

MEMORANDUM

To: IT Steering Committee

From: Brian Cohen

Date: March 26, 2009

Subject: Revised Information Technology Security Procedures

The following is a revised version of the Information Technology Security Procedures last revised and issued on October 16, 2007. The revisions represent the University's obligations under new state and federal legislation, the results of our experience with these procedures over the past seventeen months, and your comments.

INFORMATION TECHNOLOGY SECURITY PROCEDURES

I. General

1. Introduction – Each University entity (i.e., a College or a Central Office department) and all users with access to University information available in University files and systems, whether in computerized or printed form, are continually responsible for maintaining the integrity, accuracy, and privacy of this information. Loss of data integrity, theft of data, and unauthorized or inadvertent disclosure could lead to a significant exposure of the University and its constituents as well as those directly responsible for the loss, theft, or disclosure. Non-compliance with state or federal laws could lead to direct financial loss to the University. Users are directed by these Information Technology Security Procedures (“IT Security Procedures”), which cover all University networks and systems.

Any proposed exception to these IT Security Procedures must be communicated in writing and approved by the University Chief Information Officer or his designee prior to any action introducing a non-compliance situation.

2. Non-Public University Information – For the purpose of these IT Security Procedures, the term “Non-Public University Information” means personally identifiable information (such as an individual’s Social Security Number; driver’s license number or non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; personal electronic mail address; Internet

identification name or password; and parent's surname prior to marriage); information in student education records that is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) and the related regulations set forth in 34 CFR Part 99; other information relating to the administrative, business, and academic activities and operations of the University (including employee evaluations, employee home addresses and telephone numbers, and other employee records that should be treated confidentially); and any other information available in University files and systems that by its nature should be treated confidentially.

II. Access Issues

3. Access to University Information

(a) General. Access to University information available in University files and systems, whether in electronic or hard copy form, must be limited to individuals with a strict need to know, consistent with the individual's job responsibilities.

We utilize the "distributed security" feature of our Banner environment, wherein designated managers own specific security classes for their particular application domain. These designated individuals are assigned such authority by the GC

Vice-President of Administration. New users can only be created by IT; thereafter a

user is assigned to a security class by these designated individuals. These security class owners have access to reports that enable them to verify security assignments at any time; these reports are shared periodically with the VP for Administration for information purposes.

(b) Employees Permitted Access to Non-Public University Information. Except as provided elsewhere in this section 3, access to Non-Public University Information must be restricted to full-time and regular part-time employees of the University and its related entities, the University's adjunct faculty, and employees of the University's contractors who have been permitted such access under a written agreement with the University. All employees permitted access to Non-Public University Information must be specifically reviewed by the Vice President of Administration or the equivalent at the College or in the Central Office department involved in accordance with section 4 below.

(c) Employees Requiring Waiver. Employees of the University or its related entities who are not full-time and regular part-time employees (e.g., individuals hired as part of a temporary staff augmentation or in connection with an individual project), University adjunct faculty, or employees of the University's contractors who have been permitted access to Non-Public University Information under a written agreement with the University may not be permitted any such access, except pursuant to the waiver procedure set forth in section 3(e) below.

(d) CUNY Students. CUNY Students may not be permitted any access to Non-Public University Information, except pursuant to the waiver procedure set forth in section 3(e) below. For the purpose of these IT Security Procedures, “CUNY Students” means all students enrolled in any academic program, or taking any course or courses, at the University, except the following:

- (i) students who are also University adjunct faculty,
- (ii) employees of the University or its related entities or contractors who are taking a Continuing Education course at the University,
- (iii) employees of the University or its related entities or contractors who are taking a credit-bearing course at a College other than where they are employed, and
- (iv) employees of the University or its related entities who are taking a credit-bearing course at the College where they are employed, provided they are taking the course pursuant to a tuition waiver program under a collective bargaining agreement, or are excluded from collective bargaining and are taking the course under a University tuition waiver policy.

(e) Waiver Procedure. An individual who is not permitted access to Non-Public University Information under sections 3(c) and (d) above may be permitted such access on a strict need to know basis, consistent with the individual’s job responsibilities, but only if a waiver is granted by the University Chief Information Officer or his designee following a written request by the Vice President of Administration or equivalent at the College or in the Central Office department involved. Any waiver granted will be limited to a specific period of time, which may not exceed one year. In order to extend the waiver after expiration, this waiver procedure must be repeated. The written waiver request must state:

- the specific status of the individual as an employee of the University or one of its related entities or contractors and/or as a CUNY Student,
- the type and form of access that is being requested,
- the length of time for which access is being requested,
- the reasons for permitting such access, and
- how and by whom the individual will be supervised.

The Vice President of Administration or equivalent at the College or in the Central Office department will be responsible for maintaining all documentation of any waiver request and disposition.

Graduate Teaching Fellows/student employees are considered to have adjunct status. Graduate students are employed in the Library, where they have access to the legacy patron system required to function in their roles.

Among the employees who act as data entry clerks within Student Services offices are doctoral matriculates, most of whom are also teaching within the University, and who perform specific tasks consistent with precise job functions. These employees are not

short-term or transitory. Within the Office of Admissions, such employees enter

applicant data for prospective students only; they do not view or update data for enrolled students at The Graduate Center. Elsewhere in Student Services, data entry employees enter, but do not update, only data that is not listed in the Security Procedure as “Student Record Data.” All data entry employees work under close supervisory review and management and Banner security provides sufficient granularity so that all employees working in the database can view and update only the data that is necessary to perform their assigned tasks. Despite budget restrictions and constraints, the offices within the division of Student Services will continue its

efforts to appoint individuals on College Assistant and/or full-time employee lines.

(f) Acknowledgment of University Policy. All employees described in section 3(b) above and all employees and CUNY Students granted a waiver under section 3(e) above must acknowledge, by signature, receiving a copy of the University’s Policy on Acceptable Use of Computer Resources (available at <http://security.cuny.edu>) and these IT Security Procedures.

Employees with such access privileges provide such acknowledgement as part of their application process for a Banner account.

4. Review of Access to University Files and Systems – Each University entity must review, at least once during each of the fall and spring semesters, individuals having any type of access to University files and systems and must remove user IDs and access capabilities that are no longer current. This review includes, but is not limited to, access to University networks, applications, sensitive transactions, databases, and specialized data access utilities.

An attestation letter of such review must be completed by the Vice President of Administration or the equivalent at the College or in the Central Office department and

submitted to the University Information Security Officer no later than the date specified in the instructions for completing the attestation letter. Documentation showing the review steps taken in arriving at the attestation must be retained in the office of the Vice President of Administration or the equivalent at the College or in the Central Office department and be made available for further review by the University Information Security Officer and internal/external audit entities as appropriate.

5. Severance of Access upon Termination or Transfer of Employment – Access to University files and systems must be removed no later than an individual’s last date of employment. User IDs must not be re-used or re-assigned to another individual at any time in the future.

For job transfers, access to University files and systems must be removed no later than the individual’s last date in the old position and established no sooner than his or her first date in the new position.

In special circumstances where underlying information attributed to a user ID must be retained and made accessible from another user ID, approval must be obtained from both the Vice President of Administration or the equivalent at the College or in the Central Office department and the University Information Security Officer. Such arrangements, if approved, will be for a fixed duration of time, determined on a case-by-case basis.

Reports which identify separation of service actions by employees are now produced twice monthly by HR and are circulated via email among key offices at the Graduate Center; these are used to adjust access privileges accordingly. One continuing area of risk involves individuals who are paid from different funding sources (e.g. doctoral faculty from other campuses, Research Foundation, contract personnel) and hence have personnel files that are not maintained by HR.

We continue to use a small collection of named accounts to support legacy systems; these accounts are owned by various members of the current IT staff.

6. Authentication – Users of University files and systems must use an individually assigned user ID to gain access to any University network or application.

Wireless access is provided to the internet without authentication.

7. User IDs – Users of University files and systems other than technical employees within Information Technology departments at a College or in the Central Office must have no more than one individually assigned user ID per system. The user ID must be in a format consistent with University naming standards, clearly identifiable to a user, and not shared.

Generic-named user IDs used in background/batch processes or peer-to-peer processes and multiple user IDs required to maintain, support, and operate systems by technical employees within Information Technology departments at a College or in the Central Office may be allowed under limited circumstances, provided that use of such identities is auditable, individual user accountability is assigned to each of these identities, oversight is administered by line management of the user assigned to the account, and use of these accounts is specifically approved by the Chief Information Officer or the equivalent at the College or in the Central Office department.

We utilize a small number of shared accounts in Banner for specific purposes. These include an account shared among key staff of Financial Aid for the purpose of managing holds placed on student records. In this instance, there is a designated account owner that is responsible for tracking those designated to share the account.

There is a documented audit trail for the assignment of access permissions in Banner. Via the Banner distributed security environment, permissions are managed and overseen by a small number of key administrators, authorized by the Vice-President for Administration. When an individual record in Banner is updated, the Banner history is maintained to capture the originator of the change to the record.

Each University entity must maintain an accurate record of the person to whom each user ID has been assigned, including name, title, level of access, office, department, and phone number.

8. Passwords – Passwords and private encryption keys must be treated as Non-Public University Information and, as such, are not to be shared with anyone. A password must be entered by the user each time he or she authenticates to a University system. Use of auto-complete features to expedite or script user logins (e.g., “Windows Remember My Passwords?”) is prohibited.

All passwords must be changed at least every 90 days. Accounts which have special access privileges must be changed at least every 60 days. Passwords should not be based on personal information (e.g., family names, pets, hobbies, and friends) and should be difficult to guess. Passwords should be at least eight positions in length. Each University entity may adopt more stringent password controls.

System passwords used in conjunction with background,

batch, scripted or peer-to-peer processes are owned by system administrators and are

changed based on personnel changes among those individuals. Passwords for Internet Native Banner expire every 180 days, as is the case with routine network passwords.

Students and faculty are prompted each semester to change their PINs in Self-Service

Banner; these notifications appear in writing to all students via the Student Information Letter and to faculty via email correspondence to program Executive Officers and Assistant Program Officers when the system is opened for grade entry.

9. Remote Access – Access to administrative and academic support systems from non-University locations is allowed only through secure remote connections (e.g., VPN) that provide for unique user authentication and encrypted communications. The Chief Information Officer or the equivalent at the College or in the Central Office department must approve in writing all requests for remote access capability.

Remote access requests are not approved on an individual basis.

III. Disclosure Issues

10. Disclosure of Non-Public University Information

(a) General Rule. Unless otherwise required by law, users of University files and systems must not disclose any Non-Public University Information (as defined in section 2 above) to the general public or any unauthorized users.

(b) Definition of Social Security Numbers. For the purpose of these IT Security Procedures, the term “Social Security Number” means the nine digit account number issued by the U.S. Social Security Administration and any number derived therefrom. It does not include any number that has been encrypted.

(c) Special Rules for Social Security Numbers. Unless required by law, users of University files and systems must not:

- (i) Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual’s Social Security Number.

- (ii) Publicly post or display an individual's Social Security Number or place a Social Security Number in files with unrestricted access.
- (iii) Print an individual's Social Security Number on any card or tag required for the individual to access products, services, or benefits provided by the University.
- (iv) Print an individual's Social Security Number on any identification badge or card, including any time card.
- (v) Require an individual to transmit his or her Social Security Number over the Internet, unless the connection is secure or the Social Security Number is encrypted.
- (vi) Require an individual to use his or her Social Security Number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.
- (vii) Include an individual's Social Security Number, except the last four digits thereof, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless state or federal law requires the Social Security Number to be on the document to be mailed. Notwithstanding this paragraph (vii), Social Security Numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the Social Security Number. A Social Security Number that is permitted to be mailed under this paragraph (vii) may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.
- (viii) Encode or embed a Social Security Number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the Social Security Number as required by this section 10.
- (ix) Transmit an individual's Social Security Number onto portable devices without encryption as specified in section 13 below.

These special rules do not prevent the collection, use, or release of a Social Security Number as required by state or federal law, or the use of a Social Security Number for internal verification, fraud investigation, or administrative purposes.

Note: CUNY-BA will mask SSNs on transcripts effective summer 2009

11. Web Accessible Data – Because Non-Public University Information must not be made accessible to the general public, all University web pages must be programmed with a parameter to prevent the caching of Non-Public University Information by Internet search engines. Directory/folder listings of files through a web page must be disabled. Secure and encrypted data transfer protocols must be used when uploading data to a web site.

Website managers are able to FTP files for updating web content.

12. Security Incident Response and Reporting

(a) Acknowledgment and Reporting of Security Incidents. Each Chief Information Officer or the equivalent at a College or in a Central Office department must, within 24 hours of receipt by his or her College or department, acknowledge or respond in writing to any initial security incident report issued by the University Chief Information Officer or the University Information Security Officer. The Chief Information Officer or the equivalent at the College or in the Central Office department must make a full written report of such incident to the University Chief Information Officer and the University Information Security Officer, including root cause identification, explanation of the remediation plan, and extent of data loss, within 72 hours of the College's or department's receipt of the initial security incident report.

(b) CUNY Breach Reporting Procedure. The CUNY Breach Reporting Procedure (available at <http://security.cuny.edu>) must be followed whenever a security incident occurs involving the unauthorized disclosure of any of the following Non-Public University Information without encryption:

- (i) Social Security Number;
- (ii) driver's license number or non-driver identification card number; or
- (iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(c) Limiting Disclosure. When any Non-Public University Information has been disclosed without valid authorization and encryption, all reasonable efforts must be taken to eliminate further disclosure, including immediate disconnection of any computer device involved from the University network.

13. Portable Devices/Encryption – The Non-Public

University Information listed in section 12(b) above must not be stored, transported, or taken home on portable devices (e.g., laptops, flash drives) of any type without specific approval of both the Vice President of Administration or the equivalent at the College or in the Central Office department and the University Information Security Officer. Where approval is granted, additional password protection and encryption of data are required. In addition, the Non-Public University Information listed in section 12(b) above stored on non-portable devices or transmitted between devices (e.g., servers, workstations) must be encrypted. The University has made encryption tools available to staff and faculty to comply with the requirements of this procedure.

Users are advised of such practices and reminded to comply.

14. Safeguarding and Disposal of Devices and Records Containing Non-Public University Information

– Whenever records containing Non-Public University Information are subject to destruction under the CUNY Records Retention and Disposition Schedule (available at <http://policy.cuny.edu/text/toc/rrs>), the storage devices such as hard disk drives and other media (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers, or other devices) and hard copy documents that contain such information must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure. While in use, such devices and documents must not be left open or unattended on desks or elsewhere for extended periods of time.

We cannot attest to the individual behavior of every employee with regard to the requirement that “While in use, such devices and documents must not be left open or unattended on desks or elsewhere for extended periods of time.”

IV. Maintenance of Data and Systems

15. Change of Data in Records

(a) Authorization of Changes. When updates are not part of normal business processing, individuals within Information Technology departments at a College or in a Central Office department who have access to University information to support ongoing operations of administrative files and systems must not alter any such information unless given specific approval by the Vice President of Administration or the equivalent at the College or in the Central Office department. A record of any data change, including evidence of approval, must be retained in the office of the Vice President of Administration or the equivalent at the College or in the Central Office department.

(b) No Changes by Remote Access. Any direct changes to official data of record stored in University files and systems must be done from a College or Central Office location. No form of remote access that allows direct changes to student or

employee data is allowed. Students and employees may, however, have remote self-service access in order to update their own personal data.

As per item #9, secure remote access is permitted. Access to Banner pursuant to Graduate Center self-service will continue to remain available.

16. Centralized Data Management – Data that are acquired or managed by Central Office departments (e.g., CPE, skill scores) must be loaded into University files and systems and may not be modified by Colleges at the local level. Colleges will be able to view such data and through an exception process be able to request changes. Each College is responsible for reviewing a data edit report for accuracy and completeness whenever data are uploaded to its respective student or human resources systems.

17. Grade Changes – Any University system that allows for grade changes must have multiple security levels enabled, including the maintenance of a separate password that is administered and changed regularly for the purpose of authenticating individual users to the grade change function. Grade change functions must be able to create an audit trail from which edit reports will be regularly prepared for review by a management designee other than the person who has responsibility for the area making grade changes. The number of individuals allowed to make grade changes must be strictly limited to employees of the University and its related entities, subject to the additional criteria set forth in section 3 above. Current University student information systems support this requirement.

Privileges for grade changes are limited to the registrar and assistant registrar functions; when such change is made, the account making the update is logged by the Banner system.

18. Changes in Information Files and Systems – Existing and new information files and systems must comply with these IT Security Procedures. Modifications to existing information files and systems will be required to maintain compliance. Ghost files and systems and development/test files and systems holding copies of data from master files and systems must also comply with these procedures. Ghost files and systems should be eliminated to minimize the number of copies and access points to Non-Public University Information. Where files and systems cannot be modified to comply with these procedures, the University entity must notify the University Chief Information Officer and the University Information Security Officer in writing, providing a written business case justifying the decision.

Multiple test instances of Banner are in place for managing the process of system upgrades and enhancements.

19. Vulnerability Assessments – Each University entity must establish a routine program to test, monitor, and remediate technical and data vulnerabilities on its network. The program should include a combination of continuous monitoring and on-demand testing tools. Monitoring and testing should report on operating system configuration, software patch level vulnerabilities, and unprotected data. The Central Office may initiate vulnerability testing at its discretion. Regular reporting of test results must be made available to the University Information Security Officer.

Tools of this nature have been made available via the office of the University Information Security Officer.

20. Device Management – All devices that are allowed to connect to University networks and systems that support administrative, business, and academic activities and operations must be maintained at current anti-virus/malicious code protection at all times. In addition, security updates to operating systems must be applied on a timely basis after appropriate testing. Although the University does not manage student computers, procedures should be implemented to minimize the risk to University files and systems.

IT-managed systems comply with these guidelines; network access control for ensuring such compliance for end-user devices such as laptops and mobile devices is not currently in place.

21. Management Responsibility – College and Central Office management are responsible for maintaining and overseeing compliance with these IT Security Procedures within their line responsibilities.

22. Information Technology Security Procedure Governance – The University will organize working groups and work through existing councils to identify and establish procedures and other areas of change that may be instituted to further protect the integrity of University files and systems.

Additional and/or revised procedural statements may be adopted from time to time and introduced for University compliance. Further procedural documents may be developed to elaborate detail on these IT Security Procedures, but they will in no way detract or suggest a different level of compliance that is expected or required.

Non-compliance with these IT Security Procedures may result in termination of access to University network and applications until such time that compliance is re-established. Non-compliance may also result in disciplinary action.

These IT Security Procedures, related policies and advisories, and links to the New York State Cyber Security Policies are available at <http://security.cuny.edu>.