Ehime University Information Security Guidelines

1 Security Update

Be sure to update your PC or smart device OS and software on a regular basis and use the latest version at all times.

2 Virus Countermeasures

Make sure to install antivirus software and keep its virus definition files updated.

Mascot character of Ehime University "Emica"

3 E-mail

Be careful with Targeted Attack Mail and do not open any attachment files or click URL links from unknown sources.

4 Password

Use a hard-to-guess password with a combination of alphabetical characters, numbers and symbols, do not give it to anybody else. Do not use the same password for various Internet services. When there is a pre-set password, change it to one you make.

5 File Sharing

When sharing files, configure settings to prevent information leakage, such as limiting access rights.
If there is no longer a need for file sharing, promptly revoke the sharing settings.

6 Backup

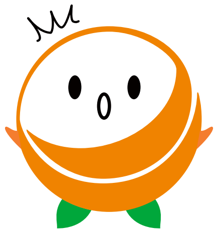
Make it a rule to back up data on a regular basis so you can prevent important information from disappearing due to malfunction or mechanical trouble.

7 Information Management

Do not leave critical information unattended on the top of your desk. Do not take devices or USB memory sticks that include critical data, such as personal information, out of the university.

8 Disposal of Information

Shred important documents. When disposing of a PC or a storage medium, you need to use data erasure software or hire a contractor for its erasure.



If you find something strange...

1. Disconnect your PC from the campus network
2. Contact the Center for Information Technology at ext. 8803 (in Japanese)

(Contact Us) Center for Information Technology, Ehime University
URL : https://www.cite.ehime-u.ac.jp/ E-mail : center@dpc.ehime-u.ac.jp
Phone : +81 89-927-8803

EHIME UNIVERSITY

Check Sheet

1. Security Update

□ Be sure to update your PC or smart device OS and software on a regular basis and use the latest version.

□ Do not use PCs or devices that have not been updated, as they may be infected with malware exploiting safety flaws.

2. Virus Countermeasures

□ Install antivirus software so you can protect your PC from suspicious web sites and e-mail-based viruses.

□ Make sure that virus definition files are updated at all times. Otherwise, antivirus software won't operate properly.

3. E-mail

□ Prior to sending an e-mail, recheck its destination address carefully to prevent a mistaken transmission.

□ Telling someone's e-mail address to others without his/her permission results in personal information leakage. Use Bcc (Blind Carbon Copy) specification to send an e-mail to multiple people who don't know each other's addresses.

□ Do not send important information by email.

□ If you misspell the email address and accidentally send it to an imposter domain (doppelganger domain) posing as the intended recipient, there is a risk of information leakage. Please verify carefully that there are no errors in the recipient's email address.

□ Targeted Attack Mail is prevalent. Regardless of whether the sender's address/content is suspicious or not, be alert for e-mail attacks with disguised files. If you find something strange, do not open the attachment or URL link but delete the mail itself.

4. Password

□ Use a hard-to-guess password with the combination of alphabetical characters, numbers and symbols, avoiding a simple one (e.g. name or date of birth). Do not use the same password for multiple Internet services.

□ Do not leave your password where it can be seen by others.
Do not tell your password to anybody else, either.

□ Make sure that you change an initially set password before using devices that are connected on the network, such as routers and office multifunctional machines, to protect your PC from illegal access.

5. File Sharing

□ Sending files by email has the risk of information leakage. Please share files using OneDrive, Groups, Teams and other services provided by Microsoft365 with your Ehime University account, or use Nii FileSender. When sharing important files, if necessary encrypt them (with password protection, etc.).

6. Backup

□ Malfunction and mechanical trouble might cause saved data in your PC or server to disappear. This will also guard against "Ransomware", which covertly encrypts specific data on the target PC and demands a ransom money for the release. Make it a rule to back up data on a regular basis in case anything goes wrong.

7. Information Management

□ Information which is left unattended on your desk is at the risk of being carried away or seen by someone else. Do not leave critical information unattended but manage and protect it in a safer place. Be sure to lock the office when everybody goes out.

□ Laptop computers, tablet devices and USB memory sticks are easy to carry around, but at the same time, at higher risk of being stolen. Do not take devices that include critical data out of the university.

8. Disposal of Information

□ Important documents thrown out in the garbage might be seen by others, which could cause critical information leakage. When disposing of documents, don't forget to shred them.

□ There is a risk that deleted data on your PC or a storage medium can be restored. Before deletion, you need to use data erasure software or hire a contractor for its erasure to see that information cannot be restored in any manner.

Supervision : Ehime University CSIRT (Computer Security Incident Response Team)