○The Ritsumeikan Trust Information System Usage Regulations

This English document is a machine translation of the Japanese version of The Ritsumeikan Trust Basic Regulations Concerning Information System Usage and Operation Management (Gakko Hojin Ritsumeikan Joho Shisutemu no Riyou oyobi Unyo Kanri ni kakawaru Kihonkitei).
The official text of the Regulations is the Japanese version.
If there are any contradictions between the Japanese version and this reference translation, the former shall prevail.

Article 1 : Purpose

These regulations provide for necessary matters concerning the appropriate use of the information system of the Trust in accordance with Article 5 of The Ritsumeikan Trust Basic Regulations Concerning Information System Usage and Operation Management (hereinafter referred to as "Basic Regulations").

Article 2 : Definition

1. In this regulations, the definitions of the terms listed in the following items shall be as prescribed respectively in those items:.

(1) The term "user" means any of the following persons who uses an Information System:.

(i) Faculty Member

(ii) Students and Children of a school established by a Trust

(iii) Any Other Person whom A Trust General Administrator has approved as a person using an Information System.

(2) Malware refers to malicious software that performs harmful or illegal actions such as interfering with the normal operation of an information system or the normal use of a user.

2. In addition to the preceding paragraph, the definitions of terms not specifically provided for in this regulation shall be in accordance with the provisions of the Basic Regulations.

Article 3 : Scope

These regulations apply to user.

Article 4 : Matters to be Observed

When using an information system, user shall comply with the following items:.

(1) Carefully manage user IDs and passwords to be used.
(2) Appropriate use of the Information System of the Trust.
(3) Follow these regulations, guidelines related to the use of information systems, rules for each information system to be used, etc.
(4) Take necessary measures against information security vulnerabilities and malware on devices connected to information systems.
(5) If an information security incident occurs, take prompt action according to the instructions of the Ritsumeikan CSIRT general manager.

Article 5：Prohibited
When using an information system, a user shall not perform any of the acts specified in the following items:.
(1) Unauthorized use, transfer or borrowing of user ID or password
(2) an act that violates the privacy or human rights of others
(3) act of destroying or stealing information about another or infringing on intellectual property rights
(4) Acts whose main purpose is business or any other profits
(5) act of seriously damaging the honor or reputation of the Trust
(6) Acts that hinder the proper operation and management of information systems
(7) Act in violation of laws and regulations or the provisions of the Trust
(8) The act of promoting the acts set forth in the preceding items
(9) Other inappropriate activities in the use of information systems

Article 6：Responding to Violations
1. When an act in violation of the preceding Article has occurred or is clearly likely to occur, the Trust General Administrator may investigate the case.
2. In cases where a violation has been found in the investigation, the Trust General Administrator may take the following measures:.
(1) To order the suspension of the offence.
(2) Suspension of use of the information system or deletion of the account involved in the violation.

Article 6-2：Responding to an information security incident
1.The Chief Information Security Officer may investigate if an information security incident has occurred or is likely to occur in the user.
2. The Chief Information Security Officer can take necessary measures in responding to an information security incident if the investigation determines that there is a risk of damage to other users or information systems.

Article 7 : Amendment
The amendment or abolition of these regulations shall be carried out by the Standing Council.

Supplementary Provisions (March 25, 2020 Partial amendment due to the establishment of information security measures promotion system)
This regulation will come into effect on April 1, 2020.