New Employee On-Boarding & Existing Employee Orientation for IT Security

Why is IT Security important at CUNY?

- We must ensure our academic and administrative systems continue to be available to run the business of the University and to serve our faculty, students, and staff.
- We must maintain accurate University data and prevent unauthorized changes (e.g., grades, financial aid information).
- We must be reputable custodians and are required by law to protect the privacy of personal data belonging to our faculty, students, and staff.

What are the IT Security risks to CUNY?

- Don't be phished. Phishing is a scam in which an email message directs you to click on a link that takes you to a web site where you are prompted for personal information such as passwords, social security number, bank account number or credit card number. Both the link and web site may closely resemble an authentic web site, but they are not legitimate.
- Don't disclose personal information to someone you don't know. Social engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without their realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person, and through e-mail.
- Don't disclose personal information within CUNY unless it is absolutely necessary. The need for disclosing your social security number outside of the Human Resource (HR) department would be unusual. When in doubt, contact the HR department directly to verify the legitimacy of the request.
- Protect your user ID and password and never share them. Your user ID is your identification, and it is what links you to your actions on CUNY's computer systems. Your password authenticates your user ID. Use passwords that are difficult to guess and change them regularly.
- You are responsible for actions taken with your ID and password. Log off or lock your computer when you are away from your workstation. In most cases, hitting the "Control-Alt-Delete" keys and then selecting "Lock Computer" will keep others out. You will need your password to sign back in, but doing this several times a day will help you to remember your password.
- E-mail and portable devices are not secure. Do not ship personal information belonging to you or CUNY faculty, students, and staff to portable devices (e.g., portable hard drives, memory) or send or request to be sent such personal information in an e-mail text or as an email attachment without encryption.
- Be careful when using the Internet. Malicious code can take forms such as a virus, worm or Trojan and can be hidden behind an infected web page or a downloaded program. Keep anti-virus and anti-malware programs and the software on your workstation up-to-date at all times. Only install software authorized by your department, and never disable or change security programs and their configuration.

Where are the CUNY IT Security information resources?

- Security.cuny.edu is available 24 hours a day from any Internet accessible location without a user ID and password. All relevant policies, procedures, and advisories, the IT Security awareness program and materials, and links to external IT Security information resources are located here.
- Find the Policy on Acceptable Use of Computer Resources under Info Security Policies.

- Find the IT Security Procedures – General under Info Security Policies.
- To take the IT Security Awareness tutorial, approximately 30 minutes, click on the padlock on the home page of security.cuny.edu.

Who to contact for help with IT Security at CUNY?

- Your supervisor.
- Your College web-site.
- security.cuny.edu
- The College IT Security Manager (click on Campus Security Managers Contact Information at security.cuny.edu under Contact Us).
- The College Chief Information Officer or equivalent in the Central Office department.
- The CUNY Central IT Security Office at security@mail.cuny.edu; or the Contact Us page at security.cuny.edu; or the Who to Contact for Help page at security.cuny.edu.

Where are some external resources for help with IT Security located?

- New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) at www.cscic.state.ny.us
- Federal Trade Commission at www.ftc.gov
- Privacy Rights Clearinghouse - Nonprofit Consumer Information and Advocacy Organization at www.privacyrights.org
- Anti-Phishing Working Group – Committed to wiping out Internet scams and fraud at www.antiphishing.org
- Microsoft Malware Protection Center, Threat Research and Response at www.microsoft.com/security/portal

What is required of me as an employee of CUNY?

- Acknowledge, by signature below, receipt of the Policy on Acceptable Use of Computer Resources.
- Acknowledge, by signature below, receipt of the IT Security Procedures – General.
- Complete the IT Security Awareness tutorial within the first 30 days of employment.
- Maintain compliance with the Policy on Acceptable Use of Computer Resources and the IT Security Procedures at all times.

If you discover or suspect a security breach, you should report the incident to your supervisor, the College IT Security Manager (click on Contact Us at security.cuny.edu) and the CUNY Central IT Security Office (security@mail.cuny.edu) immediately.

I hereby acknowledge receipt of the Policy on Acceptable Use of Computer Resources and the IT Security Procedures – General.

_____ _____

(printed name) (signed)

_____ _____

(College/business area) (date)

One copy for personnel file.
One copy to employee.