Nagoya University Information Security Guidelines

Revised on June 23, 2011
Revised on June 28, 2012
Revised on August 8, 2012
Revised on October 25, 2012
Revised on October 24, 2013
Revised on January 15, 2015
Revised on December 24, 2015
Revised on February 23, 2016
Revised on December 22, 2016
Revised on February 22, 2018
Revised on February 28, 2019.
Revised on July 2, 2020
Revised on February 24, 2021
Revised on February 24, 2022
Revised on February 16, 2023
Revised on July 4, 2023

Nagoya University

- Contents -

Nagoya University Information Security Guidelines

Introduction

These Nagoya University Information Security Guidelines (hereinafter referred to as the "Guidelines") have been established based on the "Nagoya University Information Security Policy" (adopted by the Council on March 19, 2002; revised on June 21, 2011; revised on April 1, 2016; hereinafter referred to as the “Security Policy”).

These Guidelines shall apply to all organizations and individuals who use information devices and equipment (hereinafter referred to as the “Information Equipment”), and information networks of Nagoya University (hereinafter referred to as the “University”). Accordingly, these Guidelines shall govern all Information Equipment connected to a university-wide information network, Nagoya University Integrated Communication Environment (hereinafter referred to as "NICE"). These guidelines will also apply to Information Equipment such as PCs, smart phones, and tablets, even though they are only for personal use, whenever they are connected to NICE.

All university units and members of the University are required to comply with these Guidelines. To this end, the person responsible for each section shall keep all members of his/her section informed about the contents of these Guidelines. Even those who are not members of the University shall comply with these Guidelines, as far as they are users of Information Equipment at a facility of the University such as the library (including visitors using the library and users of network devices participating in various conferences). Each section may set out its own provisions pertaining to the matters not set out in these Guidelines, if necessary for the section.

These Guidelines consist of the following five chapters and each chapter contains provisions independent of other chapters:

Chapter 1 Information System User Guidelines (User's Guide)
Chapter 2 Crisis Management Guidelines
Chapter 3 Information Security Technology Guidelines (Administrators' Guide)
Chapter 4 Guidelines for Use of Cloud Services
Chapter 5 Information Security Training and Education Guidelines

For those who manage servers and personal computers, please read Chapter 3 carefully.

In operating these Information Security Guidelines, new provisions may be added and amendments may be made from time to time with the changes to information and communication technology

environment. Necessary changes may be also made to the Guidelines to respond to changes that are not predictable at this moment. PR Guidelines and matters concerning violation of guidelines shall be governed by a relevant committee or other body, rather than stipulating them in these Guidelines.

Chapter 1 Information System User Guidelines (Users' Guide)

1.1 Outline

This Users' Guide is intended to provide, as guidance, specific information concerning use of computers and other Information Equipment, and database and other information resources provided by the University for research and educational purposes (including personal computers installed by research laboratories) to which we wish all users to pay particular attention. In this Guide, guidelines for the following matters are provided:

1. Increasing awareness of security
2. Initiation of use
3. Use of Information Equipment
4. Receipt and creation of information
5. Information management
6. Sending information
7. Teleconferencing system
8. Teleworking
9. Risk management
10. Consultation Service Desk

For those who plan to install personal computers, work stations and such other devices, as they fall within the definition of equipment administrator, please read "Chapter 3 Information Security Technology Guidelines" in addition to this chapter.

1.2 Increasing awareness of security

1.2.1 Management of authentication information

Authentication (login) information to access computers or networks is for your own personal use. It should not be used by or given to others or made public. Authentication information includes passwords for Nagoya University ID, THERS Accounts, accounts issued by a department or division (department or division email accounts, etc.), and personally managed accounts (accounts for your own personal computer, etc.)

Authentication methods include authentication using knowledge possessed by the user (for example, user IDs and passwords), authentication using items possessed by the user (for example, IC cards), and authentication using the biological information of the user (for example, fingerprint authentication), etc. It is recommended that you use multi-factor authentication,

meaning a combination of multiple authentication methods, where available. Please be sure to use multi-factor authentication when you handle information requiring protection on servers accessible outside the University.

For password authentication, you must manage your password appropriately. Please do not use a password that can be guessed easily. Your password must be at least ten characters in length and include all four of the following: uppercase letters, lowercase letters, numbers, and symbols. Also, always use a unique password for each service, information system, or other instance for which a password is required. If Information & Communications or a device manager orders you to change your password, or if a password leak is suspected, please change your password at once. Furthermore, please make sure that the new password is not similar to the previous password.

Points to remember

- Character strings that are easily guessable from the user's real name or account name, dictionary entries, or such passwords with numbers swapped in the place of letters, should not be used as they are easily guessable. For example, "123456", "asdfgh", "password", and "passw0rd" are inappropriate for use as passwords.
- If you use the same password across several accounts and services, a password leak at a single one of these services will create a greater risk of unauthorized access to the other accounts.
- Faculty members should not give out their passwords to their teaching assistants. Faculty members are responsible for inappropriate actions committed by their students. When hiring teaching assistants, faculty members should issue them a different password or take other such appropriate measures.
- Do not use your Nagoya University account on computers which are used by unknown persons, such as a computer in an internet cafe.
- To avoid password theft by phishing, be sure take precautions such as regularly checking how to change your password or bookmarking the webpage that allows you change your password.
- If you write your password on a piece of paper, please store it in a place that can be locked.
- If an application requiring muti-factor authentication asks you to "Approve" even if you have not logged in, you must "Deny" the request. Additionally, your password may have been stolen by a third party, so please change your password immediately.

1.2.2 Computer virus

When users receive information through the Internet or other sources, the providers or senders of the information are not necessarily trusted. Users must be aware of risks of computer viruses

and other malicious software and avoid accessing any suspicious information or take other appropriate actions.

Computer viruses that infect computers are spread mainly through e-mail. The way computer viruses infect computers has become more sophisticated over the years. In many cases, fake sender addresses are used. Therefore, you should not open any suspicious attachment attached to e-mail even from a close friend, and check with the sender where necessary, to protect your computer.

Your computer can also be infected through a website you access. Proper steps, such as not accessing any suspicious website, must be taken.

Installation of anti-virus software will have a certain effect on detecting viruses hidden in attached files and detecting infection by viruses downloaded through access to a website.

Intentionally creating and distributing computer viruses is, of course, strictly prohibited.

Points to remember

- An increasing number of malicious viruses are transmitted via e-mail or websites. If infected by these viruses, not only could the system be disrupted, but it could also spread confidential information, as in the case of Sircam. Recovery from such infection requires a great deal of efforts.
- Many computer viruses generate subspecies, and simply installing anti-virus software will not ensure the security. We are seeing an increasing number of cases that a virus invades and spreads over the University's system undetected before pattern files become available.
- Criminals are spreading computer viruses called Bot to take over computers. People do not realize that their computers are infected, as no apparent change will occur even when computers are infected by these viruses. Recovery from such infection requires a great deal of efforts.
- Some viruses automatically attack a large number of computers connected via a network. Some viruses create an access point for unauthorized access and you may unknowingly become an attacker of others through such access point.
- By accessing inappropriate websites, users may be at risk of executing dangerous software which may create security holes or of leaking information concerning automatic authentication (generally called "cookie") without knowledge.
- Free software could be spyware which automatically collects and analyzes individuals' web access trends. By using software with such function, hobbies and taste of users can

be analyzed and disclosed without the knowledge of the users.

- There is software called “Trojan Horse” or ”Trojan” which appears to be useful software but in fact opens a backdoor of the victim's computer for the purpose of tapping or illegally invading the computer.
- Phishing scam which sends e-mail by pretending to be from a financial institution and leads the recipient to a website where he/she is directed to input online banking user information, credit card number, pin number and other information with the intent of stealing such information is spreading.
- Do not open any suspicious e-mail. Do not access to any suspicious websites. Caution is advised to avoid the risk of infection by viruses and warms and the risk of leakage of confidential information.

1.2.3 Copyright and other intellectual property right infringement

Software and many other items are protected by law as intellectual property. It is prohibited to exchange any work created by others using P2P software, or to publish or distribute it using a webpage, without permission from the right holder.

If you obtain software through illegal means (such as the purchase of pirated software) or use software without complying with the relevant license agreement, not only you as an individual but also the entire University could be held liable for your actions.

Reference: Copyright Research and Information Center HP

Points to remember

- Downloading copyrighted materials (music, movies, comics, books, journals, computer programs, etc.), knowing that said materials are being distributed illegally, may be subject to punishment (imprisonment for up to two years, or a fine of up to two million yen, or both) and liability for damages, even if the download is for personal use.
- Downloading or using illegal software is considered copyright infringement, pursuant to Article 119 Paragraph 1 of the Copyright Act. You may be subject to criminal punishment (imprisonment for up to ten years, a fine of up to 10 million yen, or both). In addition, the copyright holder may issue an infringement injunction and/or a claim of damages.
- There may be cases where illegal software posed as genuine software is sold on online auctions. Please be sure to buy software from reputable distribution channels.
- If hardware or software is bought using expenses managed by Nagoya University (including external funds), or if such software is installed, the individual responsible for

the expenses must register the information related to the hardware, software, and installation on the Software Management System (SAM), and manage the software appropriately.

- For restrictions on the use of P2P software at Nagoya University, please refer to Restrictions on the use of P2P file-sharing software posted on the website of Information & Communications, Nagoya University when necessary.

1.2.4 Information leakage

Users must manage confidential information with great care and prevent any information leakage. To protect personal information, you are required to comply with "Tokai National Higher Education and Research System Rules on the Protection of Personal Information."
Great caution is also required when publishing information online.
Reference: Measures to prevent theft of personal computers and information leakage through theft and loss
https://icts.nagoya-u.ac.jp/en/security/pc-security.html

Points to remember

- Do not store examination questions and academic records as is in computer hard disks, as it may possibly lead to leakage of important information. Encrypt such data by installing devices for information management and information leakage prevention (such as hardware key), or take other appropriate measures.
- In principle, it is prohibited to take out personal information from where it is kept, but when doing so, it is necessary to follow the instructions of the information protection administrator (Article 33 of the Tokai National Higher Education and Research System Rules on a Protection of Personal Information). When carrying devices such as laptop computers, tablets, or smartphones that contain confidential information, it is necessary to take utmost care to avoid losing or misplacing those devices, as this may cause an information leak.
- When working in the seat in an airplane or train, a person next to you may be able to see your monitor. This may cause a problem depending on the type of information displayed.
- As mobile phones are becoming more technologically advanced, such as smartphone, they may be a cause of information leakage. Utmost attention is advised when using these devices.
- Sending e-mails containing Confidentiality Level 3 Information is not recommended.
- Sending e-mails containing Confidentiality Level 4 Information is not permitted. If you receive an e-mail containing Confidentiality Level 4 Information, please delete it from

the e-mail server immediately.

- When sending e-mails containing Confidentiality Level 2 or 3 Information, you should use the Nagoya University or Tokai National Higher Education and Research System e-mail services and obey the Tokai National Higher Education and Research System Information Rating Handling Procedures. If an e-mail you received includes confidential information, please do not leave the e-mail on the e-mail servers.
- When using cloud services, you should follow the user guidelines and check the terms of use, regardless of confidentiality of the information being stored there.

1.2.5 Annual information security check

Nagoya University conducts annual information security checks to increase members' awareness of information security and to make information security measures more substantive. Members are required to complete annual information security checks.

1.3 Initiation of use

1.3.1 Information Equipment, and information resources

The University has a university-wide network “NICE” as its information infrastructure. Information Equipment such as computers are classified into those used university-wide such as those in the library and those provided by departments, research laboratories and other organizational units. Information resources are classified into various database provided by the library, information resources provided by each section through web, information resources that are opened to public via Internet, and other types of information resources.

NICE is a network used on campus of Nagoya University. NICE will be used to access information and the Internet within the University. For details, please refer to the description of NICE posted on Information & Communications, Nagoya University.

1.3.2 User registration

To use Information Equipment, and information resources of the University, regardless of whether they are university-wide or section specific, user registration is required. In some cases, user registration may be done automatically for all students, such as the case of Nagoya University Information Media Education System.

As the University provides Information Equipment, and information resources to be jointly used

by its members, the University is in the position to be held liable for inappropriate acts committed by the users. Users are expected to be aware of this fact and act appropriately.

Some of the examples of Information Equipment, and information resources of the University are: Nagoya University NUWNET; Information Media Education System; and computer system for each department.

1.3.3 Connecting Information Equipment to NICE

When users connect Information Equipment to NICE, as a general rule, they are required to apply for authorization to connect to the person responsible for issuing IP addresses or a person to whom the power to issue IP addresses is delegated (IP address administrator). IP address administrators must register information about the equipment with IPDB immediately. When registered information is changed, users must report the change to the IP address administrator to keep the information up-to-date. When communication using an unregistered IP address is detected, the Information Security Office blocks the communication. To unblock the communication, the user shall submit a letter of apology through the head of department (in the case of use without registration of IP address), or file a claim (in the case of unauthorized use by outsider). When connecting information equipment to a specific network of a section or a research laboratory, users are also required to apply for authorization to connect to the network administrator. When connecting Information Equipment to NICE through Nagoya University NUWNET, application for authorization to connect will be made through the connection authentication process. When using Information Equipment brought into the University from outside, please make sure that such devices and equipment are not infected by viruses before connecting them to NICE.

1.4 Use of Information Equipmen

1.4.1 Proper use

Most Information Equipment of the University are intended to be shared by its members. Therefore, users are expected to be considerate and cooperative to allow many people to use the Information Equipment, and to maintain them in a good condition.

Points to remember

- It is not desirable to use shared terminals, such as those in the library, for yourself for a long period of time during the crowded period.
- A personal website created on a free website outside the University websites with

banner ads which is directly linked from a University website will give the impression that such ads on such website are endorsed by Nagoya University. Such act that may mislead the public is not desirable.

1.4.2 Unauthorized access

The Unauthorized Access Prohibition Act (officially, "Act on the Prohibition of Unauthorized Computer Access") prohibits any individual to whom authentication information is not provided, i.e. an individual who does not have the authority to use from using or attempting to use a computer by obtaining such authentication information by illegal means. The persons who commit such act could be subject to criminal penalties.

Points to remember

- Using and aiding others to use authentication information of others is to constitute a violation of the Unauthorized Access Prohibition Act.
- Altering and destroying information without authorization is to constitute a violation of the Unauthorized Access Prevention Act.

1.4.3 Unauthorized installation, alteration, carrying out and destruction of hardware

Hardware such as computers, printers and network equipment is an integral component of Information Equipment. Unauthorized installation, alteration, addition and carrying out of these Information Equipment without notifying the administrator is prohibited. Intentionally damaging or destroying such devices is, of course, strictly prohibited.

Points to remember

- Destroying network cables and other cables, computer equipment, power supplies and other devices constitutes damage to property, and is subject to a disciplinary action.
- Destroying or removing the University Information Equipment such as network equipment, computers, and their parts is deemed an action infringing property rights of the University, and is subject to criminal punishment and disciplinary punishment by the University.
- Removing and collecting mouse balls and key tops of certain characters on the keyboard without due reason constitutes intentional damage to equipment.
- Connecting computers with no IP address to NICE is prohibited. Unauthorized connection may cause a network trouble.

1.4.4 Unauthorized installation and alteration of software

Altering basic software and application software installed in shared Information Equipment such as computers for Nagoya University Information Media Education System without permission of the system administrator is prohibited. It is also prohibited to install software, such as operating system or application software, in any Information Equipment without authorization.

Points to remember
● Installing games in a terminal in the Information Media Center and rewriting basic software such as OS and application software without permission, even only for a part of it, is a serious violation of rules.

1.4.5 Taking Information Equipment off campus

Authorization is required from the equipment installation manager when taking University-controlled Information Equipment off campus. When taking such equipment elsewhere, please pay attention to the information saved on the equipment. If it contains confidential information, please carefully manage that information by using tools such as password protection and encryption.

1.4.6 Harassment

Behavior such as printing out inappropriate images on shared printers or using inappropriate images as your wallpaper (background image), etc. is inappropriate conduct.

1.5 Receipt and creation of information

1.5.1 Consideration to information created by others

Users can easily create reports, web pages and other materials and information using a computer system by which Information Equipment, and information resources are made available through a network. When creating information, users are required to give proper consideration to and respect for copyright in drawings, photographs, texts, logos, audio sources, programs and other information created by others.

Points to remember
● Using pirated software and unauthorized copy is a violation of Copyright Act. ● Music CDs and software media contain strict terms concerning the extent of permitted reproduction. Unauthorized reproduction and distribution is prohibited. ● Electronic journals are subject to "Fair Use." Printing a large amount of contents and

downloading a large number of titles is beyond the extent of Fair Use stated in the "Guidelines for Fair Use" of Ejournals.

1.5.2 Unintended use

Information Equipment of the University are provided exclusively to promote education and research and to carry out work and supporting business. Therefore, users are required to be aware of the need to draw a line between public and private and to avoid any use that is not in line with the purpose of installing the device (unintended use).

A typical example of unintended use is to accept an order from outside for data entry or program development and use Information Equipment of the University for commercial purposes to gain personal profit. As there are a wide variety of forms and modes of unintended use, in this Guide, some examples of unintended use which users need to be aware of are described under separate categories of users, namely, students, graduate students, and faculties and staff.

Points to remember

- It is not appropriate to use a bulletin board, etc. for private business.
- As a general rule, it is not permitted to do maintenance work for external computers and data using Information Equipment of the University for personal gain.
- Unless unavoidable for research purposes, net auction using Information Equipment, e-mail addresses, domain names and other properties of the University is prohibited. When using net auction under unavoidable circumstances for research purposes, advance permission is required.
- It is inappropriate to use Information Equipment of the University to promote or sell your own publication. It is out of this scope to do so for posting a list of publication or for posting information necessary for sales of text books to the students of the University who are enrolled in the course.

1.6 Information management

1.6.1 Prevention of occurrence of problems

The rapid popularization of network is causing various problems. You could be involved in a dispute caused by a minor error. You could receive unwanted soliciting mail. You could be charged an unexpected amount of money. Proper information management described in the following sections 1.6.2 and 1.6.3 are effective means to prevent such problems from occurring.

1.6.2 Personal information

Please take upmost care in managing your own personal information. Answering a questionnaire to receive a small amount of reward may cause unauthorized and uncontrolled use of your personal information you provided.

Points to remember
● Avoid providing information concerning privacy of others such as e-mail addresses without reason even when asked by a close friend. You should first try to obtain consent from the relevant individual. ● When providing personal information to others via e-mail, it is necessary to act with care, such as inserting a sentence asking "Destroy After Reading" in the mail.

1.6.3 Privacy of others

It is not rare that information provided by others contains privacy information. Common-sense judgment is necessary. For example, e-mail from friends should be handled in a manner similar to handling a sealed lett

Points to remember
● Avoid providing information concerning privacy of others such as e-mail addresses without reason even when asked by a close friend. You should first try to obtain consent from the relevant individual. ● When providing personal information to others via e-mail, it is necessary to act with care, such as inserting a sentence asking "Destroy After Reading" in the mail.

1.6.4 Handling of confidential information at the time of retirement

When retiring from Nagoya University, users are prohibited from taking any information or Information Equipment containing confidential information obtained in the course of their work. Please comply with the following rules.

Reference:

"National University Corporation Act", Article 18

(http://law.e-gov.go.jp/htmldata/H15/H15HO112.html)

"Tokai National Higher Education and Research System Employee Work Rules", Article 28, paragraph (1), item (iii)

(http://www.nagoya-u.ac.jp/extra/kisoku/act/frame/frame110000115.htm)

"Tokai National Higher Education and Research System Rules on the Protection of Personal Information", Articles 10, 33, and 42

(http://www.nagoya-u.ac.jp/extra/kisoku/act/frame/frame110000102.htm)

1.6.5 Sharing Information

When sharing information, not using an appropriate method may lead to the leakage of information. Below are some examples of methods of sharing information

- One method Nagoya University faculty and staff members share information with each other is to share files using NUSS (Nagoya University Storage Service) (for Confidentiality Level 1-3 Information) or NSSS (Nagoya-univ Secure Storage Service) (for Confidentiality Level 1-4 Information).
- You must encrypt the data in accordance with the Nagoya University Information and Communications Internal Rules on the Use of Secure Storage Services if handling Confidentiality Level 4 Information on NSSS.
- Sharing files using Nagoya University ID is available as a method for faculty and staff members to share information on NUSS and NSSS.
- The NUSS upload-only folder is available as a method to receive files from persons outside of Nagoya University.
- NUSS has a function where you can share folders via a URL. Using the URL sharing function as a method for faculty and staff members to share files is not recommended (please share files using Nagoya University ID instead.) When using the URL sharing function, it is required to set a password for any folders you do not intend to make public.

1.7 Sending information

1.7.1 Responsibilities of sender of information

Transmission of information brings numerous advantages to society, but it is also associated with various risks. Users are required to be fully aware of the significance and risks of sending information.

1.7.2 Chain mails/messages

Do not transmit or forward chain mails/messages (messages that try to convince the recipient to spread it via e-mail or SNS). Chain mails/messages overburden the information system. Also, there is a risk of misinformation being spread. Even if the messages are in good faith, please keep in mind that these messages may have a negative social impact.

1.7.3 Invasion of privacy and leakage of information

In general, websites allow people from all over the world to access them. Therefore, proper

judgment is needed when posting information concerning other people's privacy or their personal information online. The same consideration is needed when sending information via SNS or e-mail.

Points to remember

- It is inappropriate to distribute a staff directory and student directory to outsiders without permission of the issuer.
- Citing and publishing biography of others posted on a website with access restriction without the consent of the relevant individual.
- It is inappropriate to disclose secrets obtained in the course of work duties on SNS, etc.
- The reply address for an e-mail received through a Mailing List (ML) is usually set to the ML itself. Sufficient attention must be paid when replying to the person who sent an email out to the ML.
- Similarly, when sending an email, make sure to enter the recipients' addresses into "BCC:" and not "To:" by mistake.
- In addition, caution is required when bringing a webpage online. If unrelated files/data are uploaded by mistake, it may be regarded as leakage of information depending on the contents.

Also, some web services pose a risk of unintended information leakage, depending on the service's properties.

Points to remember

- If you are sharing the URL for information rated Confidentiality 2 or 3 on NUSS, please protect it with a password.
- There are websites that provide a variety of services, but there are cases where the service provider may save any uploaded files or inputted information, or a third party is given such by the service provider. Therefore, carelessly uploading or inputting highly confidential information to websites carries a risk that leads to information leakage. If you are going to handle highly confidential information online, please check the properties of the website, and only use it after confirming that there are no problems.

1.7.4 Copyright/portrait rights/publicity rights

When transmitting information, please be careful that you do not infringe on copyrights, portrait rights, publicity rights, etc.

1.7.5 Slanderous statement

Slandering other people by posting slanderous statements on SNS and elsewhere is prohibited.

Points to remember
● On SNS and online, discussions often devolve into emotional disputes due to misunderstandings and words being misinterpreted. Do not make slanderous statements even on SNS that are anonymous or have limited participants. ● When expressing opinions and commenting on websites of others who express a position different from yours, it is critical to do so reasonably and in good faith.

1.7.6 Unintended use

As a general rule, sending information for the purpose of selling goods or information using Information Equipment of the University is prohibited.

Points to remember
● Using Information Equipment or information resources of the University to sell goods or information is prohibited. ● Posting and sending advertisement using Information Equipment of the University for the purpose of selling goods and services is prohibited. ● Acting as an intermediary in the course of commercial transactions using Information Equipment, and information resources of the University is prohibited. ● Using Information Equipment of the University for political or religious activities is prohibited.

1.7.7 Sending information using social media services

If you are sending information using social media services, please remember the following points.

1. To ensure that all viewers understand that the information is being transmitted from the University, please indicate on a website managed by a Nagoya University domain (a domain ending with nagoya-u.ac.jp) either the name of the account used in the social media service, or the URL of the account.
2. If the social media services provider issues verified accounts, please try to obtain one if possible.
3. Please properly manage authentication information for social media services the same way as you would for University authentication information (please follow “1.2.1 Management of authentication information”).

1.7.8 Websites for off-campus use via outsourcing, cloud services, etc.

If you are outsourcing the creation of a website for off-campus use, or you are creating one using cloud services, please make sure to use the Nagoya University domain name (domain name ending with nagoya-u.ac.jp). By using the Nagoya University domain name, website viewers can see that the information is provided by the University.

Points to remember

- If you create a website using an external independent domain, website viewers will have a difficult time determining whether the information is transmitted from the University or by an imposter.
- If you use an external independent domain, it may be used for different purposes (including immoral or antisocial purposes) after you abandon its user rights.
- If you are using the Nagoya University domain name for a website using cloud services, please submit the "Guidelines for Use of Cloud Services Checklist" to Information and Communications.

1.7.9 Miscellaneous

In addition to the above, sending any information that is against public order and morals is prohibited.

Points to remember

- Posting and distributing information about suicide methods and bomb manufacturing methods is strictly prohibited.
- Sending indecent images to a specific person repeatedly is likely to constitute harassment. (Source: Harassment Counseling Center)
- Repeatedly sending somebody e-mails or SNS messages despite being rejected by them is considered inappropriate activity.

1.8 Teleconferencing System

If you are using a teleconferencing system for remote classes or teleconferences, attention must be paid to security so that third parties cannot disturb the remote class or teleconference.

1.8.1 Measures to be taken by teleconference participants

1. The client software for teleconferencing systems is updated on a regular basis just as

regular software would be. Please participate in teleconferences using the most recent version of the software.

2. To prevent third parties from participating in the teleconference, please do not tell others the URL of the teleconference.

1.8.2 Measures to be taken by teleconference host (lecturer)

To prevent third parties from entering the teleconference or lecture without permission and interfering with the teleconference or lecture by sharing inappropriate images and sounds, please adjust the settings for the teleconferencing system appropriately.

1. If you can set a password for the teleconference, be sure to set a password.
2. Share the URL for the teleconference only with participants of the teleconference or lecture.
3. If you can restrict the screen-sharing function at a participant level, please adjust the settings so that only the minimum required functions are available for participants.

1.9 Teleworking

As teleworking may involve carrying out University-owned Information Equipment off campus or using personally owned Information Equipment, information security measures different from the ones on campus are required. Also, attention must also be paid to the teleworking environment.

1.9.1 Teleworking using University Information Equipment

If you are teleworking using University Information Equipment, please do the following measures.

1. Before carrying out University Information Equipment, please update the Information Equipment's software and antivirus software to the newest version.
2. If you are saving any information (documents) on the Information Equipment, make sure that the information is permitted to be saved on external Information Equipment, and save the information only after encrypting the information.
3. Use of University Information Equipment for purposes other than for work (such as viewing websites unrelated to work) is prohibited.
4. If teleworking spans over a long period of time, please check periodically that the Information Equipment is updated to the newest version, and make sure that the newest version is installed at all times.
5. When you are returning the Information Equipment used for teleworking to the University

and connecting it to NICE, update the Information Equipment to the newest version and conduct a full scan using antivirus software. Also, please check that there is no unauthorized software installed.

1.9.2 Teleworking using personally owned Information Equipment

1. In principle, University-owned information must not be saved on personally owned Information Equipment when teleworking. However, if the information is expected to be publicized, and the individual responsible for the information allows it to be saved to Information Equipment not owned by the University, then saving is permitted.
2. Before starting teleworking, please update the Information Equipment to the newest version and conduct a full scan using antivirus software.
3. Please check periodically that University-owned information is not saved by mistake on personally owned Information Equipment.
4. When you are finishing teleworking, please conduct a full scan on the Information Equipment using antivirus software. If any malware is detected, save the scan results and report it as an information security incident in accordance with “Chapter 2 Crisis Management Guidelines”.

1.9.3 Teleworking environment

1. When you are teleworking, please do so in an environment where others are not around. This is to prevent information leakage through peeking or teleconferencing sounds.
2. If you are connecting the Information Equipment used for teleworking to the internet, please use a trusted network such as your home network. Please avoid using public local area networks such as those set up at cafes.
3. If you need to step away, please lock your screen so that third parties cannot use your Information Equipment.

1.10 Risk management

When a serious problem occurs to Information Equipment, users must first take emergency measures and then response measures. As used herein, emergency measures refer to the measures to be taken to handle the situation, and response measures refer to the measures to be taken to fundamentally resolve the situation. Please also refer to Chapter 2 as to how to handle crises when they occur.

1.10.1 Emergency measures

When users detect any serious problem in the Information Equipment they use such as virus infection, they are required to take immediate measures such as unplugging a network

connection cable and turning wireless LAN off.

1.10.2 Response measures

After emergency measures are taken, users shall take response measures for the Information Equipment in accordance with the instructions given by the system administrator or the Information & Communications.

1.10.3 Status Report

If users detect any unauthorized access, virus infection or any other information security incident related to the University's or their own Information Equipment or information resources (hereinafter referred to as “incidents”), they should promptly report the situation to Information & Communications. Such incidents should also be reported to the administrator of the Information Equipment in question if at all possible.

Emergency contact in the event of an information security incident
Tel: 052-789-4393 (ext. 4393)
E-mail: security@icts.nagoya-u.ac.jp
Web: https://qa.icts.nagoya-u.ac.jp/

1.11 Consultation Service Desk

The University has established Consultation Service Desk for consultation regarding the use of Information Equipment, information resources of the University. Before contacting Consulting Service Desk, please check Q&A and other pages of Information Security Technology Center website. If you cannot still find the appropriate information, contact Consultation Service Desk.

General Service Desk: IT Help Desk (Tel: 052-747-6389 (ext. 6389))

Chapter 2 Crisis Management Guidelines

2.1 Outline

These Crisis Management Guidelines aim to provide relevant parties with specific information regarding how to deal with incidents that occur when using NICE, computers and other Information Equipment, databases, and other information resources provided by the University for educational and research purposes, in order to understand the situation and to take appropriate measures in an integrated manner.

2.2 Establishment of Information Security Hotline

The Information & Communications shall establish a system (such as Information Security Hotline and IT Help Desk) to report the incident to the Information Security Office, the Information & Communications (hereinafter referred to as the " Information Security Office ") by multiple methods (such as telephone, fax, e-mail and website), and keep all members informed about the occurrence of such incident by posting information about the incident at various places through websites, brochures and bulletin boards.

2.3 Reporting Incident

The first person to find the incident or possible incident shall promptly report the situation to the Information Security Office through Information Security Hotline. Such incident shall be also reported to the administrator of the relevant Information Equipment, where possible.

2.4 Response to Incident

2.4.1 Initial response

As an initial response, the Information Security Office will contact the administrator of the Information Equipment and disconnect the Information Equipment from the network. The target response time shall be 3 hours during the normal operation hours, and 8 hours on holidays and other time outside the normal operation hours.

2.4.2 Emergency measures by Information Security Office

Upon receipt of report of incident, the Information Security Office shall resolve the issue in collaboration with the administrator of the relevant Information Equipment. However, in the

case of emergency, to prevent the damage from spreading, the Information Security Office may, without the permission of the administrator of the relevant Information Equipment, enter the place where the relevant Information Equipment are installed, suspend certain services, and block access to and from outside of the University by certain Information Equipment.

2.4.3 Notice to administrator of information devices and equipment

If the incident has not been notified to the administrator of the relevant Information Equipment, the Information Security Office shall immediately notify him/her of the incident. When a serious incident occurs (unauthorized access, invalid command execution, information falsification, information leakage, etc.), the Information Security Office shall notify also the head of department which the relevant Information Equipment belongs to. If the Information Security Office takes emergency measures without the permission of the administrator of the relevant Information Equipment, it shall explain after the fact about the situation and the contents of the emergency measures to the administrator of the relevant Information Equipment.

2.4.4 Response by the administrator of Information Equipment

After taking necessary measures, the administrator of Information Equipment shall report the situation of the incident and measures taken to the Information & Communications. When a serious incident occurs, the administrator shall report the situation and responses to the information security unit section and the head of department. If the administrator is the person to find the incident, he/she may omit reporting the occurrence of the incident to the Information & Communications. However, if it takes more than 6 hours from discovery of the incident to reporting of completion of handling thereof, reporting of the occurrence of the incident is required.

Points to remember

- In the event that a serious security incident occurs, please follow Information & Communications' instructions for carrying out the preservation of evidence for the Information Equipment. When carrying out the preservation of evidence for an Information Equipment that is suspected to have been infected with malware, do not take any action toward the Information Equipment, instead first disconnect it from the network entirely. Once the Information Equipment has been entirely disconnected from the network, please follow Information & Communications' instructions as to what to do next.
- Please don't access to the disk that is required to preserve evidence. If you need to access it, please contact to IT Help Desk (e-mail: it-helpdesk at icts.nagoya-u.ac.jp, Tel: 052-747-6389) in order to take measures to protect writing (read-only mount, use of the device to

protect writing). The disk to preserve evidence should be kept under the control of the head of department.

2.5 Reporting to Information & Communications

When a serious incident occurs, the Information Security Office shall report the response status to the Information & Communications as they think proper depending upon the situation of the incident.

2.6 Contact to the off-campus organizations

The Information & Communications reports the situation about the event of an information security incident to the off-campus organization such as Ministry of Education, Culture, Sports, Science and Technology, if the university determines that it is necessary to do so.

2.7 Effective use of Incident information

The Information & Communications shall create incident information database which shall be used effectively by the Department of Information Promotion and each information security unit section in carrying out work to help improving information security.

2.8 Establishment of Contact System in Sections

Each section needs to establish contact system in incidents.

2.9 Response on leakage of personal information

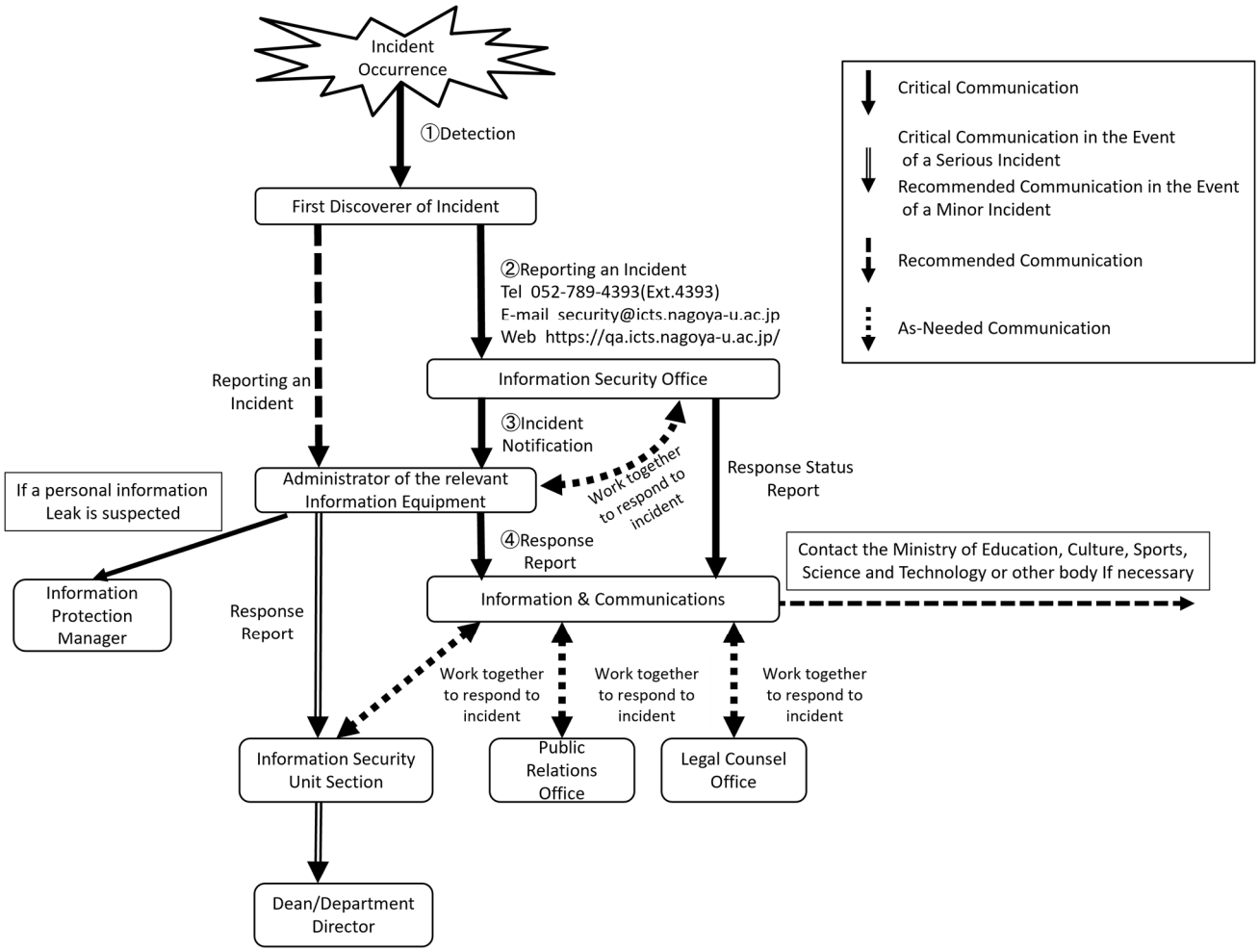
If personal information might have been leaked, please report to the information protection manager in accordance with the Tokai National Higher Education and Research System Rules on the Protection of Personal Information.

2.10 Periodic inspection of Information Security Hotline

The Information Security Office and the administrator of each information security unit section shall check Information Security Hotline as to its proper operation at least once a month.

2.11 Keeping members informed of the risk management and educational activities

Information Security Office shall keep users and administrators informed of the measures to be taken when the incident occurs and the importance of such measures through information security training, and check whether the measures to be taken at the time of occurrence of incident are properly understood.


Incident Occurrence
①Detection
First Discoverer of Incident
②Reporting an Incident
Tel 052-789-4393(Ext.4393)
E-mail security@icts.nagoya-u.ac.jp
Web https://qa.icts.nagoya-u.ac.jp/
Reporting an Incident
Information Security Office
③Incident Notification
Work together to respond to incident
Response Status Report
If a personal information Leak is suspected
Administrator of the relevant Information Equipment
④Response Report
Contact the Ministry of Education, Culture, Sports, Science and Technology or other body If necessary
Information Protection Manager
Response Report
Information & Communications
Work together to respond to incident
Work together to respond to incident
Work together to respond to incident
Information Security Unit Section
Public Relations Office
Legal Counsel Office
Dean/Department Director
Critical Communication
Critical Communication in the Event of a Serious Incident
Recommended Communication in the Event of a Minor Incident
Recommended Communication
As-Needed Communication

Chapter 3 Information Security Technology Guidelines (Administrators' Guide)

3.1 Outline

These Security Technology Guidelines (hereinafter referred to as the "Guidelines") describe guidelines concerning the management of Information Equipment, and information resources to ensure security thereof for all members of the University who connect or wish to connect Information Equipment to NICE. Attention shall be paid to the fact that, as far as Information Equipment that are connected to NICE are concerned, each user thereof becomes the administrator of his/her equipment, even if he/she is using the equipment for his/her own personal use, such as a personal computer, smart phone, or tablet (including personal computers carried into the University by individuals).

As there are other networks other than NICE in the University, in connecting the Information Equipment to a network, the specific network to which the Information Equipment are to be connected shall be confirmed. If NICE is connected to another network, communication failure may occur, causing failure of the entire networks.

If devices are not managed in a proper manner in accordance with these Guidelines, damage and failure may occur and the Information Equipment may become unusable, which may subsequently affect educational and research activities as well as business of the University. If an attack to the devices of the University due to inappropriate management thereof causes any damage to external networks, the entire networks of the University could be removed from the Internet. Please be aware that the management of Information Equipment connected to a network is not only an issue of an individual member of the University but also an issue of the University as a whole.

3.2 Information Equipment to be managed

In these Guidelines, Information Equipment to which these Guidelines apply shall be divided into the following four categories, and the method of management of the Information Equipment to ensure security shall be explained for each category:

1. Network Devices and Equipment
   Router, HUB, NAT, wireless LAN Devices and Equipment, remote access server, DNS server, DHCP server and VNP server

2. Server
   Web server, mail server, name server, file server, computational server and database server

3. Computer for Personal Use
   Personal computer (hereinafter referred to as "PC"), client WS, smartphone and tablet device

4. Special Equipment
   Control equipment, medical equipment, etc.

5. Others
   Printer, scanner, digital multifunction machines, TV conference system, NAS (network attached storage) device, measuring devices and equipment, etc.

3.3 Basic perspective of management of Information Equipment

3.3.1 Appointment of the person responsible for installing equipment and the person responsible for operation and management

Each information security unit section (hereinafter referred to as the "Unit Section") shall appoint the person responsible for installing equipment and the person responsible for operation and management (hereinafter referred to as the "Administrator") for all Information Equipment connected to NICE in accordance with the Nagoya University Information Security Policy and the provisions stipulated by the Information & Communications.

1) Person responsible for installing equipment
   The person responsible for installing equipment refers to a person who finally assumes responsibilities concerning the connection of Information Equipment to NICE. The person responsible for installing equipment may appoint the person responsible for operation and management to fulfill his/her responsibilities. In the case of Information Equipment to be used exclusively by certain individuals such as PCs, the user thereof is the person responsible for installing equipment as well as the person responsible for operation and management.

2) Person responsible for operation and management
   The person responsible for operation and management shall configure the Information Equipment and conduct day-to-day operation and management thereof, and shall be responsible for managing Information Equipment to function properly. The person responsible for operation and management shall have the duty to prepare and maintain an operational and management work record which shall record changes to the configuration of and installation of security patches to the relevant Information Equipment, as a memo for him/herself as well as to prepare for the future replacement of the person responsible for

operation and management. The person responsible for operation and management shall be required to promptly investigate and take measures when network failure occurs due to the Information Equipment operated and managed by him/her. If it is difficult to deal with the situation him/herself, the person responsible for operation and management shall be required to take emergency measures such as immediately disconnecting the relevant Information Equipment from the network upon obtaining the approval of the person responsible for installing equipment.

Points to remember

- There are some devices or equipment still being used without proper operation and management being done due to replacement of the person responsible for operation and management or due to unsuccessful handover of duties at the time of transfer of faculty and staff members or graduation of students. If the person responsible for operation and management is unable to fulfill his/her duty to operate or manage Information Equipment, he/she shall, upon consultation with the person responsible for installing equipment, remove from NICE the Information Equipment he/she is unable to manage, for the secure operation of the entire NICE.

3.3.2 Basic perspective of installation and management of Information Equipment

The Administrator shall have the duty to take appropriate measures in relation to the following two points for the management of Information Equipment:

1) Physical security: The place of installation of Information Equipment and physical access to the Information Equipment

2) Network security: Network access to Information Equipment

For a server, the Administrator shall also have the duty to take appropriate measures in relation to the following two security points in addition to the above two points:

1) Account security: user management

2) File system security: data preservation

In this section, the basic perspective of physical security and network security will be described, and server-specific matters will be described in 3.5 Server.

1) Standards for physical security

When installing the Information Equipment, a place with a secure installation environment where damage by theft and physical sabotage is unlikely to occur shall be selected. In particular, the Information Equipment for the main networks and servers and other important Information Equipment are required to be installed in an environment where physical access to them can be restricted, and managed not to be affected by instantaneous power failure by installing uninterruptible power-supply system, etc.

There have been frequent reports of theft of PCs for personal use. It is necessary to use common sense to manage such computers, such as not easily leaving notebook computers unattended and locking a research laboratory during the night.

In managing the Information Equipment installed in a shared space, it is necessary to take measures to prevent physical sabotage or theft from being committed by not only people from outside but also inside users.

2) Standards for network security

NICE is a network connected to the world, and as such, the Information Equipment connected to NICE are globally accessible. Therefore, the Information Equipment operated as an Internet server shall be configured in such a way to prevent unnecessary services from being activated. In addition, access control shall be properly set up for such Information Equipment by, for example, restricting addresses from which such Information Equipment can be accessed through the Internet.

3.4 Network Devices and Equipment

Network Devices and Equipment to be managed by the Administrator include router and HUB installed for NICE as well as router, HUB, NAT, wireless LAN devices, remote access server, DNS server, DHCP server and VNP server installed by sections and research laboratories for their own use.

3.4.1 Standards for installation

In installing network devices and equipment, attention shall be paid to the following points:

(1) They shall be installed in an environment where entry by unauthorized persons can be restricted (particularly for the main network devices and equipment).

(2) An uninterruptible power-supply system shall be installed (particularly for the main network devices and equipment).

(3) It is desirable to install them in a designated node room.

(4) No information outlet which can be used freely by unspecified users shall be installed.

(5) As in the case of high-performance computers, it is desirable to install high-performance network devices and equipment in a room with air-conditioning equipment to prevent any mechanical failure.

(6) As the smaller the network devices and equipment is, the louder the noise of the cooling fun is, it is desirable to have a node room specifically designated for network devices and equipment.

(7) When installing information outlet in a place where unspecified users can freely enter such as an unlocked class room, it is necessary to take appropriate measures to prevent any unauthorized use of such outlet, such as covering and locking the information outlet.

3.4.2 Duty of Administrator

Caution is required to operate network Devices and Equipment, as a network configuration error may have a significant impact. In particular, when connecting a private LAN operated under a private address to NICE using a NAT, the Administrator shall be careful not to allow packets with a private address to leak onto NICE.

In addition to the basic network configuration, caution is required to the following points:

(1) A password for the Devices and Equipment configuration shall be changed.
(2) SNMP configuration shall be changed.
(3) MAC address shall be used to restrict access (DHCP).
(4) Encrypted communication shall be used.
(5) User authentication shall be used (for remote access)

Leaving the default password for configuration of Devices and Equipment unchanged will invite the risk of the configuration being altered without permission by people who are familiar with the Devices and Equipment or people who learned the default password from the manual published on the Web.

Leaving the default configuration of SNMP unchanged will invite the risk of network information

being stolen or the network configuration being altered.

When creating a wireless LAN environment or installing a DHCP server, please use the method described in the Wireless LAN Security Guideline posted by the Information & Communications to prevent unauthorized persons from accessing. It is necessary to establish minimum section units for each section. The minimum section unit is a seminar or a research group, etc. and the unit should have a responsible person to operate shutdown wireless LAN access points. It will be even securer if they are used in an environment where other users in the subnet are kept away by firewall. Wireless LAN access points connected to NICE, whether directly or indirectly, shall be registered on Nagoya University IP Address Database, as in the case of other equipment.

When installing and operating a remote access server, an authentication mechanism shall be established and used to allow only authorized users to access. It is desirable to limit the scope of a network that can be accessed via remote access server to a minimum, such as within a research laboratory.

When installing a wireless LAN or DHCP server, each Unit Section (sub-net) shall establish its own policy and operate it in such a manner not to cause any subnet conflict. When installing the Devices and Equipment, "Wireless LAN Devices Configuration Check List" shall be prepared in accordance with the operating policy of the relevant Unit Section, and whether configuration has been actually made in accordance therewith shall be confirmed. Even if configuration is commissioned to a contractor, it is necessary to record that configuration has been made in accordance with the Check List.

If you need to access the equipment from outside campus, you must apply for opening the port according to the manual of IPDB for opening/blocking the port. If the equipment with the IP address is not required to access from/to outside campus, you can apply for blocking the interactive communication.

3.4.3 Maintenance

The network devices and equipment installed for NICE are constantly checked for their condition, and backup maintenance is undertaken to prevent any failure. As failure of network devices and equipment will have a profound effect, it is advisable for sections and research laboratories to take measures similar to those for NICE also for the network devices and equipment installed by them, such as preparing backup network devices and equipment.

3.4.4 Management of operation records

Operation records (logs) shall be kept for at least one year.

3.5 Server

Server devices and equipment refer to Information Equipment used by multiple users through a network, which include a Web server, mail server, file server and database server. For the server, the Administrator has the duty to manage users in addition to the server.

3.5.1 Standards for installation

A server shall be installed in an environment where physical access can be restricted as much as possible. Installation of uninterruptible power-supply system is also effective to deal with instantaneous power failure.

3.5.2 Duty of Administrator

The Administrator shall operate a server in compliance with the following:

(1) The most up-to-date security patch shall be maintained.
(2) Unnecessary Internet services shall not be activated.
(3) Access control shall be in place.
(4) Data backup shall be made periodically.
(5) Data integrity shall be checked. (Particularly for Web server)
(6) Prevention of information leakage shall be in place
(7) Protection of privacy of users shall be ensured.

1) Most up-to-date security patch

When any bug or security hole (defects in the system that allow unauthorized access) is discovered in OS or software to execute Internet service functions for any server, a patch for OS or software version-up is generally provided. Patch information for OS shall be checked on a regular basis (for example, once a month) and the most up-to-date security patch shall be maintained. In particular, when important security information is received, do not put it off. It is critical to take necessary measures immediately. It is also an effective way to turn automatic update feature, such as Windows Update and Microsoft Update, on to automatically install security patches when they become available. Please refer to the Information & Communications' website as needed, as vulnerability information concerning OS and application software is posted on the website.

2) Ending unnecessary Internet services

If unnecessary Internet services continue to be operated without proper configuration, it could create a security hole. A server shall be configured to activate only necessary Internet services.

3) Access control

For a server shared by multiple users, access control shall be in place, if the scope of users who may receive the service can be restricted to some extent, as in the case of computational servers and file servers. For UNIX, tcp_wrapper and similar tools are useful. When publishing information through a Web server, it is important to set up proper access control according to the level of importance of the information.

4) Periodic backup

Data stored in a server shall be backed up on a regular basis in case of disk failure.

5) Data integrity check

Information stored in a server shall be constantly checked for data integrity to prevent any unauthorized alteration. It is not sufficient for a Web server to just store data, but it is critical to monitor at all times whether data stored has not been altered, using tripwire or other similar tools. In the case of dynamic web pages, it is desirous to check integrity of data entered to prevent a cross site scripting attack.

6) Prevention of information leakage

It is desirous to take appropriate measures to prevent any leakage of data stored in a server. Proper update of server program, proper configuration, user authentication and other measures shall be taken with the greatest possible care.

7) Protection of privacy of users

The server Administrator shall promptly respond under its authority to any damage to the network caused by users. In doing so, the Administrator shall keep in mind that he/she shall not infringe upon the users' privacy. For example, he/she shall not access to any file not authorized to access, and when he/she needs to analyze data such as e-mail which contains personal information, he/she shall limit the analysis to only information necessary for resolving the issue.

8) Access restriction

Access restriction to our servers is effective to ensure that they may be operated safely. Measures such as restricting the IP Addresses which have access, disabling password authentication and only using public key authentication for SSH, and changing port numbers

are considered to be effective.

9) Vulnerability checks

It is necessary to take measures such as periodically making use of the vulnerability check tool to conduct inspections of server vulnerability.

10) Web Server Management

If you are using any web applications, please update them regularly. Also, if you are developing your own web applications, it is necessary to be careful to not create any vulnerabilities. If you are contracting to develop a web application, be sure to include countermeasures for typical vulnerabilities (SQL injection, command injection, etc.) in the contract.

3.5.3 User authentication systems

If the Administrator needs to identify a user who has accessed the server or has accessed information on the server and verify that the user is legitimate, they must set up a system that identifies and authenticates users.

When setting up the user authentication system, the Administrator must use an authentication method that provides sufficiently strong protection according to the rating of the information that the users can access.

Points to remember
● If users can access information requiring protection, please prepare a user authentication system using multi-factor authentication.

3.5.4 Maintenance

As any server failure will have a profound impact on many users, when such failure occurs, speedy recovery is required. To this end, mirroring important servers to create server redundancy is desirous.

3.5.5 Management of users

Management of users includes ID (user registration) management and management and education of users.

1) Prompt deletion of unnecessary IDs

In managing IDs, it is important to delete registration of unnecessary IDs such as those of graduated students.

2) Management of temporary IDs

Please pay attention to the following points when managing temporary IDs which become temporarily necessary such as the time of server configuration, multiple server configuration using virtual machines or configuration by a contractor:

(1) Please ensure that you use temporary IDs only when necessary. When you are finished using a temporary ID, please delete it immediately.
(2) Please do not use easily-guessed usernames, such as “guest”.

3) User education

Even if the Administrator manages a server properly, security may be threatened by users' action. The Administrator shall consider user management and education as part of server management. In particular, it is critical to ensure that users avoid:

(1) using a password that can be easily guessed;
(2) writing down their password;
(3) disclosing their user name and password to others; and
(4) allowing their family and friends to use the environment available to them, as doing so will decrease the level of security.
(5) The Administrator shall also check whether user's password is strong on a regular basis, using password check tools, such as crack and John the Ripper, as much as possible.

3.5.6 Management of operation records

When server security is breached, the Administrator shall grasp the situation and investigate into the cause of the breach. Operation records (logs) are needed for such purposes.

(1) Please have system logs, mail delivery logs, Web access logs and other logs which record operational status turned on at all times.
(2) Please store logs for at least one year.
(3) It is advisable to check logs on a daily basis to detect any abnormality.
(4) The default settings for the storage period of system logs may be short. Please check the storage period when setting up the server.
(5) Please be sure to keep a work record for operations related to changes to the system structure, additions/changes of users, backups, installation of patches, etc.

3.5.7 Management of web servers

Conduct the following procedures to prevent the leakage of information or the tampering of contents on a web server:

1) Updating

In order to prevent vulnerabilities from entering into the web server, the following must be maintained continuously, and versions with no confirmed vulnerabilities that could lead to information leakage or tampering should be used.

(1) Web server programs (apache, etc.)
(2) Web applications (WordPress, Joomla, etc.; Plugins included)
(3) Databases used by web applications (MySQL, PostgreSQL, etc.)
(4) Programs used by web applications (PHP, Perl, etc.)

Points to remember
● Some plugins installed in web applications may not have been maintained continuously. It is necessary to regularly check the information of plugins you use and confirm that they have been maintained.

2) Web server settings

(1) When using CMS (Contents Management System), set IP address access restrictions to the management page in order to prevent access by persons other than the CMS administrator. In addition, a sufficiently complex password must be created, rather than continued use of the default password.

(2) The directory listing function should be disabled if it is not needed.

3) Creation of web applications

When creating web applications, make sure to keep in mind their vulnerabilities while designing them, such as SQL injection.。

3.6 Computers for personal use

This section applies to PCs, client work stations smartphones and tablet devices. When using PCs for personal use, be aware that the user is the Administrator.

3.6.1 Scope of duties and responsibilities of Administrator

1) Password setting

A password shall be always set, if password setting is available. Even if the computer is for personal use, please avoid using it without setting a password. Fingerprint and other biometric authentication and TPM (Trusted Platform Module) are effective means for security.

2) Management of shared PCs

For shared PCs such as those used for business purposes, it is necessary to establish an operating policy and appoint a person responsible for operation and management when installing them. Each PC user shall use such PC in accordance with the prescribed operating policy.

3) Management of PCs capable of performing a server function

Even when personal computers, if they are capable of performing a server function, they shall be managed in a manner described in "3.5 Server." Particular attention shall be paid to prevent UNIX/LINUX Internet service, Windows IIS, file sharing or DLNA from being unexpectedly activated.

4) Installation of security patches

When any problem causing security vulnerabilities is found in OS and application software installed in the Information Equipment in use, the manufacture of the software distributes a computer program to correct the problem (security patch). The Administrator is required to check warning and update information posted on the website of the relevant company on a regular basis and take necessary measures. Please refer to the Information & Communications' website as needed, as vulnerability information concerning OS and application software is posted on the website. It is also an effective way to turn automatic update feature, such as Windows Update and Microsoft Update, on to automatically install security patches when they become available.

5) Management of Microsoft Windows

As Windows is widely distributed and used as OS for PCs, many viruses attacking its security holes are created. Infection of NICE by such viruses occurs frequently. The Administrator of Windows PCs shall pay due attention to the following:

a) Enable Automatic Updates in Windows Update.

Update information to resolve security holes of Windows OS is provided frequently. As Windows Update can be activated from the Start Menu and can be easily executed, be advised to execute Windows Update on the first day of each month, or otherwise on a regular basis. Windows has the Automatic Updates feature. By turning this feature on,

update information will be automatically searched and notified, which will prevent you from missing updates.

b) Enable anti-virus software.

The Administrator of Windows PCs has the duty to take virus protection measures. The Administrator shall ensure that anti-virus software is installed in all PCs connected to a network and configure the PCs to be able to use the most up-to-date virus definition files. It will be also a good idea to turn the automatic updates of virus definition files on. For most anti-virus software, by default, the automatic update feature for virus definition files is enabled. Nagoya University is distributing anti-virus software under the site license on the Information & Communications' website. Installing this software is also an effective way to protect PCs.

6) Management of Apple's Mac OS

Mac OS also may be affected by a virus. The administrators should install anti-virus software for Mac OS. Nagoya University is distributing anti-virus software for Mac OS under the site license.

a) Enable Automatic Updates in Software Update.

Like Windows, software updates are provided through network for Mac OS X. This feature is enabled under the standard settings. Software shall be kept up-to-date using the Software Update feature.

7) Management of tablet devices and smartphones

Users should take security measures on smartphones and tablet devices in the same way as personal computers. Users need to update OS to the latest version. Users are recommended to use anti-virus software.

8) Management of application software

As in the case of OS, in recent years, software updates are also distributed through network. It is advisable to enable automatic updates.

3.7 Special Equipment

This section applies to equipment which may cause accidents, disasters, health hazards, etc., and equipment which controls them. The followings are examples of such equipment:

1. Laser equipment

2. X-ray equipment
3. Industrial robots
4. High magnetic field generators
5. Medical equipment

1) Connection of special equipment

As a general rule, you should not connect special equipment with the internet. If this equipment does not work correctly because of illegal access, it may cause accidents or disasters. Even if you connect this equipment to the internet for safety reasons, you should connect it to a private network and use VPN.

2) Connection application

If you connect special equipment to NICE for safety reasons, you should consider the risk and security measures, obtain the approval of the head of department, and submit a connection application form to the Information & Communications in advance.

3) Management of special equipment based on general-purpose OS

As special equipment based on Windows/Linux OS may have a server function, which must be managed as a server and in a manner described in “3.5 Server” as well.

3.8 Taking out and bringing in Information Equipment

1) Permission for taking out Information Equipment

Since notebook computers, smartphones and tablets can be used in different places, you must be careful regarding security. In the case that you take University-owned Information Equipment (including rentals) outside of the university, in addition to receiving permission from the person responsible for installing equipment, you must handle them appropriately depending on the data stored on the equipment and in accordance with what is prescribed in any applicable rules (for example, "Tokai National Higher Education and Research System Rules on the Protection of Personal Information", "Tokai National Higher Education and Research System Information Rating Standards").

2) Bringing in Information Equipment

For connecting Information Equipment to NICE that are owned by the University and have been taken outside of the University or that are owned personally, please check that they have not been infected with malware beforehand. Even though they are your personal Information Equipment, when you connect them to NICE, you must take the same security measures as for the University Information Equipment.

3.9 Other Information Equipment

This section applies to Information Equipment aside from network devices and equipment, servers, personal computers and special equipment. This is applicable for printers, scanners, digital multifunction machines, TV conference system, NAS (network attached storage) devices, measuring devices and equipment, etc.

1) Password setting

A password shall be always set, if password setting is available. Even if the devices and equipment are for personal use, please avoid using them without setting a password. Even such devices like network printers which appear to have nothing to do with a password sometimes have a password setting. The default password shall not remain unchanged. Please set an appropriate password.

2) Management of other Information Equipment

Operating systems based on the Linux kernel are used in these devices and equipment. Therefore, it is required to update firmware periodically. If it is impossible to modify a vulnerability used by attacker, please don't connect it with the global network.

Points to remember

- To prevent any information leakage, please connect printers and scanners, digital multifunction machines, NAS (network attached storage) devices to a private network. The Information & Communications provides Secure NICE as a service for secure private network.
- Other Information Equipment, aside from those required to connect to the global network such as TV conference systems, are not permitted to make connections to the global network as a general rule.

3.10 Encryption methods

There is always the risk of leakage, with or without malicious intent, when communication is made through a network or information is stored in a computer. Encryption of information can be used as means of preventing leakage. More specifically, there are following encryptions:

1) Encryption of websites

By setting the entire website to use an Always-On SSL (AOSSL), you can mitigate security risks such as catfishing and communication interceptions. Widely-used internet browsers

may also notify you by an alert via the address bar when a website does not use an AOSSL. Please make sure that the website's URL starts with https:// and that a proper certificate is used. You can use the Nagoya University Web Server Certification Issuing Service (https://upki.icts.nagoya-u.ac.jp/csi_server_cert/) for server certifications.

2) Encryption of electronic mail

When communicating important contents via e-mail, the contents shall be encrypted. Please use a mail client or tool with encryption function, such as PGP.

3) Encryption of data files

There are many tools available to encrypt data files stored on a computer.

4) Encryption of communication

Please refer to the "CRYPTREC Cryptographic Operation Guidelines" and be sure that the protocol adopted for encrypting communication is one whose safety has been adequately confirmed.

URL: https://www.cryptrec.go.jp/op_guidelines.html

Points to remember_

- As the safety of protocols before TLS 1.1 cannot be adequately confirmed, they must be set to unavailable so that they will not be used._

3.11 Remote access environment

Caution is required with remote access environments, including use of VPN (Virtual Private Network) servers and remote desktops, because they are entryways into the university network from the outside. Therefore, for equipment set up inside the university on which VPN servers or remote desktops are enabled for use, please submit an application for opening a port through the "IP address management system." The application may not be approved, depending on the situation or purpose for opening the port. VPN is planned to be integrated gradually into the VPN service provided by the Information and Communications.

1) Preparation of procedures for commencing/terminating use

Procedures for commencing use of remote access environments must be prescribed so that only users requiring remote access can use the services. Similarly, procedures for terminating use must also be prescribed in order to disable user accounts that no longer require access, and a review of the users who have been granted access should be carried out at least once a year.

2) User authentication

Passwords for user authentication must be unique (do not reuse passwords from other systems).

3) Access to information

Do not place confidential information, etc. on a system configured as a remote access environment. In addition, the university system accessed through the remote access environment should be at the very least limited by IP address.

Points to remember:

- Some e-journals and Site License Software prohibit access through remote access environments. Please be careful not to violate these licenses.

4) Authentication log

A record of the authentication log must be kept for at least one year. Also, regular log checks are required to inspect for unauthorized access.

Chapter 4 Guidelines for Use of Cloud Services

4.1. Outline

In this chapter, guidelines are provided for all university members who intend to use a cloud service, so that they can use the cloud service safely. Generally, cloud services are operated by sharing computer resources with other users under the management of the cloud service companies. Therefore, it is always necessary to be aware of the mode of operation when dealing with information through cloud services. These guidelines explain the issues to be aware of when selecting a cloud service. Furthermore, please make sure to consult with Information and Communications in advance when dealing with sensitive information through cloud services.

4.2. Selection of cloud services

When using a cloud service, it is important to fully grasp in advance how the cloud service is operated. The following are points to be taken into consideration when selecting a cloud service.

4.2.1 Connecting to cloud services

Using a cloud service means using servers external to Nagoya University. Therefore, in order to ensure safe communication between the cloud service system and the computer used for the service, confirm that the items below are satisfied.

1) Encryption of communication

Confirm that communication from the user's computer to the system can be encrypted.

2) Access restriction

Regarding access to the system, confirm that access can be restricted by IP address. Also, restrict access so that only specified university computers can use the cloud service system (While access to some website pages are intended to be open to the public and should not be restricted, access to other pages such as the website management page should be restricted.)

4.2.2. Security measures for cloud services

It is necessary to be aware of security issues, even with cloud services. The following items should be checked and confirmed when selecting a cloud service:

1. Security policy

Check the security policy under which the cloud service is operated.

2. Malware countermeasures

Confirm that malware can be detected and defended against.

3. Action taken in the event of security incidents

Check how the cloud provider responds when security incidents occur.

4. System log

Make sure that the log for the cloud service system can be browsed.

4.2.3 Terms of contract

1. Clarification of the scope of responsibilities

Clarify the scope of responsibilities and damage compensation between the university and the cloud provider at the time of entering into a contract by means such as having documentation issued.

2. Applicable laws and regulations

Check which laws and regulations will be applied in case of a dispute.

4.2.4 Handling of data

1. Ownership of data and authority to use data

The ownership of data and authority to use data on the cloud service must be clarified by checking the documents provided by the cloud provider, or by having documents issued when entering into the contract, or by other means.

2) Handling of data upon termination of contract

Confirm that the data on the cloud service and the users' data are properly deleted upon termination of the contract.

4.2.5 Service quality confirmation

Make sure that, when you intend to use a cloud service for a long time, the cloud provider has the capacity to provide the service for such a long period of time. In addition, confirm in advance that the utilization rate, response time, and other performance aspects will be sufficiently provided.

4.3. Use of cloud services

4.3.1 Management of user information

As is the case with other Information Equipment, passwords must not be easily guessable, and should be different from those used with other services.

Chapter 5 Information Security Training and Education Guidelines

5.1 Outline

The Security Policy points out the need of awareness of risks and responsibilities associated with openness and convenience of Information Equipment, and information resources and provides for the "introduction of training system and implementation of educational activities." These Information Security Training and Education Guidelines (hereinafter referred to as the "Training Guidelines") are intended to provide specific guidelines concerning implementation of training and educational activities.

5.2 Information security training and education system

Information Security Training and Education Committee (hereinafter referred to as the "Training and Education Committee") shall be established as prescribed by the Information & Communications within the Information & Communications, and this Training and Education Committee and Information Security Members selected from information security unit sections shall work together to implement training and education.

5.3 Basic perspective of information security training

As a general rule, training shall be provided to the members of the University when: (1) they wish to obtain the authority to use Information Equipment connected to NICE or its sub-network; (2) the devices and equipment they use are connected or they wish to connect the Information Equipment to NICE; and (3) they are involved in the management and operation of NICE.

There are three types of information security training: initial training; periodical training; and special training. The training shall be provided to network users and the Administrator of the Information Equipment.

5.3.1 Initial training

The initial training shall be provided to persons who obtain the authorization to use various networks of the University for the first time (for example, new students, newly appointed teachers, newly appointed researchers and newly hired staff) and persons who are appointed as the Administrator of the Information Equipment for the first time.

1) Initial training for network users

Information System User Guidelines (Users' Guide) and other materials shall be used as training materials for the training for network users, and the training shall be provided with a focus on the following four issues through, among other methods, providing guidance or e-Learning:

(1) Purpose and importance of information security;
(2) Things users are permitted or not permitted to do;
(3) Measures to be taken by users when problems occur; and
(4) The need to be prepared to deal with information security for users themselves.

2) Initial training for persons who wish to connect the Information Equipment to NICE

The Information Security Technology Guidelines and Information System User Guidelines separately prepared and other materials shall be used as training materials for the training for Administrators, and the training shall be provided with a focus on the following four issues:

(1) Purpose and importance of information security;
(2) The need to be prepared to deal with information security for Administrators themselves;
(3) Information security technology Administrators are expected to have; and
(4) Measures to be taken by Administrators when problems occur.

3) Initial training for persons who manage and operate NICE

Training plans for initial training for those who manage and operate NICE shall be prepared by the Information & Communications.

4) Basic perspective of implementation of initial training

(1) Establishment of efficient training implementation plan

The Training and Education Committee is expected to closely communicate and coordinate with information security unit sections regarding the method for implementation of initial training, and to ensure that the initial training plans prepared by information security unit sections do not overlap and the plans are implemented efficiently.

In implementing the initial training, a laborsaving method such as online training shall be used as much as possible, and a mechanism to reduce burden of trainees, such as a system which allows trainees to participate in a training session at any time during the specified period, shall be introduced.

(2) Storing initial training participation record

The Information & Communications or relevant information security unit section shall store a record of persons who participated in the initial training for an appropriate period of time.

(3) Omission of initial training

As a general rule, the initial training shall be provided at each time the authorization to use the Information Equipment is newly granted. However, when the initial training taken elsewhere by an applicant is deemed sufficient, the initial training for such person may be omitted as far as the fact that the applicant has actually taken the initial training is confirmed.

5.3.2 Periodical training

The Training and Education Committee shall provide periodical training in collaboration with the relevant information security unit section. Information security unit sections shall provide their own periodical training as needed.

5.3.3 Special training

The Training and Education Committee shall provide special training in collaboration with the relevant information security unit section as needed. Information security unit sections may, as their own discretion, provide special training as needed.

5.4 Education

The Training and Education Committee shall collect from and provide to users, Administrators and members of the University information concerning information security in collaboration with the relevant information security unit section. To conduct educational activities, various media including mailing list, Information System User Guidelines and Information Security Technology Guidelines on websites, brochures and posters shall be used. All information concerning information security can be obtained from the website of Nagoya University, Information & Communications.