筑波大学
University of Tsukuba

University of Tsukuba
Organization for Information Infrastructure
(Department of Academic Information,
Division of Information Infrastructure Management)

Checkpoints for safe and secure use of information systems

(for faculty and staff)

Please read the following points regarding the use of information systems (networks, computers, etc.) at the University of Tsukuba and ensure that you have a high level of security awareness.

1 Have you taken the "INFOSS Information Ethics" course?

The Organization for Information Infrastructure provides e-learning materials for students, faculty and staff of our university to learn about information security. Faculty and staff must take this course at least once every 3 years. If you have not taken the course yet, please do so as soon as possible.

Please click the link for further details. ▶ https://oii.tsukuba.ac.jp/en/infoss-2/

You can check your attendance status from the "Learning Management System for e-Learning".

▶ https://lms4el.sec.tsukuba.ac.jp/

2 Are you using the latest software by regularly performing Windows Update, etc.?

Computer viruses exploit defects in operating systems and commonly used software (Microsoft Office, Adobe Reader, browsers, etc.) to infect computers. For Microsoft Windows, use Windows Update, and for macOS, regularly update the software, to keep it up-to-date. We also ask that you stop using older versions of the OS for which support is no longer provided; please upgrade to the latest version. Please also keep your other software up-to-date.

3 Do not open suspicious e-mails

Our university has confirmed many cases of phishing e-mails that attempt to steal personal information such as IDs and passwords by tricking system administrators and courier companies, as well as unsolicited e-mails asking the recipient to open attached files containing viruses. Please pay particular attention to the following e-mails, and check with University admin if you have any doubts.

❶ E-mails from domains other than tsukuba.ac.jp

❷ E-mails instructing access to URLs with domains other than the University's domain (tsukuba.ac.jp).

❸ E-mails that instruct you to disclose your passwords (admin will never ask you for your passwords)

※Examples of phishing emails received at the University ▶ https://oii.tsukuba.ac.jp/security/information/suspiciousmail/

4 About password management and password settings

Information system passwords need to be managed with thorough care. Please be particularly careful with your Unified Authentication System password used for systems that handle important information, such as manaba and TWINS.

❶ Never disclose your password to others. Do not delegate work to students or secretaries.

❷ Set a complex password that is difficult for others to guess.
(Use random capital and small letters, numbers, and symbols, minimum 8 characters, 12 or more recommended)

❸ Do not reuse your Unified Authentication System ID and password for other systems and services.
In recent years, there have been multiple incidents of password cracking (a malicious hacker using a program, etc. to forcibly steal passwords).
You can use the password manager that comes with your OS.

❹ You should utilize MFA (Multi-Factor Authentication) so that you can prevent illegal access if your password is leaked.

5 Personal information and confidential information with thorough care

The mishandling of devices that hold personal information and confidential information can lead to serious security incidents. So, we urgently ask that you manage personal information and confidential information with thorough care in accordance with the following.

1. If you hold personal information and confidential information across multiple devices, then try to consolidate such information onto a single device where possible. And be sure to delete any personal information and confidential information that you do not need.
2. Do not take portable devices (notebook PCs, etc.) or external storage devices (USB memory, etc.) containing personal or confidential information off campus. If you absolutely need to take such devices off campus, then do so only within the minimum scope necessary with the permission of the Personal Information Protection Manager, and be sure to implement measures against theft or loss, such as setting passwords and encrypting data. Also, ensure that information is deleted after use.
3. Our university has established rules regarding information classification and handling restrictions. Please handle information appropriately in accordance with these rules. ▶ https://oii.tsukuba.ac.jp/en/information-security/kakuduke/
4. Our university has introduced an online storage system (UTOS) for faculty and staff of our university to safely access, view and edit files from information devices on- and off-campus. ▶ https://utos.tsukuba.ac.jp/
5. Please refer to the 'Guidelines for Using Cloud Services' when constructing, operating, or contracting an information system that handles personal or confidential information using external cloud services. ▶ https://oii.tsukuba.ac.jp/en/regulation-3/
6. Email addresses are considered personal information. When emailing external parties or large groups, please use the BCC field. Before sending, double-check that all recipients are correct and that no BCC addresses have been mistakenly placed in the To or CC fields.

6 Points to note when using third-party group mail services and online storage services

Are you using Google Groups, OneDrive, Google Drive, Dropbox, etc.? There is a risk of unintentionally disclosing information to the world by using services on the Internet such as these storage services. For example, being careless with your security settings can allow third parties to view your files, or file syncing can unintentionally upload files containing sensitive information to public folders. Ask others around you to check that your security settings are as intended. Also, strengthen security by setting a strong password, enabling multi-factor authentication, etc.

7 About the dissemination of information on the Internet through social media, etc.

What you say and do on the Internet can be seen by many people. Careless posting on the Internet may cause trouble and bring the decency of the University and its members into question. Please be careful not to transmit inappropriate information on the Internet such as by posting confidential information or content that is contrary to public order and morals.

※Guidelines for Use of Social Media in the University of Tsukuba ▶ https://oii.tsukuba.ac.jp/en/regulation-3/

8 Reference information

- **Software licenses provided by the Academic Computing & Communications Center**

1. EES：https://www.cc.tsukuba.ac.jp/wp/service/sl/ees/
   Our university has a subscription to Enrollment for Education Solutions (EES) from Microsoft. Products such as Windows and Office are available to faculty and staff of our university.
2. Antivirus software：https://www.cc.tsukuba.ac.jp/wp/service/sl/trendmicro/
   Our university has signed a site license agreement for anti-virus software. Faculty and staff of our university can use anti-virus software free of charge, and we encourage you to take advantage of it.
3. Other licensed software：https://www.cc.tsukuba.ac.jp/wp/service/sl/

- **Organization for Information Infrastructure website**：https://oii.tsukuba.ac.jp/en
- **Guidelines for the Use of Information Systems at the University of Tsukuba**：https://oii.tsukuba.ac.jp/en/regulation-3/

Please report any information security incidents to the following contact.

Contact ▶ The University of Tsukuba Information Security Incident Response Team (ISIRT)
E-mail：incident@cc.tsukuba.ac.jp

Revised March 2026