Duty and Prohibition to utilize Information Services (computing)
What to do in the case of emergencies, such as computer virus infection.

University of Toyama Information Services (computing)

Computing Service Policies, Rules and Guidelines

University Information Services (Computing) provides computing facilities and related services in support of research and teaching (including related clerical work) in the University of Toyama. All the users of University of Toyama's network and computer resources ("users") are responsible to use them properly, protect the security of information and information resources, and respect the rights of others. This policy provides guidelines for the appropriate use of information resources. Users ought to be strict with such computer ethics. If not, computer troubles and problems will lead up to prosecution, compensation claim and downfall of our University's fame. In order to avoid these, all users should read this Computing Service Policies, Rules and Guidelines carefully.

Chief Information Officer, University of Toyama
Information Technology Center, University of Toyama

User Obligations and Duties

While it is necessary for university life, the information systems are always facing threats, such as computer virus attacks, unauthorized access, and information leaks. To protect the security of network and computer resources, each user must take all appropriate actions.

1. Control over User Authentication Credentials

User Authentication Credentials mean ID and Password to identify your user name (user ID and account). If your password is compromised, someone may involve you in crimes. You must control over user authentication credentials thoroughly in order to protect your personal information and for the sake of system security.

- Never share your password with others.
- Set your password of an appropriate length.
- Your password must be at least eight characters long and contain at least one uppercase letter, one lowercase letter, and one number.
- You must not use words easily guessed as your password (e.g., words in the dictionary).
- You must not leave your computer when you log in.

2. Countermeasures against Malware

Today's computer viruses not only destroy data or slow PC operation down, but also steal important data from your PC furtively and disclose it over the internet. They may even control your PC remotely, and, as a result, implicate your account in some plots cryptically. To avoid this, countermeasures (listed as follows) against malware (main source of computer viruses) are mandatory for you.

- Install anti-virus software, keep the virus definition files updated, and run a virus scanner regularly.
- You must not open any attachment nor click URLs in emails unless you are expecting them and confident that they are not malware.
- As for free software, assess its reliability carefully, and download the latest version from reliable distribution sites. In addition, read the software's terms and conditions of use to make sure that it can be used for our university.
- You must not browse dangerous web sites nor download unnecessary files, software, nor applications.
- Be sure to run a virus scanner before you use downloaded files or send a file to other people.

3. Countermeasures against Unauthorized Access

Defects in the setting of the PC or software, or security holes (computer vulnerabilities caused by software defects) left unfixed are dangerous. If the PC has these, it may allow unauthorized users to access, steal or tamper with data in the PC, or use the PC to attack other IT devices. You must control over software on your PC strictly, lest you should become an unintentional offender.

- Check over OS and software and keep them up-to-date regularly. We strongly recommend you the automatic update setting.
- You must not turn off the firewall nor open the ports inadvertently.

4. To Respect the Terms of Social Media and Abide by Them

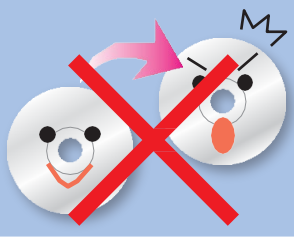
Default private settings are "public" of such web services as social media (Facebook, X, Instagram, LINE, etc.) and cloud services (Dropbox, OneDrive, Google Drive, box, etc.) in most of the cases. In such cases, posted private data and files are open to the public. In addition, individuals become more identifiable by correlating data gained from those services. You are strongly advised to be watchful to use those services and use them as a responsible individual.

- It is noteworthy that complete removal of what you posted on or entered into web sites is impossible. Even if you delete an entry, it is just in the state of being not displayed, and may remain in the system of the site.
- Before posting a message on a web site or store a file on the internet, watch whether the information may violate others' rights when it is open to the public or suddenly vanishes.
- You must not post on or enter into web sites unnecessary information.

Prohibited Activities against Network and Computer Resources

As consequences of misuse of information resources, a user found to have violated the University Code of Conduct, the Fundamental Standard, will be subject to appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action.

1. Prohibition against Usage like Illegal Copy



Users must not violate copyright law and must respect licenses to copyrighted materials (copyrighted contents and images of websites, software and applications as well as books, treatises, copyrighted reports, music, images and other copyrighted things). For the avoidance of doubt, unlawful file-sharing (to reproduce, adapt, or publically distribute them without express permission of copyright holders, though exceptions are provided in the Copyright Law) using the University's information resources is a violation of this policy.

- Do not plagiarize from books, articles, or online text when writing reports, etc.
- Do not copy music, videos, etc. from friends' media to your own devices.
- You must not install software on your PC without express permission, even if the University laboratories or research offices you are working for are the copyright holders.
- You must not install software received from others onto your PC inadvertently.

2. Prohibition against Usage like Unlawful File-Sharing

Users must not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law, especially the Copyright Law. It prohibits even Personal Use, and makes it illegal to upload the fraudulent.

- When you are going to use contents on websites, confirm that they are not illegal.
- Do not use P2P (file sharing) software.
- To use cloud services, you must check carefully the website's service and security, sharing range settings, and copyrights of uploaded or downloaded contents.

3. Prohibition against Unauthorized Access

Unauthorized access to a system or attempts to gain another person's information (i.e., to steal passwords by exploiting software vulnerabilities) violate applicable law. These action, including to access files by spoofing and spamming, are potentially subjecting the users to both civil and criminal liability.

- Users of information resources must not access computers, computer software, computer data or information, or networks by someone else's user authentication credentials.
- Users of information resources must not access computers, computer software, computer data or information, or networks by exploiting the system vulnerabilities.

4. Prohibition against Violation of Others'Rights

You must not violate others' rights against the Fundamental Standard, whether related laws prohibit the activities literally or not.

- You must not contribute to the creation of a hostile environment in social media, internet bulletin boards, emails.
- University information resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages, especially in the form of spam, except as permitted under University policy.
- Without express permission, you must not give away others' personal information.
- Do not use the university network for purposes other than education or research, such as playing mobile phone games or exchanging photos and videos via social networks.

Other Guidelines

1. Regarding dissemination of information

When you dispatch information via network and computer resources, you must be conscious of both civil and criminal liability. When you receive it, you must be careful whether it is trustworthy or not.

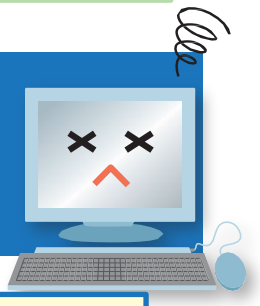
- You must not dispatch false or unverified information intentionally.
- You must not spread unverified information by forwarding emails.
- You must protect secret information by encoding or setting a password.
- You must pay close attention when entering your personal information.
- Never set automatic forwarding email from your official accounts to outside the university.
- (Email forwarding setting to outside the university is strictly prohibited)

2. About data

When you graduate or withdraw from the university, your account issued by us will be deleted. (Some accounts of those who go on to further studies will be deleted.)

- Your data on the university's network will be deleted after graduation, so be sure to transfer any data you need to your personal storage before graduation.
- After graduation, any cloud data that requires a university account will become inaccessible and be deleted, so please transfer any data you need before graduation as described above.

What to do in the event of a computer virus infection (including a suspicious case)



If you discover a virus on your computer, disconnect the computer from the network immediately. Viruses may be transmitted via storage media such as USB flash drives. Please take precautions to prevent the spread of infection, such by not carelessly using such media on other computers.

【Gofuku/Takaoka Campus】
Information Technology Center, University of Toyama 3190 Gofuku, Toyama 930-8555 TEL 076-445-6946 FAX 076-445-6949

【Sugitani Campus】
Sugitani Branch Office of Information Technology Center, University of Toyama 2630 Sugitani, Toyama 930-0194 TEL 076-434-7167 FAX 076-434-5008

For further information on network and computer resources in the University of Toyama, see the website as follows:
University of Toyama Information Technology Center Website (https://www.itc.u-toyama.ac.jp/)

Issued in February 2024