CUNY Information Security Guidelines for Working Remotely

Working Remotely During the COVID-19 Outbreak

Distance learning and remote work present unique challenges in maintaining a secure environment in which work can be safely performed. This document will help faculty, students, staff and consultants fulfill their responsibilities in maintaining the appropriate security and confidentiality of CUNY information irrespective of their work location.

Follow Best Practices for Secure Learning, Teaching and Working Remotely

- DO contact your Help Desk or Campus IT Security Manager immediately if you received a suspicious email, clicked on a suspicious hyperlink by mistake or think your computer's security has been compromised. Messages with a COVID-19 theme are being used to spread malware and phishing.
- DO use up-to-date antivirus/antimalware software.
- DO install Microsoft and Apple software security updates as they are released.
- DO install web browser software updates as they are released.
- DO use CUNY-approved applications to collaborate and complete your tasks. Don't substitute your own preferred tools for ones that are approved for use by CUNY.
- DON'T store or download personally identifiable information (PII), non-public University information (NPUI) or sensitive documents on cloud storage or home computers (see the CUNY Acceptable Use of University Data in the Cloud policy).
- DON'T forward your CUNY email to a personal email account.
- DON'T share the home computer you use for work with other family members, if possible.
- DON'T save CUNY user IDs and passwords on the computer or in web browsers.
- DON'T use out-of-support Windows or MacOS software. See the minimum requirements in "Follow Endpoint Minimum Security Standards" that follows.
- DON'T use public Wi-Fi or guest Wi-Fi connections that do not have encryption and a password or passphrase to connect.

Follow Best Practices for Secure Online Meetings and Teleconferences

Regardless of the online meeting or audio/video teleconferencing tool used, you should observe the following best practices from the NY State Intelligence Center Cyber Analysis Unit to ensure that uninvited guests do not participate:

- DO use the service's waiting room to vet who is allowed to access the meeting.
- DO limit the number of attendees allowed to join a meeting.
- DO manage screen sharing through the host account to prevent an attendee from taking over what is shown on the screen.
- DO password protect meeting access.
- DO ensure that meeting attendees are using the latest version of the service's software.
- DON'T share meeting invitations in public forums found on social media or published on websites.

Be Aware of New, Opportunistic Threats

Malicious actors are actively attempting to take advantage of the coronavirus outbreak and remote teaching and learning situation. An increase in phishing attempts has been observed both at CUNY and nationally. Be wary of unsolicited messages or urgent requests for access or services.

Be particularly wary of urgent requests by email from external (non-CUNY) sources, or those with a COVID-19 theme. Many CUNY email systems insert a warning banner marking email that has originated from external sources.

- Contact your campus Help Desk for guidance before opening any unsolicited or suspicious email attachment or clicking on suspicious links.

Follow CUNY Policies and Guidelines

It is important to remember that CUNY IT Security and other policies are applicable while working remotely. Compliance is especially important when connecting with the CUNY network, applications and services using devices, wireless networks and Internet connections that are not managed by CUNY.

Please review and abide by the following CUNY policies:

- Computer Use Policy — even if you use your own devices and Internet connection, you will be accessing the CUNY network, applications and services
- Antivirus Software Policy — reduce the risk of viruses or malware spreading across the CUNY environment by keeping your antivirus software up-to-date on all devices accessing the CUNY network

- Acceptable Use of University Data in the Cloud — make sure you know what types of University information can be stored and shared using Dropbox, Microsoft Office 365 and Webex and any cloud-based application
- CUNY Data Classification Standard — provides definitions and examples as to what data is Confidential, Sensitive and Public to help ensure compliance with the Acceptable Use of University Data in the Cloud and while working remotely with CUNY information
- Email Auto Forwarding — CUNY generally prohibits the forwarding of CUNY email to a non-CUNY email address

Follow Endpoint Minimum Security Standards

CUNY Information Security policy requires that computers and devices accessing the CUNY network, applications and services use a vendor-supported operating system that receives regular system updates. The specifics are device dependent. The information that follows applies to the most common uses and is correct as of this document's publication date.

Note:
Some CUNY applications and services may prevent your access if you use an unsupported operating system.

Microsoft Operating Systems

Microsoft posts the latest supported operating system information on their Windows lifecycle fact sheet page.

Note:
Windows 7 is not supported and not acceptable for remote work.

Preferred Windows Operating System

Windows 10 version 21H2 or newer

Minimum Windows Operating System

Windows 8.1

Mac Operating Systems

Apple posts the latest operating system updates on its Apple Security Page.

Preferred Mac Operating System

MacOS Monterey 12.4 or newer

Minimum Mac Operating System

MacOS Catalina 10.15.7

Mobile Devices

Minimum iOS Operating System

Apple iOS 12 or newer

Minimum Android Operating System

Android 8 (Oreo) or newer

Antivirus/Antimalware Software

The CUNY Antivirus Software Policy requires that every device connecting to CUNY networks or online resources has an up-to-date antivirus capability.

Apply Web Browser and Application Updates

Like your computer's operating system, you should keep your web browser and other application software updated with the latest version.

Avoid Storing CUNY Files on Your Remote Computer

The Acceptable Use of University Data in the Cloud and CUNY Data Classification Standard apply to all CUNY data you maintain on your remote computing environment.

Recommendation:

Avoid storing any CUNY data or information on your remote computing environment. To protect you and the University, use remote access to your CUNY desktop computer and suitable, CUNY-provided web applications for all confidential, personally identifiable information (PII), and proprietary data and information. For other data, subject to the Acceptable Use of University Data in the Cloud policy, you can use Dropbox and Microsoft Office 365 for Education and other tools made available by CUNY for storing, sharing and collaborating.

Avoid Remote Printing

Avoid printing confidential, personally identifiable information (PII), and proprietary data and information to a remote printer while working remotely.

Review Helpful Information Security Resources

Please visit the following links for more information and best practices while learning, teaching and working remotely:

- CUNY National Cyber Security Awareness Month pages
- CUNY Security Awareness pages
- New York State Cyber Security pages
- StaySafeOnline COVID-19 Security Resource Online pages
- National Institute of Standards and Technology User's Guide to Telework and Bring Your Own Device (BYOD) Security

Have Questions about this Document?

If you have questions about this document, please send an email to security@cuny.edu.