DATA SECURITY AT CCNY

1. CCNY/CUNY's information security policies require all personnel to secure **Non-public University information (NPUI)** which includes social security numbers, grades, copies of identification, credit card information, userid/ passwords, student records and health records.
2. Do not store NPUI on online services unless without explicit permission.
3. When storing NPUI data effective password and encryption technology must be used (e.g. McAfee, TrueCrypt, or operating system encryption (i.e. MS Word/Excel password protection) on a secure, remote server rather than on end point devices such as desktop, laptop or flash drives.
4. Reports containing full social security numbers should be modified to include only the last four digits-- except when required for regulatory compliance.
5. Unattended computers and mobile devices should always be secured against physical theft and tampering. Secure them with locks, set up a screen saver with preset time-out and password protection.
6. Don't distribute NPUI to anyone unless it is absolutely required by job-related duties and responsibilities.
7. Transmitting NPUI as text in an email body is strictly prohibited; transmitting by email attachment is strongly discouraged but when necessary the data must be encrypted.
8. Be cautious when you print, copy and store documents containing NPUI — do not leave them in an open area and dispose of them securely according to the records retention schedule.
9. When you backup digital data containing NPUI ensure that it is encrypted and located in a secure location.
10. Securely delete data containing NPUI when no longer necessary for retention purposes.
11. Before disposing of equipment containing NPUI ensure that the data has been securely removed. Consult with your local IT support person for assistance.
12. Strictly follow CUNY security policies, procedures and advisories (**http://security.cuny.edu**), and report violations and issues when they occur to your supervisor and the Information Security Office x**5221** or **ITSecurity@ccny.cuny.edu** department.

WHAT TO DO IF SECURITY PROBLEMS OCCUR?

If any sensitive non-public data has been compromised because of theft or loss of a computer or a laptop, portable device, breach of network security or through any other means try your best to minimize the damage and:

- Report it immediately to **ITSecurity@ccny.cuny.edu** or **(212) 650-5221.**
- Change all passwords immediately

When using e-mail or other web services, you may encounter spam, phishing scams, obscene material, aggressive behavior or theft of your account or identity.

- Report immediately to CCNY IT Security Office:
- **(212) 650-6185** or ITsecurity@ccny.cuny.edu

The City College
of New York

GUIDE TO PROTECTING YOUR COMPUTER & YOUR IDENTITY @ CCNY

FOR FACULTY/STAFF

Office of
Information Technology

September 2013

Email: ITsecurity@ccny.cuny.edu
Phone: Information Security **(212) 650-5221**

For more information visit the CCNY Information Security website:
http://www.ccny.cuny.edu/it/security.cfm

INFORMATION SECURITY • USER RESPONSIBILITIES

All members of the City College community are required to abide by the University's Policy on Acceptable Use of Computer Resources. These policies can be found on the CUNY Information Security website at **http://security.cuny.edu** under the Security Policies & Procedures section.

Of particular concern is the usage of Non-Public University Information (NPUI), which include:

- Social Security numbers
- Debit and credit card numbers
- Userids with passwords
- Student records (GPAs, transcripts, grades, test results)
- Health records
- Drivers Licenses or other government-issued identification

If your job duties require you to store NPUI on your desktop computer or mobile devices, you must obtain written authorization by your supervisor and the Dean or Vice President overseeing your area. To apply for authorization please submit an Authorization to Use and Store Non-Public University Information form, which may be obtained at the CCNY Information Security website:

http://www.ccny.cuny.edu/it/security.cfm

Those authorized to use NPUI must use encryption to store and to transmit data.

As the internet and mobile devices proliferate, maintaining information security has become a vital part of all our lives. With so vulnerabilities to potential data and identity theft on computers and mobile devices and cyber threats incessantly attempting to exploit them, each member of the City College community is responsible for ensuring the security measures and protection of electronic information resources over which he or she is charged.

To help minimize risks, you are urged to use the tips in this brochure as a guide to eluding threats and securing information on your computer and mobile devices. Selective usage of these basic security measures increases your vulnerability to threats.

Also, review the information we have prepared at the CCNY Information Security web site (which can be reached from the CCNY Web site, under Faculty Staff, CCNY IT, and IT Security):

http://www.ccny.cuny.edu/it/security.cfm

For assistance or more information on how to improve your security posture, please contact your local IT support personnel, the Help Desk at **212-650-7878**, or visit the IT Security web site.

INFORMATION SECURITY TIPS TO E.L.U.D.E THREATS

Ⓔnvironmental Awareness

1. Physically secure your computer with security cables/plates; always lock building/office doors and windows when your workspace is unattended.
2. Never leave mobile devices unattended; thieves can steal your hardware and your identity.
3. Use discretion when logging onto and entering personal information into online resources: treat senstive information like it could be there *permanently*, accessible to *everyone*.

Ⓛogins and Passwords

4. Use strong passwords that cannot be easily guessed or deciphered: at least eight characters including upper and lower case letters, numerals and symbols. Avoid using simple identifiers like common names, dictionary words, birthdates, and anniversaries. Never, ever share your password or login account!
5. Always require a password to login to your computer, especially at start-up; use a screensaver to automatically password lock your unattended devices.
6. Use a generic user account for day-to-day tasks (browsing, email, working); only use administrative accounts for installing new software, updates and performing system maintenance.
7. Always log out of computer workstations, applications, social media and websites, even if you will only be away for moments.

Ⓤpdates and Upgrades

8. On all your devices, always check for and install updates and security patches before using software products—including operating systems, applications, browser plug-ins and add-ons; only use products that are currently maintained by their publisher.
9. Always use licensed and up-to-date malware protection to protect against attacks from malicious agents viruses, worms, zombies, and rootkits.
10. Obsolete programs contain security vulnerabilities; if you don't need it, delete it!

Ⓓata and Information Management

11. Exercise caution when opening unexpected or suspicious email messages or websites, which may contain malicious attachments or links that appear legitimate.
12. Classify and organize documents in order to minimize exposure of sensitive information (SSNs, financial records, credit card information, health records, etc.). If you don't need it, delete it!
13. Ensure critical backup files are encrypted and securely stored in safe, secure backup site.

Securely delete unneeded data that contains confidential information, emptying the trash is not enough.

Ⓔncryption

1. Use file, folder and/or full disk encryption to protect all confidential data.
2. Before transmitting confidential data always ensure that data encryption protocols are in effect (e.g. HTTPS:// for websites and SSL/ TLS for file transfer).
3. Storage devices (hard disks, DVDs, USB drives, smart phones, network storage, etc.) containing confidential information (SSNs, financial, health, and academic records) must be securely overwritten or physically destroyed to prevent unauthorized disclosure.