Safe and Secure Use of The Information Systems

This brochure describes the rules and the important points you must follow when using the information systems (networks, computers etc.) in our university. Before using these systems, please read the brochure carefully. After confirming its contents, please check the items in the checklist below.
For more details regarding this brochure, please go to:
https://oii.tsukuba.ac.jp/en/oii-security-2/details/
Please acquire the correct knowledge and utilize the information systems safely and securely in our university.

筑波大学
University of Tsukuba

☑ Check!

- ☐I have completed the “INFOSS Information Ethics” Course.
- ☐I regularly update Windows and use all software programs in their most recent version.
- ☐I have installed an antivirus software program. In addition, I confirm that the virus definition file is automatically updated to protect the computer from viruses.
- ☐When I use the Internet, I pay close attention to fraud.
- ☐I never give my password to anyone.
- ☐I never use other people’s passwords and user names.
- ☐I have set up a password which is hard to break.
- ☐I always manage personal information carefully and I always take measures to prevent information leakage.
- ☐As a member of the University of Tsukuba, I act responsibly and ethically when posting information on social networking sites and the Internet in general.
- ☐I never duplicate any copyrighted materials or make them available to a third party on the network.
- ☐I do not have any file exchange software program installed.
- ☐I never download software programs of unknown origin.

Organization for Information Infrastructure

Safe and Secure Use of The Information Systems

I have completed the "INFOSS Information Ethics" Course.

Organization for Information Infrastructure has prepared e-learning materials to support you in acquiring knowledge about ICT (Information and Communication Technology), network security, laws, manners etc., which are needed for carrying out various activities at the university, and for avoiding harm and trouble in our network society. Every student enrolled in our university must complete the course at least once (each time your student ID changes, you must do the course again, at least once). If you have not completed the course yet, please do so as soon as possible.

For more details, please go to https://oii.tsukuba.ac.jp/en/infoss-2/.

I regularly update Windows and use all software programs in their most recent version.

Computer viruses can spread maliciously through the operating system (Microsoft Windows, macOS, etc.) and can take advantage of defects in popular software programs (Microsoft Office, Adobe Reader, web browsers, etc.). For Microsoft Windows, you need to perform Windows Update; for macOS, you need to regularly do software updates to maintain the software in its latest version. If the support for an old version of an operating system has ended, stop using that version. You need to update to the latest version. For all other software programs, you should always update to their latest version.

For more details, please go to https://oii.tsukuba.ac.jp/en/oii-security-2/details/.

I have installed an antivirus software program. In addition, I confirm that the virus definition file is automatically updated to protect the computer from viruses.

When a computer is infected with a virus, not only data on the computer are destroyed but also the computer itself is taken over by the virus, and it might be used to send spam e-mails and attack other computers. Infection routes have diversified and using e-mails is not the only way a computer virus can spread. Actions such as browsing the Web or simply inserting a USB memory into the computer may cause infection. To avoid being infected with a virus, it is important to install an antivirus software program and update the virus definition files on a regular basis.

Our university has purchased a site license of an antivirus software program. The antivirus can be installed on up to three personal devices (Windows machines, Macintosh machines or mobile devices). The total number of installations must be less than 4. If you have no other antivirus program installed or if you are not sure whether you are paying a license fee for an already installed antivirus program, please install this one.

For more details, please go to https://oii.tsukuba.ac.jp/en/oii-security-2/details/.

Q What if the computer is infected with a virus?

To avoid further infection, remove the infected computer from the network (remove the network cable, use the airplane mode, or turn Wi-Fi and cellular data network off) and contact us at the address on the last page of this brochure.

When I use the Internet, I pay close attention to fraud.

While it is convenient to use the Internet, it is also possible to face unexpected troubles.

If you are in trouble and cannot handle the situation, do not attempt an easy solution. Please contact your friends or faculty members or contact a consumer center first.

Phishing

In a phishing fraud, an attacker masquerades as an administrator etc. of a reputable company such as a bank, Rakuten, Amazon, Apple, Microsoft etc., and directs users to a website which is very similar to their real website, in order to steal the users' personal information such as IDs and passwords. **The bank and other companies will never ask you to input and confirm personal information via e-mail.** If you receive a suspicious mail, do not provide your information immediately. In such a case, do not contact the address you find in your e-mail, but contact the company directly.

※Examples of Phishing Emails :
https://oii.tsukuba.ac.jp/security/information/suspiciousmail/
(In Japanese/Limited to on-campus)

Tech Support Scams

Tech support scams scare web users by suddenly displaying fake warning messages stating that a virus infection took place. They ask you to call a contact phone number, making you install a remote-control software, and forcing you to pay some money. **Even if a pop-up message is displayed during web surfing, do not easily trust it and do not call the phone number in the message.**

If the symptoms do not improve even after force quitting the browser or restarting the computer, try the solutions described on the supplementary explanation page of this pamphlet. After that, it is a good idea to run a virus check to make sure your computer is safe.

One-click fraud

One-click fraud means that if you click once on a link in an e-mail or on a website, you appear to have entered into an agreement and you are requested to pay a certain amount of money. If you encounter such a situation, ignore the request; do not make any payment for any purchase you are not aware of and do not give out your name or address. However, in some cases the fraudsters exploit the judicial process. If you receive notice that seems to come from court, do not ignore it, but check the address of the courthouse on its web page (https://www.courts.go.jp/) and contact that address. Do not contact the address in the letter sent to you.

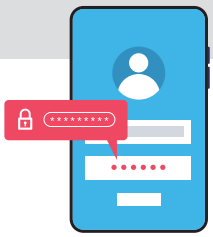
I never give my password to anyone.

Usernames and passwords used for the information systems in our university are important information to identify the users. If you give your username and password to a third party and he/she causes trouble while using the information systems of our university, you are also responsible for the problem because you gave away your password. Furthermore, you must not use a username and password given to you by somebody else.

I never use other people's passwords and user names.

It is against Act on the Prohibition of Unauthorized Computer Access to acquire somebody else's username and password and log in as that person, or to take advantage of a security hole (flaw in a software program) for avoiding the username and password confirmation, and log into a computer.

I have set up a password which is hard to break.



If a password is easy to break (your name, user name, birthday, phone number, repeating the same characters, using an English word more than once, using the alphabet in sequence on a keyboard, like "qwerty", or using the above in reverse), a third party may gain illicit access to your account. **It is important to set a password which is difficult to break (more than 8 characters, 12 characters or more recommended, combination of capital letters, small letters, symbols and numbers).** Even if a password is difficult to break, **it is not advisable to write it down and make it available to a third party.**

Furthermore, **it is not advisable to use the same password on different Internet services.**When you use a different password for each service, even if a password were leaked from one Internet service, the other services would not be affected. When you use your personal device, you can use the password manager that comes with your OS.

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

I always manage personal information carefully and I always take measures to prevent information leakage.

Faculty members as well as students may handle personal and medical information collected through surveys and so on during lectures and practice classes, but that information must not be released on the network. It is also forbidden to take the information outside the university. If you need to take part of the information out of the campus, you need to obtain permission from an administrator of the respective information, or a person designated by the administrator (an instructor of a class, or a supervisor of a laboratory, in case of a lecture or practice class) and take measures to secure the information (e.g. encrypt it), before carrying it away from the campus. You are not allowed to keep personal information on a computer that is managed personally. If this is unavoidable, you must encrypt the information first.

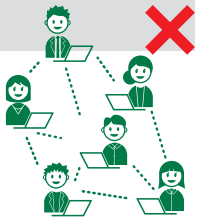
As a member of the University of Tsukuba, I act responsibly and ethically when posting information on social networking sites and the Internet in general.

Everything you post on the internet can be seen by anyone. If posting carelessly, you may get into trouble and your actions may affect the reputation of our university. You should be very careful not to post confidential, inappropriate or offensive information on the Internet.

I never duplicate any copyrighted materials or make them available to a third party on the network.

The purpose of the copyright law is "to provide for, and to secure protection of, the rights of authors, etc. and the rights neighboring thereto with respect" to "[copyrightable] works as well as performances, phonograms, broadcasts and wire-broadcasts, while giving due regard to the fair exploitation of these cultural products, and by doing so, to contribute to the development of culture." If you duplicate copyrighted works illegally and make them available to a third party without the author's permission, you are subject to punishment.**You may also be punished for downloading any kind of copyrighted material (not only digital audio or visual recordings) when you are aware that it was uploaded infringing copyright.**

I do not have any file exchange software program installed.



Using file exchange software is very dangerous because some people distribute files with bad intentions. Moreover, the file you have downloaded is automatically uploaded for a third party. **Our university forbids the use of any file exchange software program inside the campus network,** including on the users' personally owned computers. There is a system in place that blocks the use of file exchange software 24 hours a day and if you violate these rules, **you may be punished by the authorities of the university.** If you have a legitimate reason to use a file exchange software program on campus, please contact the Organization for Information Infrastructure, University of Tsukuba. If you are a student, depending on the purpose of use, you need an authorization from your adviser or your class supervisor.

I never download software programs of unknown origin.

If you find a web page of unknown origin distributing expensive software programs free of charge or at low cost, do not download these programs. In many cases, these are distributed without permission. Besides infringing copyright, you risk infecting your computer with a virus, since the software may have been modified. There is a system in place that monitors downloading of software programs of unknown origin. **Do not download software programs of unknown origin.**

Contact us if you find any problems

Please contact us immediately if you encounter problems like those below or if you face other issues with the information systems.

- Infringement of copyright.
- Leaking of classified or personal information about faculty members of our university.
- Security vulnerabilities and defects in the information systems of our university.

The University of Tsukuba Information Security Incident Response Team (ISIRT)
e-mail ❯ incident@cc.tsukuba.ac.jp

For the brochure's PDF file and more details regarding this brochure, please go to：
https://oii.tsukuba.ac.jp/en/oii-security-2

This brochure has been created by Organization for Information Infrastructure at the University of Tsukuba.

Issued in March, 2025