Important Points for the Safe and Secure Use of Information Systems (for faculty members and employees)

Revised May 2020
University of Tsukuba
Organization for Information Infrastructure
(Division of Information Management)

Handling of information in the University

To maintain a high level of security awareness, please note the following points:

1. Be sure not to use Windows 7.

Microsoft's Windows 7 is no longer supported by the manufacturer. Be sure not to use Windows 7 PC as it may cause security problems.

(1) If you are still using Windows 7, please upgrade to Windows 10 immediately.
(2) If you cannot upgrade, disconnect from the network and apply the extended security update program as soon as possible.

(Extended security update program: https://docs.microsoft.com/en-us/lifecycle/faq/extended-security-updates)

2. Notes on using group mail service and online storage service of third parties

Are you using Google Groups, OneDrive (formerly SkyDrive), Google Drive, Dropbox, etc.? Services on the Internet, such as online storage services, may inadvertently release information to the world. For example, depending on careless security settings, it may be possible to view a third party, or the file synchronization function may inadvertently upload a file of confidential information to a public folder.

When you would use such storage services to place your data outside the university, you must always conform to the "rules of information rating and limitations for handling" (available in Japanese only) to always check whether or not you can use the service, and that the security settings of the service are your intended ones. For "rules of information rating and handling limitations", please refer to:
https://oii.tsukuba.ac.jp/en/information-security/kakuduke/

3. Be sure not to open suspicious e-mails.

The University of Tsukuba has observed an increase in suspicious e-mails. These often include phishing scams, involving fraudulent e-mails that masquerade as e-mails coming from a mail system administrator that try to steal your account information. Cyber-attack e-mails claiming to represent delivery notifications from delivery companies designed to let you open an attachment file in order to infect your computer with a virus have also been increasingly observed. Be aware of the following points, and if you seem suspicious, ask the university administrator.

(1) E-mails from domains other than that of the University of Tsukuba (other than "tsukuba.ac.jp").
(2) Access instruction to URL of domain (other than "tsukuba.ac.jp") other than that of the University of Tsukuba.
(3) Instruction to enter password (The administrator will never learn about the password).

(Reference)
Examples of Phishing E-mails https://www.u.tsukuba.ac.jp/en-phishing-collection/

4. Transmitting information to the internet, such as via SNS

Your remarks and behavior on the Internet are possible to be exposed to many people, and careless writing may cause trouble. It results in loss of the public's confidence in the university and its members. Please be careful not to transmit inappropriate information such as matters to be kept secret and contents contrary to public order and morals.

(Reference)
Guidelines for Use of Social Media in the University of Tsukuba:

https://oii.tsukuba.ac.jp/wp-content/uploads/sites/29/campus-only/social_media_guideline_en.pdf

5. Have you taken the "INFOSS Information Ethics" course?

The Organization for Information Infrastructure provides e-learning materials on information security for all students, faculty members, and employees.
Faculty members and employees must take the course once in at least 3 years.
If you have not taken this course yet, please do it as soon as possible.

For detailed information, refer to https://oii.tsukuba.ac.jp/en/infoss-2/

You can check your attendance of INFOSS Information Ethics at the Learning management system: https://lms4el.sec.tsukuba.ac.jp/

6. Proper management of equipment containing personal and confidential information

If personal and confidential information are not properly handled, serious security incidents may occur.
Please make sure that equipment containing personal and confidential information is managed properly along the following points.

(1) If you have more than one device that have personal and confidential information, please consolidate the information as much as possible on one device.
Please delete unnecessary personal and confidential information from the other devices.

(2) For devices that hold personal and confidential information, please make sure that access controls (set passwords to devices, communication control by firewalls) and authentication are performing reliably.

(3) Please do not take out portable devices (notebook computer, etc.) and external storage devices (USBs, SDs, etc.), which store personal and confidential information, outside the University. If unavoidable, please limit to the minimum necessary information, make sure to set passwords and encrypt the data to prevent from theft or loss, and then delete information after use.

(Reference)
Procedures Concerning Information Classifications and Handling Restrictions:
https://oii.tsukuba.ac.jp/en/information-security/kakuduke/

7. Password management and setting

You must properly manage information system passwords.
Be especially careful as the Tsukuba University Integrated Authentication System password is also used in systems such as manaba and TWINS that handle important information.

(1) Passwords should not be shared with anyone.
(2) Don't ask students or the secretary to do work that requires your password for you.
(3) Set passwords that are difficult and hard to guess.
(4) Don't reuse the ID and password of the Tsukuba University Integrated Authentication System for other systems and services.

Recently, cases where passwords are cracked frequently (Hackers steal passwords using password cracking tool), so we must set a strong password.

8. Do you know about the software licenses provided by the Academic Computing and Communications Center?

① EES:

The University of Tsukuba has made an agreement for EES (Enrollment for Education Solutions) with Microsoft. Faculty members and employees can use Windows (upgrade only), Office, etc. for university computers.

For detailed information on EES, refer to https://ds.cc.tsukuba.ac.jp/ms-ees/

② Antivirus Software:

The University of Tsukuba has purchased a site license of an antivirus software program. Faculty members and employees can use antivirus software.
For detailed information on antivirus software, refer to
https://www.cc.tsukuba.ac.jp/wp/service/sl/trendmicro/

③ Other software licenses:

For detailed information on the other software, refer to
https://www.cc.tsukuba.ac.jp/wp/service/sl/

You should immediately report any actual or suspected information security breaches by e-mailing: incident@cc.tsukuba.ac.jp