Sophia School Corporation
Detailed Rules for Information System Security Measures

Established; April 1, 2019
Revised: October 1, 2019

Article 1 (Purpose)

Based on Sophia School Corporation Information System Security Rules Article 11, the Detailed Rules stipulate the necessary items for faculty and staff members of Sophia School Corporation (excluding junior and senior high schools, hereinafter called “Sophia School”) to practice as security measures in using the school information system. The Detailed Rules are established for Sophia School to practice smooth and effective information distribution and to operate the information system in a stable and efficient manner while maintaining the highest level of order and safety.

Article 2 (Coverage)

2.1 The Detailed Rules are applicable to all faculty and staff of Sophia School.

2.2 The Detailed Rules shall apply to all the information and devices owned and managed by Sophia School (including those temporarily connected to the network, hereinafter the same).

2.3 Information mentioned in 2.2 shall include “important information” which is defined as follows:

(1) Sophia School’s original information which shall, in case of leakage, damage its social credibility and hinder business operations and research activities. Such information includes but is not limited to the following:

a. Internal information related to management, etc.

b. Information related to entrance exams, regular exams, etc.

c. Information related to research results such as inventions and know-how based on Sophia School’s original research for which a patent application has yet to be made or which has not been disclosed to the public.

d. Information related to Sophia School’s original research contents not yet presented at an academic conference or as an academic paper.

(2) Sophia School’s non-original information or personal information which shall, in case of leakage, violate the law or a contract with a third party, damaging Sophia School’s social credibility and impairing the trust relationship with the third party. Such information includes but is not limited to the following:

a. Information related to personal information and privacy of faculty, staff and students.

b. Information disclosed as confidential items based on contracts.

c. Information provided as confidential items in joint research, entrusted research, etc.

d. Information related to research results such as invention and know-how based on joint /entrusted research for which a patent application has yet to be made or which has not been disclosed to the public.

e. Information related to joint research contents not yet presented at an academic conference or in an academic paper.

2.4 Even in cases where applicable members mentioned in 2.1 use personally owned and personally managed devices, if they are used for business operations or education and research activities, or if they are used by connecting into the network owned and managed by Sophia School, Detailed Rules shall apply.

Article 3 (Specific Information System Security Measures)

Faculty and staff of Sophia School, in using the information or devices mentioned in Article 2, must practice security measures as follows:

(1) Software Vulnerability Measures (OS, Office applications, etc.)

For web browsers, e-mail software, OS, Office applications, etc., in order to prevent malware infection and intrusion into the computer, the following measures must be taken against software vulnerability:

a. Update OS and software regularly.

b. Avoid using OS or software that is no longer supported unless circumstances exist that make this unavoidable.

c. When a firewall is implemented as a standard procedure in the computer, make sure it functions appropriately.

(2) Measures against malware containing viruses (hereinafter, “malware”) for computers, etc.

To prevent information leakage due to malware infection, the following measures must be taken against malware for computer, etc.:

a. Install anti-malware software.

b. Automatically update the anti-malware software definition (pattern) file to keep it up to date.

c. Run virus scan on a regular basis.

d. Stay aware of troubles caused by malware infections occurring inside and outside of the school.

e. When using storage media execute malware check before opening the folder or file.

(3) Security measures for wireless LAN

To prevent communication contents from being stolen, the following security measures must be taken when using wireless LAN:

a. On campus, use Wi-Fi provided by Sophia School unless unavoidable circumstances exist.

b. When working for Sophia School’s operations or education and research activities, avoid using wireless LANs that do not require passwords or use common passwords unless unavoidable circumstances exist.

c. When installing a wireless LAN which was purchased personally by the user, strengthen security by combining WPA2-AES or MCA address authentication.

d. For LAN router name (SSID), avoid using easily guessed names such as that of the user or organization.

e. Use wireless LAN security functions to take all possible measures to prevent misuse by a third party.

(4) Safety measures for file-sharing

When file-sharing becomes necessary for business operations or education and research, the following measures must be taken:

a. When using file server, etc., set access rights appropriately.

b. When use of cloud services is necessary, use OneDrive of Office365 provided by Sophia School as much as possible.

c. When use of external services is unavoidable, use those with trustworthy security measures (e.g. contract terms exists).

(5) Password management

In creating and managing a password, the following measures must be taken:

a. Avoid using easily guessable personal information such as name or birthdate.

b. Try to use 8 or more characters including alphanumeric, combining upper and lowercase letters, numbers and symbols.

c. Avoid leaving a memo with a written password at a place where others can easily see.

d. Never give your password to others.

e. Do not use the same password with multiple services.

f. Use multi-step authentication (security code apart from ID and password) where necessary.

(6) Management of access to important information in sharing devices

When sharing devices, the following measures must be taken to avoid browsing of archived information on the shared device by a third party via network connection, or misuse of the device:

a. Limit the number of persons with access rights to a minimum.

b. Do not use the same ID or password.

c. Avoid keeping the initial password or initial setting.

(7) Measures against targeted email attacks

To prevent damages by targeted attacks via email (emails with skillfully attached malware which appear as regular business communications aiming to steal important information from the targeted organization), the following measures must always be kept in mind:

a. Do not open attached files carelessly.

b. Do not click on a URL indicated in the email carelessly.

(8) Measures to prevent missending of email

To prevent sending an email to the wrong recipients, the following measures must be taken:

a. Check the address carefully (multiple times, etc.) before sending.

b. Check carefully (multiple times, etc.) that the use of “To,” “Cc” and “Bcc” is appropriate.

c. When sending an email frequently to the same group of addresses, use the ML (mailing list) prepared by Sophia School. If you do not use the ML, put your own address for “To” and send the email using “Bcc” for all addresses to be sent. Before sending, also check with multiple persons where necessary to confirm that the settings are correct.

d. Where necessary, use the “confirmation dialogue” function of email software (such as Outlook) which prompts checks before sending.

(9) Measures against information leakage via email

To prevent leak of information via email, the following measures must be taken in handling important information:

a. Sophia account users should use the OneDrive function and set the scope of disclosure strictly, and use methods such as only sending links.

b. Avoid using attached files except under unavoidable circumstances, and use file transfer/sharing services with trustworthy security measures.

c. When sending attached files, use a password and encode the files.

d. Do not indicate the password in the email to which the file is attached. Use other communication methods such as phone or a separate email to inform the recipient of the password.

(10) Avoiding Internet trouble (SNS)

To avoid trouble in using SNS, etc., the following measures must be taken. These measures also apply to the use of the information and devices not within the scope of the Detailed Rules:

a. Use common sense and appropriate manner such as complying with terms of use, etc.

b. Do not carelessly write inappropriate content that violates the rights of others such as malicious slander, illegal information, information which may threaten public safety or order and harmful information.

c. Do not carelessly write your own personal information.

d. Do not write contents that may impair the reputation of Sophia School.

e. Manage the account information (ID, password, etc.) appropriately.

(11) Backup of important information

To prevent loss of data due to breakdown, handling mistake, malware infection, etc. of a computer/storage media, users must backup important information to a file server, external hard disk, cloud service, etc., on a regular basis.

(12) Management of important devices

When important information is recorded on a computer (including a tablet type, etc.), the following measures must be taken to prevent the computer from being stolen or prevent leakage of the information recorded:

a. At the end of business operations or education and research activities, keep the computer in a locked place.

b. Where possible, encrypt the data when using the computer or storage media.

(13) Physical management of important information

The following measures must be taken to physically manage important information, such as preventing the data displayed on the computer (including a tablet type, etc.) screen from being browsed by others:

a. Do not leave the computer (including a tablet type, etc.), storage media (USB, etc.) and documents with important information at your desk or classroom, etc.

b. When leaving your computer, lock the computer screen.

c. Keep the documents with important information in a cabinet with a lock so that others cannot see.

(14) Management related to taking important information out from the facility where it is used.

To avoid leakage of information, the following must be observed in the handling of important information:

a. In principle, it is prohibited to take important information offsite.

b. When handling a computer (including a tablet type, etc.), storage media, and documents with important information, always keep your eyes on it. Be careful not to lose it or have it stolen; for example, do not place it on the rack of a train.

c. If you need to take important information offsite, use encodable media such as USB flash memory that requires a password for reading.

d. Important information must be handled at a place where the access of others is limited. Do not handle in a public space where a large number of the general public can see.

e. When leaving your computer, lock your computer and the room, etc. to prevent others' access to the important information.

f. Avoid physically carrying out important information. Instead, use the cloud service authorized by Sophia School when necessary. In this case, if the user has a Sophia account, OneDrive provided by Office365 is recommended.

g. Check on a regular basis whether important information carried out in the past has been left in the computer or USB flash memory. Delete the information if it is no longer necessary.

(15) Procedures for disposing of unneeded computers

When disposing of items such as a server used for research, one of the following measures must be taken to prevent the risk of theft, information stealing, and direct operation of the item:

a. Erase data using software created for this purpose or ask a professional data-erasing company.

b. Remove the hard disk mounted on a computer or other device and physically destroy it.

c. When discarding medium on which personal data is recorded (CD-ROM, document, etc.), destroy it physically with a shredder or the like.

(16) Proper software management

Since software is protected by copyright, the following measures must be taken:

a. Confirm the usage rights and other details of software licenses.

b. Do not copy the software without the permission of the owner of the copyright.

c. To download software, purchase or get it from an official website. Do not download any software which is suspected as unofficial.

d. Use software as stipulated in the contract.

(17) Server room management

When setting up a server for education and research activities, the room where the server is placed must be managed with the following measures to prevent the risk of theft, information stealing, and direct operation of the server:

a. The room where the server is kept must be locked.

b. Access to the server room must be recorded by access log, etc.

(18) Taking part in information security workshops

To take prevention measures, faculty and staff members must take part in workshops, etc. for information security education held by Sophia School on a regular basis.

Article 4 (Division in charge)

Administrative work related to information system security is handled by ICT Office.

Article 5 (Review)

ICT Office shall conduct timely restudy of the contents of information security measures. When deemed necessary, the measures will be reviewed through discussions with the General Affairs Division and other related divisions.

Article 6 (Revision)

The Detailed Rules shall be revised according to the process stipulated by Sophia School.

Supplement

The Detailed Rules became effective on April 1, 2019.

The Detailed Rules were revised on October 1, 2019.