliance Requirements

- The ISO should consider whether any testing is required in terms of information security.
- The ISO must record the test that is conducted in terms of information security.

## **9 ENFORCEMENT**

Any employee found to have violated this standard may be subject to disciplinary action up to and including termination of employment.