Attestation of Compliance with CCNY / CUNY Information Security Policy & Procedures

- ❑ I will comply with (1) Policy on Acceptable Use of Computer Resources, (2) Information Technology Security Procedures, (3) Breach of Private Information Procedure, and (4) Private Information Advisory (*).
- ❑ I have completed the CUNY Security Awareness Program/CCNY workshop(*).
- ❑ I affirm that I will not share my computer access password with anyone and will immediately change it and notify my immediate supervisor and the College Information Security Officer if I believe that it has been compromised.
- ❑ I understand that Non-Public University Information is confidential. I will not transport, remove from CCNY premises, or redistribute any unencrypted files containing Non-Public University Information to any unauthorized persons. I further understand that I am permitted to share confidential information only as required to perform my job or as required by the business needs of my unit or department. I understand that I will be held accountable for the loss or disclosure of unencrypted or unprotected Non-Public University Information.
- ❑ I have eliminated all programs and files for personal use from my workstation where Non-Public University Information resides or from where it is accessible and will comply with published Secure Computing Practices (*).

Name: _____ Title: _____

Signature: _____ Date: _____

Please find all referenced documents (*) on the College web site, in Faculty and Staff section, CCNY IT, IT Security. See: http://www.ccny.cuny.edu/it/security.cfm

Approval Signatures

The above individual is permitted to use and store Non-Public University Information while performing duties for CCNY.

Immediate Supervisor

Name: _____ Title: _____

Signature: _____ Date: _____

Dean or Vice President responsible for this activity

Name: _____ Title: _____

Signature: _____ Date: _____

After completing please return this form to the CCNY Information Security Office:
NAC 4/225 • 160 Convent Ave, NY, NY 10031
Email: ITsecurity@ccny.cuny.edu • (212) 650-5221 • Fax: (212) 650-6747

The City College of New York

CCNY

Authorization to Use and Store Non-Public University Information

August 2013

As members of the CUNY community, we are all responsible for maintaining information Security. This self-assessment is part of a mandatory biannual review of our compliance with all University and College information security policies to protect the Non-Public University Information (NPUI) of our employees and students.

You are being asked to complete this checklist in order to (re)authorize you to use one or more information system that hosts student, human resource and/or financial information. Your completion of this check-list will help to identify and to verify the security of any NPUI for which you have been entrusted and to plan remedial action to secure this information if needed.

Date: _____

User Name: _____ SIMS User ID: _____

Department: _____

E-Mail: _____

Location: _____ Phone: _____

Office of Information Security
Division of Information Technology

Email: ITSecurity@ccny.cuny.edu
Phone: x5221
http://www.ccny.cuny.edu/it/security.cfm

Non-Public University Information (NPUI) Inventory

1. What kinds of Non-Public University Information (NPUI) do you work with?
   - ☐ Social Security numbers
   - ☐ Drivers licenses or other official identification
   - ☐ Credit card numbers
   - ☐ Financial records
   - ☐ User ids with passwords and access codes
   - ☐ Student records (GPAs, transcripts, grades, test results, etc.)
   - ☐ Health records (Physical, immunization, counseling, etc.)

Please describe the NPUI data and/or systems for which you are responsible (consult with IT personnel if necessary):

_____

_____

_____

_____

2. How is the information stored?
   - ☐ Paper documents
   - ☐ Digital records (files, spreadsheets, email)
   - ☐ CCNY website
   - ☐ Departmental database
   - ☐ Central IT-based database
   - ☐ Stored on/transmitted to external service
3. What type of device do you use to store and access the NPUI?
   - ☐ Desk drawer/ file cabinet
   - ☐ Portable storage device (flash drive, external hard drive, CD/DVD, smart phone, etc)
   - ☐ Digital devices:
     - ☐ Laptop
     - ☐ Desktop
     - ☐ Server
     - ☐ File share
     - ☐ Other _____
   - ☐ Do you access NPUI remotely?
4. Do student workers access this information?

E.L.U.D.E. Data Protection Measures

Please check all the data protections measures you use to help safeguard NPUI with which you have been entrusted:

1. Ⓔnvironmental Controls
   - ☐ Security locks/ plates
   - ☐ Computrace tracking software installed *and* enabled
   - ☐ Surveillance cameras
   - ☐ Security alarm
2. Ⓛogins and Passwords
   - ☐ Strong password for each user account (8+ letters, numbers, symbols)
   - ☐ Login screen enabled and password-enabled screensaver
   - ☐ Generic (non-administrative) account
   - ☐ No shared login accounts
3. Ⓤpdates and Upgrades
   - ☐ Up-to-date operating system (critical security patches)
   - ☐ Up-to-date McAfee Anti-malware endpoint protection
   - ☐ Up-to-date applications (remove outdated/ unused apps)
   - ☐ Disable extraneous applications and services
4. Ⓓocument Management
   - ☐ Store NPUI on local hard drive
   - ☐ Store NPUI on portable device
   - ☐ Store NPUI on remote share(s)
   - ☐ Automated data back-up
   - ☐ Routinely and securely delete unnecessary copies
5. Ⓔncryption methods in use
   - ☐ File encryption
   - ☐ Folder encryption
   - ☐ Full-disk encryption
   - ☐ Secure file transmission (HTTPS, SSL, TLS)
   - ☐ Unsure

NPUI System Administrator and Device Information

For items you are unsure of please confer with IT support personnel.

IT Support Name: _____ Email _____

Device Location: _____ CIT#: _____

Device Make/Model: _____

Host Name: _____ IP address: _____._____._____._____

MAC Address: _____:_____:_____:_____:_____:_____