Information Security Quick Guide

Published June 2021
Second edition

京都大学 KYOTO UNIVERSITY

Emergency procedure

If you suspect an information security incident, immediately contact either of the following security desks.

Detector
Students, faculty members and office personnel

- Your department's security desk
- All-campus security desk

Report items:
- IP address of the equipment involved
- The nature of the incident (URL, captured images, etc.)
- The time the incident was discovered (JST)
- Name and contact information of the detector

If there is a possibility that a PC in use may have been infected with a virus, by accessing a defaced website for example, run a virus scan to ensure that it remains secure.

Information Security e-Learning

At Kyoto University, every member is obliged to take e-Learning courses on information security. Take the courses every academic year because the content is updated every year.

To begin, access the website of the Institute for Information Management and Communication.
https://www.iimc.kyoto-u.ac.jp/en/

Enlarged view

Do not use P2P file sharing programs

P2P file sharing programs are programs that let users share files with a large number of unspecified users over the Internet. These programs are strictly prohibited* in the network systems of the University to avoid problems such as software piracy and virus infections.

Examples of prohibited programs:

Programs that have a P2P function to automatically transfer files to the public such as BitTorrent, Xunlei, Winny, Share, Edonkey, and WinMX

* When a notification is made under the name of a department chief, those programs can be used in the KUINS-II as an exception.

Security policy of the University

"Kyoto University Basic Policy for Information Security" and various other regulations have been established to ensure efficient management and protection of information assets, which are essential for our activities at the University. An overview of the regulations can be obtained through the Information Security e-Learning introduced in this leaflet.

For details, refer to the "Information Security" page on the website of the Institute for Information Management and Communication. https://www.iimc.kyoto-u.ac.jp/en/ You can use the 2D bar code in the "contact point for security-related matters" in this leaflet.

Have you already taken these steps?

The same steps need to be taken with your smartphone.

- ◆ Properly manage your accounts and passwords.
- ◆ Always update OS and application software to the latest version.
- ◆ Install anti-virus software and activate it with the latest version.
- ◆ Be careful when clicking on URL links or opening email attachments.
- ◆ Do not use information assets for any purpose other than the original intent.

Do not reuse the same password.
Make your password at least 12 characters and difficult to guess.

Neglect of any of these measures may lead to:

- ✻ Leakage of confidential and personal information,
- ✻ Modification of the contents of web pages,
- ✻ Loss of credibility for Kyoto University and related departments,
- ✻ Monetary damage, due to illegal money transfer, and
- ✻ The launch of attacks on other computers without knowing it

To avoid this damage, everyone must raise their awareness of information security and be involved in daily security operations.

Contact point for security-related matters

◆ Your department's security desk
(Fill in the following information)

Department

TEL

MAIL

◆ All-campus security desk

Information Security Management Office

i-s-office@iimc.kyoto-u.ac.jp

http://www.iimc.kyoto-u.ac.jp/en/services/ismo/

TEL:075-753-7490

You can send email to the above address and access the information security website by scanning the 2D bar code.

Mountain fold
Valley fold