Guidelines for the Use of Information Devices

Center for Information Technology, Kansai University

1 Purpose of these Guidelines

The purpose of these guidelines is to mitigate the risks associated with security breaches and information leaks when using the university's information environment, including its network. These guidelines outline the necessary precautions that users should be aware of in advance to safely use information equipment.

2 Intended Audience for these Guidelines

These guidelines apply to all users (hereinafter referred to as "users") who utilize accounts within the university's information system, including the university's network.

3 Devices Covered by these Guidelines

These guidelines apply to IT equipment (hereinafter referred to as "information devices") such as personal computers, tablets, and smartphones.

4 Use of Information Devices

Users are required to adhere to the following conditions when using information devices:

(1) Do not engage in any activity that may cause physical damage to information devices.
(2) Do not allow individuals without accounts to use the information equipment, except in cases specifically approved by administrators for educational or research purposes, among others.
(3) Disable remote access for accounts with the necessary system management permissions (administrator accounts).
(4) Take theft prevention measures.
(5) Do not monopolize network bandwidth with the following actions:
  1) Using applications that frequently send query packets or similar data.
  2) Using streaming services that are not necessary for educational, research, or business purposes.
(6) When using shared computers in computer labs or similar facilities, follow the instructions provided by the facility (including the rules of each computer lab).

5 Installation and Use of Applications

Users must adhere to the following regulations when installing and using applications:

(1) Stay informed about vulnerability information related to the operating system and applications you are using and promptly address any software issues.
(2) Before downloading an application, ensure it is provided from an official website or a trusted source.
(3) Use the application in accordance with the terms and conditions of use.
(4) Install antivirus software and ensure that the virus information database is always up to date.
(5) Do not install or use applications that are not intended for educational, research, or business purposes on information devices purchased using public funds (e.g., shared computers in computer labs).

6 Security Measures

(1) Take precautions to prevent the leakage of authentication information (passwords and secret keys).
(2) When using external storage media such as USB drives or various memory cards, comply with the following conditions:
  1) Do not take personal information or educational data (such as grades and exam

questions) outside of the university.

2) If personal information or educational data (grades, exam questions, etc.) is not included, the use of USB drives is allowed. When storing data, take protective measures such as encryption and manage the encryption key appropriately.

3) When it is necessary to carry data containing personal information outside of the university for work-related purposes, avoid using external storage media, such as USB drives and webmail. Implement protective measures like encryption and use secure methods (e.g., Kansai University's file delivery service "KU File Post" or services contracted by the university, such as Microsoft 365 OneDrive) that ensure strict security.

(3) In case any of the following issues are discovered, promptly contact the Center for Information Technology:

1) When security vulnerabilities or malfunctions are found in the device's OS, applications, or the information system installed within the university.

2) When confidential information or personal data is exposed to an unspecified number of individuals.

3) When there is a leakage of personal or confidential information.

Supplementary Provisions

1. These guidelines shall be in effect from November 6, 2019.
2. These amended guidelines shall be in effect from October 4, 2023.