Kansai University Information System Use Regulations

Establishment: March 17, 2016

(Objective)

Article 1 The Regulations establish matters related to the use of information systems of Kansai University and schools established by the incorporated education institutions (hereinafter referred to as the "University") with the objective of ensuring information security and smooth use of the information system.

(Definition)

Article 2 The terms listed in the following clauses shall be defined and used in these Regulations as follows:

(1) Account: Rightful authority given to subjects in the information system that is recognized as requiring subject authentication. In the narrow sense, the term is defined as the combination of a user ID (identification code) given to users and password (subject authentication information), or one of the above.

(2) University-wide account: the account used for the information system corresponding to University-wide unified certification. The term also includes an account for the use of outsourced systems and services the University has a contract with.

(Range of application)

Article 3 The Regulations apply to members of the University and individuals who have been permitted to use the University's information system.

2. The University information system is a network, information devices and information service the University has set up and uses or receives service by contract. The term also includes devices connected to these services.

3. The University information system includes devices that store information rated by the Kansai University Document Handling Regulations.

(Matters of compliance)

Article 4 Users of the University information system must comply with these Regulations and the procedures related to the use of the University information system.

(ID and password)

Article 5 Users must comply with the following clauses regarding account management.

(1) Users may not allow others to use their account or disclose it to others.

(2) Users may not obtain or use the accounts of others.

(3) Users accessing the University information system from outside the University using their account must follow the established procedures. Users must also ensure that account leakage does not occur.

(4) Users whose accounts have been used by others or if there is a danger of such use, must immediately report the incident to the Center for Information Technology.

(5) Users who no longer need the system must report to the Center for Information Technology without delay. However, it does not apply if the Center for Information Technology has stipulated that reporting is unnecessary.

(6) Users must appropriately manage the account according to the guidelines established separately by the Center for Information Technology.

(Staff and Student ID (IC card))

Article 6 Users must manage their IC cards as follows:

(1) IC cards must be managed with safety precautions to prevent use by unintended individuals.

(2) IC cards may not be transferred or lent to others.

(3) Users must ensure that they do not lose their IC cards. If lost, it must be immediately reported to the Center for Information Technology

(4) In the event an IC card is no longer used, the card must be returned to the University without delay.

(Use of information devices)

Article 7 Users must comply with the clauses below when using information devices for the creation, use, and storage of information.

(1) When a user wishes to connect a new information device to the University information network, the user must obtain approval for connection from the Chief Information Security Officer (hereinafter referred to as "CISO") as stipulated in the Kansai University Information System Operation Basic Regulations. However, this does not apply to a temporary connection to the University information system through information consent or wireless LAN provided by the University, or when using a connection method designated by the Center for Information Technology.

(2) Users must report to the Center for Information Technology when canceling the use of an information device for which the permission was obtained.

(3) In the event the information device is equipped with an authentication system and log function, such function must be set up and operating. For devices with unauthorized software

countermeasure functions, said functions must be the newest versions to protect the system.

(4) Information devices must be at the newest version possible and not vulnerable to external infiltration.

(5) Users must implement measures to prevent information leakage.

(6) Users must exercise caution to prevent loss or theft of the information device.

(7) In the event of loss or theft of the information device, users must immediately report such to the relevant department.

(8) Users must take care to appropriately protect the information devices according to the guidelines prescribed separately by the Center for Information Technology.

(Obligation to attend information security measure education)

Article 8 It is desirable for users to attend a class regarding the use of the University information system once every year, according to the annual course schedule.

(Handling information)

Article 9 Users must handle rated information according to the method noted in the Kansai University Document Handling Regulations.

(Prohibited matters)

Article 10 Users shall not commit acts noted in the clauses below regarding the University information system.

(1) Use of the information system and information for purposes not stipulated

(2) Access into the University information system using the University-wide account from outside the University through undesignated methods

(3) Allowing use of the University information that has been designated to an individual not a member of the University

(4) Acts in breach of confidentiality

(5) Acts of discrimination, defamation, insult or harassment

(6) Acts violating personal information or privacy

(7) The creation, possession and distribution of malware

(8) Acts infringing on property rights, such as copyrights

(9) Acts infringing on confidential communications

(10) Use of the University information system for business or commercial purposes

(11) Acts disrupting the smooth operation of the information system by excessive load, etc.

(12) Acts violating unauthorized access prohibition law or similar act

(13) Other acts that are subject to punishment by other laws

(14) Acts that promote the acts in the previous clause

(Dealing with violations)

Article 11 In the event that an action is recognized as a violation of the previous article, the person in charge (supervisor) shall cooperate with the CISO to conduct an investigation to confirm the facts. For the confirmation of facts, interviews shall be conducted, to the extent possible, with the person suspected of said action.

2. In the event of the above, the person in charge shall report to the CISO without delay.

3. In the event a violation is revealed through the investigation, the person in charge may request that the CISO take the actions noted in the clauses below.

(1) Order of the cessation of the said act to the said individual

(2) Order to the department to cut off the transmission of information related to said act

(3) Order to the department to stop or delete the account of said individual

(Use of e-mail)

Article 12 In regard to the use of e-mail, users must follow the user guidelines and strictly comply with the ordinances as well as exercise proper etiquette.

(Use and disclosure of the Web including social networking services)

Article 13 Users must comply with the clauses below regarding the use of the Web and information disclosure through the Web.

(1) When doing website browsing, information transmission, file download, etc. by using a web browser, users must follow the user guidelines established separately by the Center for Information Technology.

(2) When creating and disclosing a web page, the user must exercise discretion to prevent it from damaging the social credibility of the University.

(3) In the event of a violation of the Regulations and guidelines for the web page and web server operation, the CISO may cancel permission for the disclosure and delete the web content.

(Use of the University information system from outside the University)

Article 14 Users accessing the University information system from outside the University must comply with the clauses below:

(1) Users accessing the University information system through their account from outside the University must do so according to the designated method.

(2) Users may not allow the use of the information system by persons without access permission.

(Safety management obligations)

Article 15 Users shall be aware that they are the primary responsible person for maintaining the safety of the information device they manage, regardless of the status of the connection to the University information network, and thereby follow the clauses below.

(1) Use the newest version of the software and malware countermeasure functions

(2) Do not open files suspected of being malicious programs by the malware countermeasure function.

(3) Enable automatic inspection function of the malware countermeasure function.

(4) Regularly check that no malicious programs exist in all electronic files with the malware countermeasure function.

(5) Check that no malicious software is present when downloading data or software into information devices from external sources, or when providing data or software outside.

(6) Always keep an eye open for the newest security information and prevent infection by malicious software.

(Incident response)

Article 16 When identifying incidents during the use of the University information system, users shall act according to the "Information Security Incident Response Procedure" established separately by the Center for Information Technology.

(Administration)

Article 17 The Information Technology Promotion Division shall perform the administration of these Regulations.

Supplementary Provision

These Regulations shall come into effect from April 1, 2016.

Supplementary Provision

These Regulations (revision) shall come into effect from April 1, 2018.