(Note: this English version is provided as a translation of the Japanese version, the original, for the user's convenience.)

Password Guidelines for Users of Kyoto University Campus-wide Accounts

(Effective from March 9, 2022, as established by the Chief of the Institute for Information Management and Communication)

1. Purpose

This guideline aims to provide users and others with essential information regarding the use of passwords for Kyoto University campus-wide accounts, in accordance with Article 2, Item 3 of the Kyoto University Campus-wide Account Usage Agreement (established on March 29, 2022, by the Chief of the Institute for Information Management and Communication).

2. General Cautions Regarding Passwords

2.1 Changing the Initial Password

Users and others are required to change their initial password immediately upon receiving it.

2.2 Password Composition

The password created by users and others must meet the following criteria:

- It must be at least 12 characters long.
- It must include at least one character from each of the following groups: A, B, and C. Additionally, it may contain characters from Group D.
    - A) Uppercase letters (A to Z)
    - B) Lowercase letters (a to z)
    - C) Numeric digits (0 to 9)
    - D) Symbols (e.g., "@", "!", "#", "%", etc., as specified separately by the Institute for Information Management and Communication)

The following password strings should be avoided, as they are easily guessable:

- a) Passwords that can be easily derived from the user's account information (e.g., name, user ID, etc.)
- b) Combinations of strings mentioned in a), or combinations of a) with numbers or symbols
- c) Words listed in dictionaries
- d) Names of celebrities or other proper nouns
- e) Simple keyboard patterns (e.g., qwerty123456)
- f) Repeated sequences (e.g., abcabc123123)

2.3 Changing a Password

Users and others must periodically change their passwords as instructed by the Chief of the Institute for Information Management and Communication. If immediate password change is mandated, it must be done promptly. The new

password must not resemble the previous password.

2.4 Password Management

Users and others must securely manage their passwords, taking utmost care to avoid disclosing them to others or allowing unauthorized access due to negligence.

2.5 Prohibition of Password Reuse

Users and others must not reuse passwords from their campus-wide account for other information system accounts they manage. Additionally, the password set for their campus-wide account should not be used for other information systems.

3. Password-related Procedures

3.1 Password Recovery

If users and others forget their password, they must request a password reset from the Institute for Information Management and Communication. Once the password is reset, immediate modification to a new password is required.

3.2 Reporting Password Incidents

If users and others discover any unauthorized use or potential threats to their account, they must promptly report the incident to the Chief of the Institute for Information Management and Communication.

Supplementary Provision

This guideline will be effective from March 9, 2022.