Tokyo University of Agriculture Information Security Policy

1. General Policy

In the current highly information-dependent society, it is essential to establish information security in order to improve the quality of education and research activities, and maintain effective administration at Tokyo University of Agriculture, hereafter referred to as TUA.

Tokyo University of Agriculture Information Security Policy, hereafter referred to as "IS policy", is defined in order for all members of TUA to correctly understand the importance of information security and to protect the information resources of TUA.

The IS policy aims to:

(1) prevent violation of information security at TUA,

(2) prevent acts of information security infringement to/from TUA,

(3) protect and manage information resources,

(4) provide a guideline for evaluation and improvement of information security.

2. Scope of Policy

The IS policy covers all information resources at TUA, including information systems and devices accessing the TUA information resources.

The IS policy applies to all users of information resources at TUA, including faculty (full-time/fixed term), staff (full-time/fixed term), short term employee, adjunct professor, temporary employee, assistant, contract employee, medical staff, researcher, all personnel working at TUA through an employment agency or work contract, graduate student, undergraduate student, research student, part-time student, technical trainee and others receiving training/education services, and temporary users including alumni, guardian, and visitor.

When an elementary school, junior high school, or high school within Tokyo University of Agriculture Educational Corporation is to be allowed access to information resources at TUA, the relevant school must define its own IS policy complying with the general policy defined in 1. General Policy.

3. Rules and Regulations regarding Policy

Personnel covered by the scope of the policy must comply with the IS policy, related TUA rules, regulations, guidelines, and related Japanese laws, regulations and practices.

4. Organization

(1) Information security chief supervisor (university president)

The information security chief supervisor is responsible for information security at TUA.

(2) Information security general supervisor (risk management vice-president)

The information security general supervisor takes charge of information security at TUA under the direction of the information security chief supervisor.

(3) Information security management supervisor (dean of graduate school, dean of faculty, administrative director)

The information security management supervisor is responsible for information security within the TUA campus.

(4) System management general supervisor (director of computer center, director of information center for education and research)

The system management general supervisor takes charge of maintenance and improvement of information security, to provide safe and smooth operation of the computer and network system at TUA.

(5) System management supervisor (manager or equivalent appointed by system management general supervisor)

The system management supervisor oversees system administrators under the direction of the system management general supervisor.

(6) System administrator (staff appointed by system management supervisor)

The system administrator manages the computer and network system under the direction of the system management supervisor.

5. Classification and management of information

Appropriate information security procedures are applied according to information classification based on importance.

6. Physical security

Physical security measurements will be implemented at locations of information

resource storage, and computer and network system hardware.

7. Human factor security

IS policy education and information security training will be implemented.

8. Technological security

Technological security measurements against violation and infringement of information security will be implemented.

9. Evaluation and Improvement

Information security management supervisors will periodically evaluate information security at TUA and if necessary propose improvements to the information security general supervisor.

10. Definitions of terms

(1) Information resources

Refers to all information and information management methods, including information systems, related documents, and electronic/magnetic stored data.

(2) Information system

Refers to the whole and components of the information system, including servers, computers, smart devices, network hardware, software, storage media and related documents.

(3) Information security

Maintaining the confidentiality, integrity and availability of information resources.

(4) Confidentiality

Allowing only permitted users to access information.

(5) Integrity

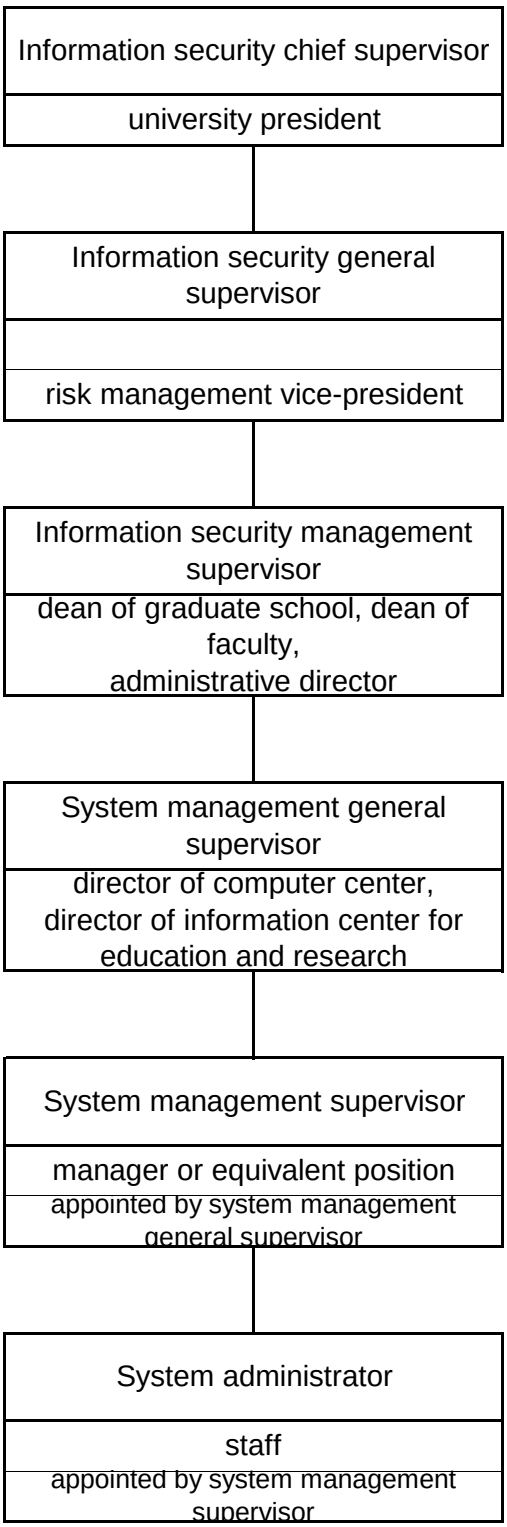
Ensuring the accuracy and consistency of the stored information. Protecting the information from damage, alteration, and deletion.

(6) Availability

Providing permitted users reliable access, continually without interruption, to information and related resources when requested.

Tokyo University of Agriculture Information Security Policy

Organization



The information security chief supervisor is responsible for information security at Tokyo University of Agriculture (TUA).

The information security general supervisor takes charge of information security at TUA under the direction of the information security chief supervisor.

The information security management supervisor is responsible for information security within the TUA campus.

The system management general supervisor takes charge of maintenance and improvement of information security, to provide safe and smooth operation of the computer and network system at TUA.

The system management supervisor oversees system administrators under the direction of the system management general supervisor.

The system administrator manages the computer and network system under the direction of the system management supervisor.