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

Guidelines on the Management of Logs of the Information System of Kyoto University

(Decided by the Director of
Institute for Information Management and Communication
On April 1, 2017)

I. Purpose

1. The purpose of these Guidelines is to clarify matters that should be complied with by department information security technical managers and department information system technical staff members regarding the handling of trials obtained, usage records collected from an information system, and records of events arising in an information system (hereinafter collectively “logs”) under Articles 85, 86, and 89 of the Kyoto University Information Security Program Standards (hereinafter the “Program Standards”) and Article 23 of the Rules for Using the Kyoto University Campus-wide Information System (hereinafter the “Use Rules”).
2. The purposes of log management are as follows:
(1) To detect and monitor illegal communications and activities for information security
(2) To detect abnormalities, such as failure of an information system, and to identify and monitor the state of abnormal processes
(3) To investigate and identify the cause of problems in an information system after any occurrence
(4) To implement use statistics (including reports) and usage analysis of an information system
(5) To certify events arising in an information system
3. These Guidelines do not cover the provisions of paragraph 2 of Article 89 of the Program Standards.

II. Definition

Unless otherwise prescribed in the Regulations on Information Security of Kyoto University (hereinafter the “Regulations”), the Program Standards, or the Use Rules, the following terms used herein have the meanings set forth in the respective items:
(1) *Events* mean the events arising in an information system or network.
(2) *Log management* means the life cycle management of logs, including their acquisition or collection (hereinafter “collection,” “collect,” “collecting,” or “collected”), storage, use, and disposal.
(3) *Storage of logs* means periodical archiving of logs made as part of the regular operational activities.

III. Covered Equipment and Log Classification

1. These Guidelines cover the following information systems:
(1) Campus-wide information systems
(2) Specific department information systems
2. In collecting logs, a department information system technical staff member shall specify the following log classification and the purpose under paragraph 2 of Article I:
(1) Security software logs:
Antimalware, intrusion detection, remote access, web proxies, vulnerability management,

authentication, routers, firewalls, network quarantine, etc.

(2) Operating system logs:
System events, audit records, etc.

(3) Application logs:
Client requests and server responses, account information, usage information, important events in the operation, etc.

IV. System

1. A department information system technical staff member shall implement log management on campus-wide information systems and specific department information systems in accordance with the purposes set forth in items of paragraph 2 of Article I.
2. A department information security technical manager may instruct the department information system technical staff member about audits and improvement of log management.

V. Collection and Storage of Logs

1. In collecting logs, a department information system technical staff member shall implement the following items:

(1) Logs will be collected with a function of the information system to be managed or a coordinated information system.

(2) Collected logs will be kept by a function of the information system concerned or a coordinated information system for a period of at least 90 days. At the time of backup of the system, the logs will also be included.

(3) For the collection of logs, the log classification, purpose of use, period and place of storage, and other relevant matters will be specified in advance in the operation procedure manual of the information system concerned.

(4) If the storage of logs is not possible for technical reasons, including capacity limitation of the information system, such fact will be reported to the department information security technical manager to obtain approval.

2. If a department information system technical staff member finds that logs must be kept for more than 90 days in the light of their importance or for other reasons, the storage period may be extended by giving the department information security technical manager notice of the storage period and the manner and place of storage.
3. A department information security technical manager shall prepare, regarding the information systems of his/her department, a management register specifying the names of the systems, log classifications, purposes of use, periods and places of storage, and other relevant matters, and shall give a report to the department information security manager.
4. A department information security manager or a department information security technical manager may provide a user with notice of the collection of logs under Article 87 and paragraph 7 of Article 89 of the Program Standards by disclosing to the user the names of the systems, log classifications, and purposes of use that are specified in the management register set forth in paragraph 3.

VI. Use of Collected Logs

1. A department information system technical staff member may use collected logs within the purposes set forth in paragraph 2 of Article I and shall comply with the following items:

(1) When collected logs are analyzed and published in part of the use statistics and the measure

for promotion of use, a department information system technical staff member shall perform anonymizing processing of them so that no individuals may be identified.

(2) The relevant department information system technical staff member shall disclose to the department information security technical manager such collected logs as are necessary for the investigation of an incident set forth in item 6 of Article 2 of the Regulations and a suspicious activity set forth in Section 7 of the Kyoto University Rules for Information Asset Use (hereinafter “Investigation of Incident”).

(3) On the requirement of the chief information security officer, or the Information Network Risk Management Committee or the Information Network Ethics Committee regarding Investigation of Incident, a department information security technical manager shall disclose the logs to such requiring party under the direction of the department information security manager.

(4) If inquiry is received from any outside organ (including individuals and legal bodies; the same applies hereinafter) regarding logs in connection with Investigation of an Incident, a department information security technical manager shall respond to it in accordance with the Procedures for Response to Information Security Incidents of Kyoto University under the direction of the department information security manager.

(5) At the occurrence of a failure in an information system, or of any event where such failure is expected, a department information system technical staff member shall disclose the necessary collected logs to the department information security technical manager.

(6) Within the purposes set forth in items 1 through 3 of paragraph 2 of Article I, a department information system technical staff member may disclose logs to the company to which the management of the information system is consigned.

2. Except for cases specified in paragraph 1, a department information security manager, a department information security technical manager, or a department information system technical staff member shall not disclose any logs to a third party.

VII. Protection of Collected Logs

1. A department information system technical staff member shall protect logs collected from an information system to prevent any prejudice to their confidentiality, integrity and availability.
2. For the protection of logs collected and kept, a department information system technical staff member shall implement access control, physical security measures, encryption, etc.
3. If a department information security technical manager is requested for the protection of logs in connection with Investigation of an Incident by the chief information security officer, or the Information Network Risk Management Committee or the Information Network Ethics Committee, or by any outside organ, etc. through due procedures, the manager shall protect those logs appropriately in accordance with the Procedures for Response to Information Security Incidents of Kyoto University under the direction of the department information security manager. In this case, in order to specify the period of protection required, a request shall be made to the party requesting such protection.
4. A department information security technical manager may audit the state of protection of logs and make a recommendation for improvement if he/she finds it necessary.

VIII. Destruction of Collected Logs

1. A department information system technical staff member shall promptly destroy logs collected from an information system upon the expiration of a storage period, when no extension of the

storage period is necessary.

2. A department information security technical manager shall promptly destroy logs for which protection has been requested under paragraph 3 of the preceding article in connection with Investigation of Incident upon the expiration of a protection period designated, when no request is made for extension of the protection period.
3. A department information security technical manager may audit the state of destruction of logs and make instructions for improvement if he/she finds it necessary.

IX. Miscellaneous Provision

Beyond what are provided in these Guidelines, the matters necessary for log management shall be prescribed by the director of the Institute for Information Management and Communication.

Supplementary Provision

These Guidelines shall come into force on April 1, 2017.