ORIENTATION FOR IT SECURITY

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

Why is IT Security important at CUNY?

- We must protect the privacy of personal data belonging to our faculty, students and staff as reputable custodians and as is required by law.
- We must maintain accurate University data and prevent unauthorized changes and transactions (e.g., grades, financial aid information).
- 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.

What can you do to support IT Security at CUNY?

- Be careful when using the Internet. Malicious code known as malware (e.g., virus, worm or Trojan) can be hidden behind an infected web page, an email attachment 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.
- Don’t be phished. Phishing is a scam in which an email message entices you to respond to in some way that potentially leads you to disclose personal information such as passwords, social security number, bank account number or credit card number. Phishing email may closely resemble authentic communications, 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 by email, telephone or in person.
- Don’t disclose personal information within CUNY unless it is absolutely necessary. For example, 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 IDs and passwords 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, pressing 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.
- Email and portable devices are not inherently secure. Do not transmit 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.

Where can you find 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 there.
- Find the Policy on Acceptable Use of Computer Resources under Security Policies and Procedures.
- Find the IT Security Procedures – General under Security Policies and Procedures.

- To take the IT Security Awareness tutorial, approximately 30 minutes, click on the padlock on CUNY Security homepage.

Who can you contact for help with IT Security at CUNY?

- Your college helpdesk
- The college IT Security Manager (click on the Campus IT Security Managers tab at security.cuny.edu under Contact Us)
- The college Chief Information Officer or equivalent in the Central Office department
- The CUNY Central CIS IT Security Office at security@cuny.edu; or the Contact Us page at security.cuny.edu

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

- Stay Safe Online
- Federal Trade Commission at www.ftc.gov
- Privacy Rights Clearinghouse - Nonprofit Consumer Information and Advocacy Organization at www.privacyrights.org
- Microsoft Malware Protection Center, Threat Research and Response at https://www.microsoft.com/en-us/wdsi

What is required of you 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@cuny.edu) immediately.

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

Signature: Sarah Abdorab

Digitally signed by Sarah Abdorab
DN: CN=Sarah Abdorab, E=saraabdorab523@gmail.com, C=US
Reason: I am the author of this document
Location: correct documents
Date: 2022.10.19 19:41:18-04'00'
Foxit PDF Editor Version: 12.0.1

Name *(printed)*: Sarah Abdorab

College: Lehman

Date: 10/19/22

One copy for personnel file.
One copy for employee.