<For general users>

Information Security Textbook

April 2024

Muroran Institute of Technology
Information Infrastructure Council

Table of Contents

1. Introduction

Information security and our lives

In modern life, the use of personal computers and smartphones has become something we take for granted. In order to utilize information technology, which is evolving daily, in our daily lives and for work and research activities, it is essential that we pay attention to how information is handled.

This book summarizes the basic matters concerning information security in an easy-to-understand manner and constitutes a manual that clearly describes specific methods for using information systems.

We hope to see people observing the rules and protocols of etiquette laid out in this book, use information systems at this institution of learning for education and research purposes, and comfortably make use of the information services that are provided to the general public in our daily lives.

Muroran Institute of Technology's Information Security Policy

When using an information system operated by this institution, take note that an Information Security Policy has been prescribed as a set of rules for the use of that system. Whether you are a faculty member or student, you are required to comply with the Information Security Policy.

Scope of the applicability of the Information Security Policy

The scope of the applicability of the Information Security Policy is as follows:

- Information infrastructure and education systems
  - Institute's official email (Web Mail)
  - Institute's official website
  - Learning support system (Moodle)
  - Personal computers installed in study rooms
  - Personal computers installed on campus, including personal computers in libraries and international exchange rooms
- Network systems on campus (campus information network systems)
  - Internet access from a location on campus (accessing via SINET)
  - Communications using a wireless network installed on campus (edutroam)
  - Communications using a wired network or wireless network (Wi-Fi) in a laboratory (including use of a wired network or wireless network with your own personal computer or smartphone)
- All information systems on campus, including the library information system, academic information system (Campus Square), and groupware system (Garoon)

Supplement 1: The Information Security Policy applies even when you use your own personal computer or smartphone to connect to and use a network operated by the Institute.

Supplement 2: The Information Security Policy applies even when you connect to a wireless LAN access point installed in a laboratory or department. Use such access points in a manner that is compliant with points to be observed in this book.

2. Prohibition against actions carried out for a non-intended purpose and cooperating with operations

- Do not use a personal computer or network belonging to the Institute for a non-educational or non-research purpose
  Example: Do not download unlawful content or browse games or adults-only sites via Wi-Fi or a laboratory network.
- **Do not use file-sharing software**

Prohibition against use for a non-intended purpose

The Institute's personal computers and networks are provided for educational and research purposes. Do not use these items for a non-educational or non-research purposes. The following are examples of use for a non-intended purpose.

(1) Accessing a site for a non-intended purpose from a location on campus

Browsing any of the following types of sites using a network belonging to the Institute (including via Wi-Fi):

- Sites for the unlawful downloading of music or movies
- Sites for the unlawful downloading of commercial programs
- Sites for games or adults-only content
- Sites for the downloading of cracking tools

Do not access such sites because they are a potential source for a virus infection or may otherwise cause problems.

(2) Using a personal computer for a non-educational or non-research purpose

Do not use a personal computer to produce a flyer for your part-time job or to engage in a political or religious activity.

(3) Use of Winny or any other file-sharing software is prohibited.

Since file-sharing software poses a substantial security risk, you are urged to avoid using such software even at home.

Cooperating with operations

(1) Connecting a personal computer or smartphone not protected by antivirus measures or a personal computer that may already be infected by a virus to a network can infect other people's personal computers and smartphones. Do not connect a personal computer or smartphone that may already be infected by a virus to a network since this action could cause the network in a laboratory or elsewhere to shut down.

(2) A network is a finite resource shared on campus. Effective use of this resource requires that users refrain from accessing and monopolizing it. For example, you should avoid downloading massive files as this can strain the network for a prolonged period of time.

(3) In order to obtain a prompt resolution in the event that a personal computer provided by the Center has failed, a service defect has occurred, or a relevant malfunction is otherwise detected, contact the Information & Education Center's Technical Office.

Inquiries, consultations, and the submission of reports
Information and Education Center, Technical Office (C301)
Telephone: 0143-46-5895 or 0143-46-5896
Website: https://wp.mmm.muroran-it.ac.jp/

3. Proper use of IDs and passwords

- **Use strong passwords and change them regularly**
- **Do not use your on-campus passwords as passwords in other areas of your life**
  (Prohibition against the recycling of passwords)
- **Do not let others know your passwords**
  (Do not write your password on a sticky note affixed to your personal computer)

IDs and passwords are used as means of authenticating the individual. The theft of an ID or password could allow a third party to use a system and steal information. You will need to thoroughly manage your IDs and passwords.

Setting up a password

(1) Set up a password consisting of a combination of eight or more alphanumeric characters and symbols.
(2) Do not use words that can be easily surmised in case a dictionary attack is carried out in an effort to crack your password.
(3) Regularly change your password.
(4) Do not use a password you use for services provided by the Institute for services provided by outside parties. If a password you use for a service provided by an outside party were to be leaked, there would be a greater chance that a service provided by the Institute could be compromised.

Managing your IDs and passwords

▪Protect your IDs and passwords from other people.

It is important to manage your IDs and passwords to prevent them from being leaked to outside parties. Do not engage in actions by which your password is revealed to another person or by which your password is written on a sticky note that is affixed to a personal computer. Do not post your ID or password anywhere where it might be seen by a large number of other people, such as an on-campus bulletin board.

▪Do not leave any Center-issued notices in a classroom or other location.

After changing the initial password, discard your notice.

▪The lending or borrowing of IDs is prohibited.

For example, even where permitted by a friend, do not use your friend's ID or password to log on to a system or use a service.

▪Exercise caution when it comes to ID linking.

For social-networking services and other types of services, a means of logging on to the service by way of linking to the user's ID is sometimes provided. (For example, you might log on to Instagram with your Facebook account.) If an ID is linked in this way and the linked ID or password is then leaked, multiple services might possibly be compromised. The management of IDs and passwords requires greater care under these circumstances.

4. Personal computer software

- **Do not use operating systems and applications that are no longer supported by the publisher.**
- **Be sure to update operating systems and applications.**

Software for a personal computer is “raw.” Basic software (operating systems) and application software are supported by software vendors for a fixed period of time. The continued use of software that is no longer supported is risky in that it could allow vulnerabilities to be exploited and the software to be infected by a virus.
Be sure to use software that is supported.
Connecting an operating system that is no longer supported to a campus network is prohibited by the Muroran Institute of Technology. If you wish to use an older personal computer in a laboratory or elsewhere, verify that the deployed operating system continues to be supported.

Prohibition against the use of an operating system that is no longer supported

Use an operating system that is currently supported and refrain from using an operating system that is outdated. The following operating systems are not permitted to be connected to a campus network:

- Windows: Windows 8.1 or earlier, Windows10 Version 20H2 or earlier
- macOS: macOS 10.14 Catalina or earlier

Automatic updating of an operating system

Enable automatic updating of the operating system and be sure to install an update whenever one has been announced.

Prohibition against the use of an application that is no longer supported

Use supported applications and refrain from using applications for which support has expired.
The following applications are no longer supported as of April 2020; they are not to be used:

- Adobe products
  - Any version of Acrobat up to and including Acrobat 2017, / Acrobat Standard 2017/ Acrobat Reader 2017
  - Acrobat DC Pro / Acrobat DC Standard /Acrobat Reader DC
- Java related products
  - Products other than Oracle Java 10(LTS), Oracle Java 17(LTS)
  - Products other than OpenJDK 11(LTS), OpenJDK 17(LTS

Updating applications

Be sure to update applications. Where possible, configure to allow automatic updates to maintain your applications in an up-to-date state.

5. Software licenses

●Use software under license
(Do not use pirated software)

PC software constitutes copyrighted works for which the scope of allowable use is stipulated in the terms and conditions of a license. Use such software properly in accordance with the terms and conditions of use. If you were to violate the terms and conditions of a software license, you and/or the Institute could be sued by the copyright holder or punished under the law.

Complying with a software license

Use software in accordance with the terms and conditions of the license. Do not install software for which you have not been granted a license or software with an unclear license that has been downloaded from the Internet.

Using freeware

Freeware (for which no license fee is charged) is available on the Internet. In using freeware, you must pay attention to the following points:

・Verify the terms and conditions of the license

Freeware licenses come in various forms. In some cases, commercial use is prohibited. For this reason, you will need to confirm that there are no problems posed by the purpose for which you intend to use the freeware in question.

・Source

Obtain freeware from a trusted site, such as the site of the publisher or a major repository of software. Keep in mind that software that may be infected with a virus or that has been maliciously tampered with are in circulation.

Prohibition against the use of altered software

Refrain from downloading from the Internet any commercial software that has been unlawfully tampered with to eliminate the need for activation (pirated software) and the use of such software. Even if software has been tampered with to avoid activation, communications with the software vendor's activation server may still occur when the software is launched. Communications could allow a commercial software vendor to detect that software is being unlawfully used by someone at the Institute. There have been cases in which users and universities have been sued for license violations.

Use of software licensed to the Institute

Software licenses obtained by the Institute can be used only for as long as you are enrolled in the Institute.

- Microsoft (EES)
- Apex One

Any software licensed to the Institute should be uninstalled after the user graduates since such a license cannot continue to be used in that case. The software will need to be repurchased if you wish to continue using it after graduation.

6. Antivirus software

Be sure to install the software that is provided by the Institute (Apex One)

Inadequate if only using Windows Defender

Install even if you are using macOS or Linux

Enable virus protection (real-time scanning) and have pattern files automatically updated.

Regularly perform a full scan.

If you connect a personal computer into which no antivirus software has been installed to the Internet, you will be sure to cause your computer to be infected with a virus at some point. Be sure to implement antivirus measures. Connecting a personal computer that is not protected by antivirus measures to a network operated by the Institute is prohibited.

Installation

Once you have purchased a personal computer, be sure to install Apex One, software that is provided by the Institute.

While Windows comes with Windows Defender, this option is inadequate as an antivirus software tool since its detection rate is low, and it is updated infrequently. Apex One should also be installed for macOS and Linux computers since there many viruses that target these operating systems as well.

If your purchased personal computer comes with preinstalled commercial antivirus software, it can be used as is without modification. Since such software can no longer be used once the trial period or license term expires, however, you should install Apex One before the license for the preinstalled commercial antivirus software expires.

Updating pattern files

Once antivirus software has been installed, enable real-time scanning. This feature will check for viruses when you save a file (virus check).

In addition, turn on automatic updates to ensure that your virus pattern definition file is regularly updated.

Performing regular scans

While a virus check will be performed whenever a file is saved when real-time detection scanning is turned on, a virus pattern updated sometime after a file is saved could recognize new viruses in the file that managed to go undetected earlier. For this reason, you should regularly (see Supplement 1) perform a full scan (see Supplement 2) to check to see whether existing files have been infected with viruses.

Supplement 1: Should ideally be performed at least once a week.

Supplement 2: If a full scan is not available as an option, scan your personal computer's hard drive (HDD).

What to do in the event of a virus infection

If symptoms of a possible virus infection, such as where something is abnormally displayed on your personal computer or where your personal computer is operating very slowly, is apparent, please do the following:

Step 1 Take your personal computer offline

Unplug the network cable and turn off the wireless LAN (Wi-Fi) feature (in order to block any attempt to attack other personal computers via the network).

Step 2 Obtain the required antivirus software using another personal computer

Download the latest version of the required antivirus software (Apex One) installer using another personal computer not suspected of being infected with a virus.

Step 3 Install the required antivirus software

Using a CD or USB thumb drive, save and run the required antivirus software (Apex One) installer on the affected personal computer.

Step 4 Update the pattern file

Connect to the network and update the pattern file for the required antivirus software.

Supplement 1: Update only.

Supplement 2: You should not connect to a network when your personal computer is in a state where it is or is suspected of being infected with a virus. If possible, also obtain the latest pattern file in Step 2 and carry out Step 4 on an offline basis. These days, however, some antivirus software tools are premised on the establishment of an online connection, such that updating may not be possible unless you are online.

Step 5 Perform a full scan with your personal computer in an offline state

Disconnect once again from the network (carry out Step 1). You should then perform a full scan with the antivirus software to remove the virus.

Step 6 Update your operating system

Connect to the network and update your operating system. (Use Windows Update for Windows and Software Update for macOS. The name of the relevant feature varies depending on the specific operating system in the case of Linux.)

If you run into difficulties, such as not being able to remove a virus, please contact the Information & Education Center.

- **If you cannot get in touch with the Center**
  Turn off the affected personal computer while it is offline. If you are attempting to deal with the situation yourself, search for information with a safe personal computer and exercise prudence to ensure that information can be trusted. Note that you might come across fake solutions and tools.

7. Use of smartphones

Use supported devices and operating systems and avoid using older devices.
Obtain applications from trusted sources and be sure to keep them updated.
Lock your device with a password or biometric tool and implement measures to ensure that you do not lose your device.
Use features designed to protect you in the event that you lose your device.

A smartphone is functionally equivalent to a personal computer and requires security measures to be implemented. Since it typically holds a substantial amount of information that cannot be leaked without causing problems, such as the addresses of and contact information pertaining to your friends and acquaintances, you will need to protect it against malicious applications. Measures must be implemented since the potential damage caused by the loss of your smartphone, which you carry around with you every day, is huge.

OS

Older operating systems are vulnerable and can be infected by viruses if used. Be sure to update your operating system. You will enjoy peace of mind if you set up automatic updates. Use supported devices and operating systems and avoid using older devices. The Muroran Institute of Technology prohibits the connection of smartphones that are no longer supported to a campus network.

Applications

Obtain applications from trusted sources (such as an official app store). An application distributed online through unofficial channels can result in a leakage of information stored on your smartphone or come with malicious features. Since a vulnerability might be detected even after an application has been installed, replace any obtained application with an updated version whenever one is released. If you are using a social networking app, set it up to prevent personal information from being divulged unintentionally.

Protection

Lock your smartphone with a password or biometric authentication feature in order to prevent it from being used by others. In addition, attach a strap to your smartphone or otherwise implement measures to prevent it from misplaced or left behind in a location. In order to ensure that information is not leaked in the unlikely event that you lose your smartphone, it might be a good idea to configure your smartphone in advance to enable it to be remotely swiped.

8. Use of email

Confirm the email address of the intended recipient before pressing the send button.
When sending an email message, be sure to fill out the subject field.
Discard spam messages without reading them and do not click on URL links or open attachments.
Implement measures to prevent information leaks when using a free email service.

Points to keep in mind when drafting an email message

- **Avoid sending email by mistake**

  Since an email message cannot be canceled once it has been sent, be sure to confirm the email address of the intended recipient for any errors before sending it. You are urged to use a feature that allows you to preview the contents to be sent or a feature that can delay the transmission of a message (until a certain period of time passes after the send button is pressed).

- **Add a subject**

  Add a simple subject to an email message as a way to describe the contents of the message.

- **When sending an attachment, indicate the fact that you are doing so in the text of the email message.**

- **Do not send very large files (of several tens of megabytes in size or larger).**

Points to keep in mind when receiving email

- **Discard suspicious email messages without opening them**

  Be especially careful about email messages received from strangers. Check to make sure that an email message is not spam and that the source has not been spoofed. Determinations can also be made in part by looking at the subject. If an email message lacks a subject, it could be spam, in which case, you should discard it without reading its contents. Even if you have no choice but to check the contents of an email message, refrain from clicking on any URL links or opening any attachments included in the email message.

- **Do not use HTML email**

  Configure your email software to ensure that messages are received in plain text format and not displayed in HTML format. If you were to open an HTML email message, any linked image

or file will be automatically downloaded, thereby enabling the sender to know that you have read the email message.

Use of email services not provided by the Institute

If you use Gmail, Yahoo! Mail, or any other email service not provided by the Institute, the provider of the service might read the contents of the body of your email message.

Use such a service while keeping the following points in mind:

- **Do not use an email service not provided by the Institute for a commercial purpose.**
- **If you need to use an email service not provided by the Institute, do not send confidential contents, such as grade-related information.**
- **If you need to send grade-related information or other confidential contents using an email service not provided by the Institute, protect the contents to be sent with a password and encrypt the message before sending it.**

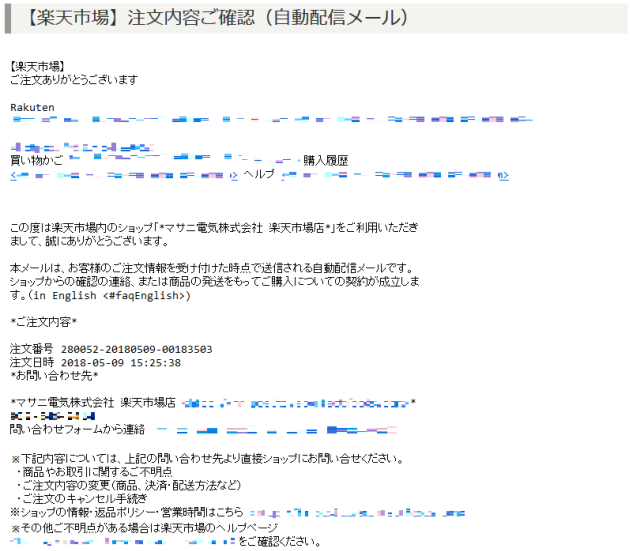
Beware of phishing email

Phishing email refers to an email message sent by someone claiming to be a legitimate company or organization in an attempt to induce the recipient to visit a malicious site where the recipient's information will be obtained by deception. If you receive an email message that you do not recognize, delete it without clicking on any links or opening any attachments included in the message.

Example of phishing email

The volume of suspicious email messages being sent has been growing in recent years. There are plenty of examples of sophisticated email scams that have been perpetrated by senders claiming to be public institutions or major companies or that are designed to look like automatic notifications sent by delivery companies or as part of the procedures for online purchases.

[Actual example] Email purporting to be from Rakuten



【楽天市場】注文内容ご確認（自動配信メール）

【楽天市場】
ご注文ありがとうございます

Rakuten

買い物かご ・購入履歴
ヘルプ

この度は楽天市場内のショップ[*マサニ電気株式会社 楽天市場店*]をご利用いただきまして、誠にありがとうございます。

本メールは、お客様のご注文情報を受け付けた時点で送信される自動配信メールです。
ショップからの確認の連絡、または商品の発送をもってご購入についての契約が成立します。(in English <#faqEnglish>)

ご注文内容

注文番号 280052-20180509-00183503
注文日時 2018-05-09 15:25:38
お問い合わせ先

*マサニ電気株式会社 楽天市場店
問い合わせフォームから連絡

※下記内容については、上記の問い合わせ先より直接ショップにお問い合せください。
・商品やお取引に関するご不明点
・ご注文内容の変更(商品、決済・配送方法など)
・ご注文のキャンセル手続き
※ショップの情報・返品ポリシー・営業時間はこちら
※その他ご不明点がある場合は楽天市場のヘルプページ
をご確認ください。

9. Use of LINE

Use LINE with an understanding of the risks involved.
Set up the app to prevent the loss of your address book and other content.
Do not receive any message or call from someone you have never met in person.

LINE is widely used as a casual means of transmitting information to others. It is popular among university students and is used by almost our entire student body.
Use this app safely by observing the following precautions.

Prevent your friends list from getting leaked

Implement strict privacy controls to prevent your friends list (address book) from becoming leaked.

Examples: Make the following settings through "Add friends":

- **Turn off "Auto-add friends."**
- **Turn off "Allow others to add me."**
- **Under "Privacy," turn off "Allow others to add me by ID."**

If you fail to make the above settings, you may soon find unintended "friends" registered to your friends list, and they will be connected to you as friends before you are aware that this is happening.

To avoid getting involved in crime

In order to avoid the risk of becoming involved in a crime when you are contacted by a stranger, endeavor to implement the following measures.

- Block messages and telephone calls from strangers.
- Do not exchange IDs through the Internet with strangers.
- Since hijacked accounts are sometimes used for criminal purposes, make sure that your own IDs and passwords are carefully managed.

Risk of an information leak

The contents of even messages that you exchange with only friends can be viewed by a service provider. The exchanging of important information by other means needs to be considered.

10. Using a social networking service (SNS)

Use social networking services with the understanding that they constitute space that is public in nature.
Do not exchange personal or sensitive information.
Do not make slanderous remarks about others.

Using an SNS

Twitter, Facebook, Instagram, LINE, and other social networking services are popular as media channels for the informal exchanging of information and are casually used as a way to exchange information with friends.

While these services are convenient, they also come with risks. For this reason, you will need to be careful when transmitting information.

Precautions for use

- **Be aware of contents you transmit**
  Transmit information with the awareness that there is no anonymity when using an SNS. Even if you think that nobody has seen your post, it can still be found later by searching the network. For example, there have been cases in which someone who may have posted about an unlawful or unethical action that had been taken was then identified and severely criticized (flamed online).
- **The releasing of information cannot be undone**
  Once information has been released to the Internet, it will be cached on networks and cannot ever be erased even if the original post is deleted.
- **Do not transmit personal or sensitive information**
  Refrain from exchanging the following types of information using an SNS:
  Personal information: Information that can be used to identify an individual, such as a name, address, date of birth, gender, telephone number, or email address.
  Sensitive information: Bank account number or balance figure; credit card number or whether you have any debts outstanding; health insurance card number or other related information; medical information, such as your medical history, the details of any chronic illnesses, and your blood type; information on your family, relatives, and hometown; and information related to personal interests and preferences.
- **Do not transmit anything that is slanderous or defamatory**
  A post that slanders or defames someone else can eventually reach the person to whom it refers to cause the relationship with that person to become broken.
- **Be aware of any additional information embedded in images**
  An image file also includes such information as the time when and place where the image was taken (EXIF). When uploading images to an image-sharing site, configure settings to ensure that such information will not be leaked.

11. Cloud services

SNS, storage services, email services, and other examples of free cloud services should be used with a full awareness of the risks that are posed.

Do not upload important data.
Encrypt your data.
Back up your data by other means.

Free applications provided online are referred to in this book as cloud services. Cloud services include the following:

- X (formerlyTwitter), LINE, Facebook, and other social-networking services
- Dropbox, Google Drive, iCloud Drive, and other storage services
- Gmail, Yahoo! Mail, and other email services

Cloud services are free to use and convenient but carry the following risks.

Usage risks

(1) Use of user data by a service provider

Free service providers operate by using accumulated user data, which means that you should assume that the contents of data are being used (read). For example, the use of user data includes, but is not limited to, their use for targeted marketing and advertising.

(2) Leakage of user data caused by administrative oversight on the part of a service provider

There is a risk that user data will be leaked to the Internet because of an error in operations on the part of the service provider.

(3) Loss of user data and the continuity of services

There is a risk that user data will be lost because of an error in operations on the part of the service provider. There is also a risk that a service will be unilaterally terminated by the service provider with no warning that might otherwise allow you to recover user data uploaded to the service provider.

Precautions for use

(1) Prevention of leaks (do not entrust)

Do not use for exchanging or accumulating important data or business data whose leakage would cause difficulties.

(2) Prevention of leaks (encrypt)

If you really need to deal with important data or business data, upload after encrypting the data on your personal computer.

(3) Backing up important data

Back up data by way of a method that does not involve a cloud service in preparation for the loss of data caused by an error in operations on the part of the service provider or the sudden termination of a service.

12. Points to keep in mind concerning the transmission of information

Keep the following points in mind when transmitting information.

Do not place sensitive information on an information-transmitting server.
Review information that is transmitted on a regular basis.
Do not infringe on the rights of others.

Keep the following point in mind in order to safely transmit information online.

Ensuring the safety of information-transmitting systems

(1) Ensuring security

Operating systems and software should receive patches and information should be constantly maintained in an up-to-date state. The same applies whenever the production of a page is outsourced.

(2) Prohibiting the use of CGI/SSI and the establishment of public bulletin boards (BBS)

Use of these tools with a public server operated by the Institute is prohibited since they may be used for unintended purposes.

(3) Point to keep in mind concerning hidden directories

Confidential information that will not be disclosed to outside parties should not be stored even in hidden directories.

Review information that is regularly transmitted

(1) Indicate the period for which the information will remain valid

The period for which information published through a web page remains valid should be appropriately indicated. Information should be deleted from a server when its period of validity expires.

(2) Regularly take inventory of information

Take stock of information and review the necessity of the transmission of information at least once a year. Information found during this process to be no longer valid should be either deleted or the period for which it will remain valid should be updated.

(3) What to do in the event of an organizational change

If there has been an organizational change, steps to ensure continuity by the organization taking over operations should be undertaken. (If no such organization exists, then information transmission should be discontinued.)

Respecting copyrights and other forms of intellectual property

Keep the following points in mind:

- Do not infringe the intellectual property rights of others.
- Do not infringe portrait rights, publicity rights, or other such intellectual property rights.
- Do not post content that slanders or defames others or that infringes the privacy of others.
- When using the logo of a company, consult with the other party in advance.
- Be sufficiently aware of the risks you face when exposing your face in photos and through other channels.

13. Information leakage measures

Do not take out unnecessary information and minimize the information you choose to remove.
When taking out information, endeavor to prevent the theft of your personal computer.
Do not store important data on a USB thumb drive and walk around with it in your possession.
When discarding an information device, erase or destroy the hard drive first.

The first way to prevent information leaks is to refrain from taking out unnecessary information. If you have no choice but to take out information, measures to prevent information leakage are vital. When discarding an information device, exercise care to ensure that information is not leaked from the information device to be discarded.

Taking out information

Try to avoid taking out unnecessary information. If you really need to take out information, come up with a way to minimize the information that you will ultimately take out. Configure a login password on your personal computer. Encrypt your hard drive to prevent it from being analyzed if it were to be removed from your personal computer in the event that it is stolen.

Measures to prevent the theft of information devices

If you are traveling by car, refrain from leaving your personal computer unattended in the vehicle as a way to avoid getting it stolen. If you are traveling by train, keep the bag containing your personal computer on your person at all times rather than placing it on a rack. If you are participating in a social gathering while on a business trip, do not bring your personal computer to the venue in question.

Using a USB thumb drive

Since USB thumb drives are easy to misplace, you should avoid keeping important data in these drives and walking around with them on your person. If you have no choice but to use a USB thumb drive, you should use one that comes with an encryption feature or devise a comparable measure to keep your data safe. To avoid accidently taking out information that is not needed, be sure to empty any USB thumb drive that you have finished using before you put it away.

Disposing of information devices

If you wish to dispose of your personal computer, erase information on your hard drive by using dedicated software. If possible, you should physically destroy the hard drive or take similar actions. If you ask an outside business to dispose of your personal computer, ask a business that can be trusted and obtain a certificate of erasure.

Reference: With respect to personal computers for business use, please contact us since the Engineering Department carries out waste disposal on behalf of the Institute.

14. Actions to be taken in the event of a computer security incident

If a computer security incident occurs (or is discovered), calmly contact the CSIRT (Computer Security Incident Response Team).
Notify the CSIRT as soon as possible.

What is a computer security incident?

The following events are treated as computer security incidents:

- Loss or theft of a personal computer or USB thumb drive containing confidential information
- Loss or theft of confidential information (documents)
- Computer virus infection
- Incorrectly sending confidential information by email (incorrect recipient)
- Transmission of a large volume of spam or junk email
- Information leakage from a web server or personal computer (unintended disclosure)
- Information leakage from a discarded information device

What is the Computer Security Incident Response Team?

In the event of a computer security incident, action needs to be taken as quickly as possible to minimize the damage. For this reason, the Computer Security Incident Response Team (CSIRT) has been set up to deal with incidents.

Who to contact in the event of a computer security incident

Email: m-csirt@mmm.muroran-it.ac.jp (CSIRT)
Telephone: 0143-46-5896 (Technical Office, Information & Education Center)

Describe your situation specifically and in detail when you contact the CSIRT.

April 2024: Ver 9
March 2023: Ver 8
April 2020: Ver. 7
November 2019: Ver. 6 (electronic)
March 2018: Ver. 5
March 2014: Ver. 4
March 2012: Ver. 3
March 2010: Ver. 2
March 2009: First version

Editorial supervision and production by
Information & Education Center, Muroran Institute of Technology
https://www.icte.muroran-it.ac.jp