The City College of New York

From The Office of Information Technology

To: All CCNY Faculty and Staff
From: CCNY CIO
Subject: Important Information Security Announcement

Information security is part of all our jobs. Each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control. Please review the information we have prepared regarding this topic at the **CCNY IT Security** web site.

User Responsibilities

- You are required to abide by the University's Policy on Acceptable Use of Computer Resources. See:**http://www.cuny.edu/about/administration/offices/CIS/policies/ComputerUsePolicy.pdf**
- If your job requires using or managing confidential data and systems please also review the University's Information Technology Security Procedures. See: **http://www.cuny.edu/about/administration/offices/CIS/security/pnp/CUNY_Data_Center_Security_and_Environment_Supports.pdf**
- Be aware of other information security policies, procedures, and advisories which can be found on the CCNYIT Security web site. CUNY Information Security web site can be found following the link to **CUNY Security Advisories**.
- Protect your computer system and electronic data from unauthorized use, malicious programs and theft. Report to your supervisor any security policy violations, security flaws/weaknesses you discover or any suspicious activity by unauthorized individuals in your work area.
- If your job requires you to use and store personally identifiable information, such as Social Security numbers, on your office computer, use encryption to protect the data. Please contact your local IT Personnel, the Service Desk at 212-650-7878, or visit the IT Security web site for step-by-step instructions on implementing proper encryption of your data. You must be authorized to do so by filling the form for Authorization to Use and Store Non-Public University Information.
- Personal identifiers, such as Social Security, Driver's License, non-driver identification card, credit or debit card numbers, must not be stored, transported, or taken home on portable devices (e.g., laptops, flash drives, and external hard disks) of any type without specific approval of the Dean or Vice President overseeing your area and the Chief Information Officer and the Vice President of Administration. Where approval is granted, additional password protection and encryption of data are required.

What can you do to protect your computer?

- Use software products that are currently maintained by their publisher and keep the software products updated with critical security patches.
- Use secure passwords that cannot be easily guessed and do not share your password.
- Storage devices (hard disks, tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices) that contain Non-Public University Information must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure.

What else can you do to protect your computer?

- Delete unneeded electronic information with personal identifiers.
- Ensure critical data files are backed up and the backups are securely stored in another location.
- Physically secure your computer by using security cables and locking building/office doors and windows.
- Complete the Security Awareness Program. It is approximately 30 minutes in length, covering the basics of why information security is important and best practices. Everyone at CCNY who handles confidential data is required to enroll and complete this training. All others are strongly urged to do the same. When you connect to this site, please enter your name, email address and select City College from the pull-down menu.

Information security is an extremely serious topic. Please take special care to protect your information, your computer, and the integrity of all the systems we share.