Handbook of Information Security Measures for Faculty and Staff

Edition 1.2

December 9 , 2022

国立大学法人
和歌山大学
wakayama
univ.

aic
和歌山大学
学術情報センター

Chapter 1 Handling Information

1.1 Rating of information

Information handled by the University is rated under the following three categories: “confidentiality,” “integrity” and “availability.” It is recommended that all information be clearly marked so that the rating can be recognized. In addition, stating the handling restrictions will also provide clarity on the method of handling of information. As examples of handling restrictions, set “limited to the person in charge,” “no reproduction” or “no transfer” as appropriate.

1.2 Use and Retention of Information

Once the information has been rated, it must be handled in accordance to the manner described in the “Unified Standards for Information Security Measures at Wakayama University.” In addition, if you are unsure about the rating or the handling restrictions, please check or consult with the creator or recipient of the information.

Chapter 2 Basic Security Measures

In order to implement information security measures correctly, basic measures must be taken on a daily basis. Here, we shall describe these basic measures.

2.1 ID and password

You will need a username and password to use the computer. In addition to the password issued by the Academic Information Center, it will be necessary to enter passwords in a variety of situations. These include ordering and purchasing systems, off-campus services, network-connected hard disks (NAS), and printers, etc. The kinds of passwords that users use are critical in terms of system security. Please refer to the checklist items below to make sure that your ID and password are handled correctly.

<Check the checklist items below>

□Passwords must be at least 11 characters

□Passwords must be complex and a mixture of uppercase letters, numbers, and symbols

□Do not use normal words, people's names, or anything else that is easy to guess

□Passwords used at the University and passwords used for off-campus services should be completely different

□Don’t write passwords on notes where they can be seen by others

□Don’t share passwords between multiple users

□The ID and password you use at the University must not be entered on PCs used by a large number of unspecified people, such as in Internet cafes

□If you enter your ID or password after clicking on a link you receive in an email, confirm that it is the correct web page

□If default passwords are set on IoT devices such as NAS, Wi-Fi routers, and printers, etc., change them to more difficult passwords

2.2 Software Updates

OS (Windows, etc.) and application software (Office, etc.) operate on PCs used on a daily basis. Such software is updated from time to time to improve functionality and fix security holes. Failure to update the software can result in security holes being attacked, your PC being hijacked and result in information leaks. Always update your OS and application software to include the latest software updates.

Additionally, as support will be discontinued once the OS becomes out of date, updates will no longer be provided after that point. In such as case, it is necessary to take measures such as updating the OS or the equipment itself.

In addition to PCs, IoT devices, such as NAS, Wi-Fi routers, network cameras, and printers are equipped with software called firmware. Check each manufacturer's web page to see if their firmware has been updated; if it has, install the updated firmware immediately. Refer to the manual or the website of each manufacturer for information on how to update the firmware.

Depending on the model and manufacturer, firmware updates may not be available after a certain period of time has passed since its launch. In this case, it is strongly recommended that you replace or discontinue use of the equipment.

2.3 Countermeasures Against Computer Viruses

If your computer becomes infected with a computer virus, it can lead to serious damage, such as the leakage of confidential information including your personal information, remote manipulation, files being deleted, and unauthorized encryption of important files by ransomware, all of which can interfere with the normal execution of business. Always take care and act to combat viruses on a daily basis.

<Check the checklist items below>

□Anti-virus software has been deployed on all PCs
□Anti-virus software is always updated to the latest version.
□Once a week, all files on the PC’s hard drive and SSD are checked using antivirus software
□OS and application software are always updated to the latest versions.
□Files brought in from external sources using USB memory, email, etc., are always checked using anti-virus software
□Do not download files or free software for which the safety cannot be verified from the Web, etc.

2.4 Use of Application Software

Be aware of the following when installing application software on your PC, etc.:

<Check the checklist items below>

□Software is installed only within the scope permitted by the license

□Any free software is downloaded from a legitimate website and only used after confirming its safety through virus checks and other means.

□Never install any software that is unrelated to your work

□ If the OS has the functional ability, place restrictions on access to data such as devices (cameras, microphones, etc.) and contacts on devices where the software is available, as necessary

Chapter 3 Use of Email

Email usage is increasing at work, but can inadvertently lead directly to security incidents. Make sure you understand the content of this chapter and use email in the correct way.

3.1 Things to Watch Out for in Email

Email is a convenient way to communicate, but there are some things that should be kept in mind.

<Check the checklist items below>

□Confirm that the recipient(s) is/are correct

□Make use of BCC when you do not want the recipients to know who you are sending the message to, such as when you are sending a message to all recipients at once.

□Do not forward work emails to free email services (e.g., Gmail, Yahoo! Email, etc.)

□ Check every now and then that forwarding parties have not been added without permission.

3.2 Attaching Confidential Information

Emails, in the same way as postcards, can be viewed by third parties. Recently, email accounts have been hijacked, allowing the hacker unlimited viewing of the emails. Sending incorrectly also increases the risk of leakage. In principle, attaching confidential information is prohibited. If this is unavoidable, however, adhere to the following procedure:

(1) Use the password setting function for Office files and use complex passwords.

(2) For files that cannot be password-protected, such as text files, use encryption software such as AttachéCase to encrypt the files, and use complex passwords.

(3) Do not use emails to communicate passwords. Make arrangements in advance to communicate using other media such as short message services (SMS), or telephone calls, etc.

<Reference>

When exchanging confidential information, use online storage (Proself) for file exchange. In addition, encrypting files in case Proself authentication is broken gives you even more security.

Proself: https://proself.center.wakayama-u.ac.jp (authentication required)

3.3 Targeted Attack Emails

There are many targeted attacks aimed at specific universities, companies, and organizations carried out by sending emails with computer viruses attached to them. A number of tricky techniques are used to get the virus loaded in the attachment to run. Be careful of the following points to avoid being deceived by targeted attack emails:

<Check that the emails you receive do not contain the following:>

Subject line or main text written in poor Japanese.

Unknown sender, company, or free e-mail such as Yahoo, Gmail, etc., is being used

(3) Non-work-related content

(4) Content that is clearly a blatant attempt to have you open up the attachment. Examples: [Important Notice], [Emergency], [Important], etc.

(5) The extension of the attachment is compressed such as ZIP, LZH, RAR file types.

(6) Requests for payments for things of which you have no knowledge (Be careful as they may be impersonating your clients.)

<If you accidentally open the attachment>

If you accidentally open the attachment, take the following actions as soon as possible.

(1) Disconnect your PC from the network immediately (remove the LAN cable or disconnect it from the wireless LAN). Do not shut down your PC.

(2) Share information within your department and check whether any similar emails have been received.

(3) Contact the CSIRT immediately. *You can find their contact details on the final page.

3.4 Phishing

Phishing refers to emails or SMS (short message service) messages pretending to be from financial institutions, the Japanese postal service, couriers, etc.,

that direct users to a fake URL to exploit their personal information, credit card information, IDs, passwords, etc.

Since there have been cases of our university being targeted in the past, please be aware of the following points.

<Check the checklist items below>

□Don't trust emails asking for personal information

□Don't trust the sender's name described in the email

□It should be possible to trace email links from the sender's organization's web page, and these should only be used after checking that they are the same as the organization's domain, etc.

Chapter 4　Use of Network Services

Online storage services and social networking services (SNS) are widespread, and when used properly, they become powerful tools. However, if you use them without understanding their characteristics, you may get involved in unexpected problems. In particular, it may not be possible to delete confidential information once it has spread throughout the network. Be aware of the following precautions to ensure that network services are being used securely.

4.1 Using Online Storage Services

Online storage services such as Google Drive, Dropbox, and OneDrive are very useful for storing, referencing, and exchanging files with external parties, regardless of workplace and travel destination. However, if you use them incorrectly, there is also the risk of information leakage. Be aware of the following points when using them.

<Check the checklist items below>

□Use complex passwords as described in 2.1.

□You must not duplicate the use of the same password, including those of the University.

□In preparation for problems that may occur with Online Storage Services, make sure that you have a backup of the files in another location.

□Configure sharing settings in a way that avoids public disclosure.

□When storing confidential information, encrypt it using a difficult password

4.2 Use of SNS

Communicating using LINE, Facebook, Twitter, Instagram, etc., is very convenient, but you must be careful as unintentional remarks or misuse of the system can lead to unexpected problems.

<Check the checklist items below>

□Don't post confidential information or anything that detracts from the reputation of the University

□Fully understand the features of public/private settings

□Exercise sufficient caution regarding friend requests from strangers

1 □ Even if the group is set to private, be aware that someone in your group may forward the information to other groups or other social network sites

□Take sufficient care before agreeing to service collaboration

□Don't make unauthorized posts of private information about friends, acquaintances, students, etc.

□Do not post any defamatory or false content

Chapter 5 If This Happens…

5.1 Using PCs Outside of the University

There is a risk of loss or theft if you take your work PC with you on a domestic or overseas business trip. In principle, it is recommended that you do not take it out. However, if you need to take it out for unavoidable reasons, be aware of the following:

<Check the checklist items below>

□ When using Wi-Fi, use a network that displays security protection and has a key mark (🔒).

□If you are using Free Wi-Fi in a hotel or public place, only use sites for which the address starts with "https"

□Don't store confidential information on your PC

□If taking confidential information out of the office is unavoidable for any reason, make sure it is encrypted with a complex password

□ Set the password for the BIOS before the OS starts up

□If you take confidential information out, make sure that you know exactly what it is

□Promptly delete any confidential information that is no longer needed

If you delete files using the OS standard functions, **it may be possible to recover** them. When deleting confidential information, **make sure you completely erase the files in such a way that is difficult to restore them.**

□ When erasing files from USB memory

When erasing confidential information stored in USB memory, completely **format (initialize)** the USB memory. (*This will delete **all files in the USB memory.)**

✓ Please note that doing a Quick Format is not sufficient

Reference: Data Rescue Center https://www.rescue-center.jp/elementary/vol04.html

□ When deleting files from an HDD

If you want to completely erase confidential information from magnetic storage devices, such as an HDD, be sure to use file erasing software.

Reference software: ERASER (Windows, English) https://eraser.heidi.ie/download/

□ When erasing files from SSD

Carry out deletion per OS standards. (If you have moved them to the recycling bin, be sure to empty the recycling bin) Using the Trim function, traces of files are periodically erased.

Reference: EaseUS: How to disable/enable TRIM for SSDs in Windows 11/10

https://jp.easeus.com/knowledge-base/how-to-enable-disable-trim-on-ssd.html

5.2 Your PC is Infected or is Suspected of Being Infected with a Virus

(1) If your PC is infected with a virus, carry out the following the procedure:
Promptly disconnect the PC from the network (remove the LAN cable or disconnect it from the wireless LAN). Do not shut down your PC.

(2) Contact CSIRT immediately and follow their instructions.
*You can find their contact details on the final page.

5.3 Your PC or Other Terminal Has Been Lost or Stolen

If you discover that your PC or USB memory containing confidential information has been lost or stolen, carry out the following the procedure:

(1) Contact your manager and CSIRT with the following details:

*Situation in which it was stolen or last checked

*Details of sensitive information, including personal data, if stored, and whether it is encrypted with a complex password

(2) If the PC that you have lost is discovered, report this to your manager and CSIRT immediately.

5.4 I Have Purchased IoT Devices such as NAS, Wi-Fi Routers, Network Cameras, and Multi-Functional Devices

IoT devices such as NAS, Wi-Fi routers, network cameras and multi-functional devices are computers with their own network functions. Failure to manage such devices properly after installation can result in external intrusion, leaking of documents, photos, and videos, and attacks on external organizations using the IoT devices as a platform. To prevent external intrusion, do the following:

<Check the checklist items below>

☐ Change passwords for IoT devices from the default passwords to complex passwords immediately after purchase and installation

☐ Always update the firmware (software embedded in the IoT devices) to the latest version

☐ Apply for new IP addresses without using those obtained in the past

5.5 Software and Copyright

Software is copyrighted and can only be used under the terms and conditions described in the license agreement. The use of software that has been obtained illegally or in violation of a license is a violation of the law, and may result in criminal proceedings or claims for damages. It also represents a security risk because it cannot be properly updated. Use the software in an appropriate way.

<Check the checklist items below>

☐ Software has been purchased from an authorized distributor

□ Read the license terms and be careful not to violate them

□ Always uninstall any trial versions of software after you have used them

5.6 If You Have Any Other Problems…

If you have any concerns or feel something is wrong when using your PC, etc., be sure to consult with the Academic Information Center.

Chapter 6　Appendix

Collection of Reference Links

・Wakayama University Academic Information Center Security Information https://www.wakayama-u.ac.jp/aic/security/index.html

・National center of Incident readiness and Strategy for Cybersecurity(abbreviated as NISC) Information Security Handbook　https://www.nisc.go.jp/security-site/files/handbook-all.pdf

・Information-Technology Promotion Agency, Japan (abbreviated to "IPA") Important security information　https://www.ipa.go.jp/security/

・IPA Technical Watch "Examples of targeted attack e-mails and how to recognize them"
https://www.ipa.go.jp/security/technicalwatch/20150109.html

・The Shiori Series of IPA Measures
https://www.ipa.go.jp/security/antivirus/shiori.html

・For Software Users of the Association of Copyright for Computer Software
https://www2.accsjp.or.jp/sam/user.php

Revision History

Edition No.	Date of issue	Revision History
1st Edition	January 21, 2020	Initial Edition
Edition 1.1	March 25, 2021	Added 5.5 Software and Copyright
Edition 1.2	December 9, 2022	Added 5.1 Examples of Complete File Erasure

In the event of an information security incident or suspicion of it, promptly isolate the target device from the network (e.g.,Remove the LAN cable) and contact the following immediately.

Information Security

Wakayama University CSIRT (Computer Security Incident Response Team)

TEL: 073-457-7177 (extension 7177)

E-mail: csirt@ml.wakayama-u.ac.jp

In addition, please feel free to contact the following in regard to any daily inquires.

Technical Questions and Opinions

Academic Information Center (technical representative)

E-mail: query@ml.wakayama-u.ac.jp

Other uses of PCs/networks

Academic Information Center (Information Management Section)

TEL: 073-457-7177 (extension 7177)

E-mail: aic@ml.wakayama-u.ac.jp