Center for Information Technology and Management, Okayama University

February 2024 Edition

Security Checklist for Determining the Availability of Network Access at Okayama University

Okayama University aims to reduce security risks by asking students to confirm in advance the security status of the computers they plan to bring to the University and their level of security awareness.

Please answer the following questions and be sure to confirm that your computer is appropriate for connection to the campus network and that you have a high level of awareness regarding security.

1. Check the status of security measures on your computer

In order to connect your computer to the network, certain security measures must be in place. Please make sure that all of the following conditions are met. If you do not have a computer that you plan to bring with you, please proceed to **2. Check your security awareness level** on the reverse side.

	Campus network availability conditions	☑
1	**The computer you plan to bring is installed with an OS*1 that is within the support period.** When an OS for which support has expired is found to have a security flaw called a vulnerability, no patches are provided to eliminate it. In this case, you may be infected with a virus simply by accessing a website. Be sure to install an OS that is within the support period. Note that only students of Okayama University can use software*2 for upgrading to a Windows OS that is within the support period after enrolling in the university.	☐
2	**The computer you plan to bring automatically or periodically updates its OS.** If the latest patches are not applied to the OS within the support period, vulnerabilities may arise in the computer. It is important to promptly apply updates when update notifications are received, etc.	☐
3	**The computer you plan to bring has the scan function of antivirus software (including standard OS*3) enabled and is confirmed to be virus-free.** OS updates that correct known vulnerabilities alone cannot protect computers from unknown viruses or threats caused by user mishandling. Therefore, it is essential to install and activate antivirus software that provides real-time threat detection and protection. Also, if you are using non-standard OS antivirus software, check the expiration date of the license. If it has expired, please activate the scanning function of the OS standard antivirus software and confirm that your computer is not infected with a virus. Please note that only Okayama University students may use the antivirus software*2 provided by Okayama University under a comprehensive contract after enrollment.	☐
4	**The computer you plan to bring is set to enable the screen lock function.** While many of the potential threats that arise through network connections are eliminated by the conditions listed above, if a computer containing various sensitive information is physically accessed without authorization, serious security risks such as personal information leakage and financial damage may occur. The screen lock feature is important to protect yourself from such threats when you are temporarily away from your computer or if your computer is stolen.	☐

*1. For the MacOS, use up to the three latest OS versions as a guideline.

*2. Software license provided by Okayama University (https://www.okayama-u.ac.jp/tp/life/softwareteikyo.html)

*3. Microsoft Defender for Windows OS and XProtect for MacOS are included as standard antivirus software.

Continued on the back side

2. Check your security awareness level

Even if your computer security is strong, security risks may increase depending on the user's awareness. Be sure to confirm that all of the following items are understood and addressed.

	Security awareness check	☑
1	**I understand the dangers in using software that is no longer supported.** As with the OS, vulnerabilities occur when software support expires. Therefore, it is dangerous to use expired software carelessly, even if it is used for experimental equipment, etc. If you have no choice but to use the software, please take measures to prevent the vulnerability from being exploited, such as using the software in an isolated network.	☐
2	**I understand the dangers of using the same password over and over again, and I am taking measures to prevent it.** If you use the same password for multiple services, a breach of login information for one service increases the security risk for all services connected to it. Therefore, we recommend that you avoid using the same password for all services as much as possible. In particular, it is strictly prohibited to use the same password for services within the University as those outside of the University. In addition to extremely malicious acts such as stealing another person's password or attacking or hacking into information systems, it is strictly prohibited to transfer or share your login information (ID and password) with others, as this may encourage such malicious acts.	☐
3	**I understand the risks involved in using suspicious sites, software or files.** Their use carries a high risk of virus infection, personal information leakage, and device hijacking. Do not use suspicious sites carelessly, and use prudent judgment to ensure your safety. There are also phishing scams that use links on websites or files attached to e-mails, which can lead to personal information leakage and financial damage. In addition, be cautious about file-sharing cloud services (e.g., OneDrive, GoogleDrive, BaiduDrive, pCloud, Mega, etc.), which are used often. While these services are convenient and easy to share files, they are also dangerous because the files shared by third parties may contain viruses.	☐
4	**I understand copyright laws and will never do anything illegal.** Software, videos, images, and other content are generally protected by copyright laws, and unauthorized use of such content constitutes an illegal act. Currently, there are a wide range of tools that make software available for use without regard to its license, and websites that make movies, animations, etc. available for free. It is prohibited to use these tools, sites, etc. Not only do these uses constitute an infringement of the very copyright, but they are also used by malicious third parties as a perfect opportunity to spread viruses. In addition, software that facilitates the sharing of illegal content (e.g. BitTorrent, uTorrent, qBittorrent, etc.) is prohibited at Okayama University.	☐

Date of response ＿＿＿＿＿＿ year／＿＿＿＿ month／＿＿＿＿ day

Name of graduate/undergraduate school ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Name ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

You are not required to submit this checklist.

Inquiry form: https://msgs.ccsv.okayama-u.ac.jp/a/