Cybersecurity Best Practices

a. Keep software up to date by installing software updates as they are released, including installing Microsoft and Apple software security updates.

b. Maintain up-to-date antivirus/antimalware software.

c. Practice good password management by choosing strong and unique passwords for every account or application. Never share your password.

d. Use enhanced authentication features such as multi-factor authentication where available.

e. Avoid phishing scams and fraud. Always verify unsolicited inquiries and offers and be careful not to click on links from unknown sources. 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.

f. 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.

g. Use CUNY provided accounts to issue and receive CUNY-related communications and to perform work on behalf of CUNY.

h. Log out of applications and systems at the end of every session.

i. Back up important data. It may be the only way to recover data lost in a security incident.

j. Don't store or download personally identifiable information (PII), non-public University information (NPUI) or sensitive documents on cloud storage or on computers. (See CUNY Acceptable Use of University Data in the Cloud policy.)

k. Don't save CUNY user IDs and passwords on the computer or in web browsers.

l. Don't use public Wi-Fi or guest W-iFi connections that do not have encryption and a password or passphrase to connect.

m. Don't forward your CUNY email to a personal email account.

n. Review and follow these CUNY Policies, Standards, and Guidelines at https://security.cuny.edu including:

   i. CUNY Policy on Acceptable Use of Digital Assets and Resources — even if you use your own devices and Internet connection, you will be accessing the CUNY network, applications and services.

   ii. 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.

   iii. Information Security Guidelines for Working Remotely — follow the Minimum Security Standards.

   iv. 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 any cloud-based application (unless otherwise approved).

   v. 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 policy and while working remotely with CUNY information.

   vi. Email Auto Forwarding — CUNY generally prohibits the auto-forwarding of CUNY email to a non-CUNY email address.