

MEMORANDUM

To: IT Steering Committee

From: Brian Cohen

Date: August 30, 2006

Subject: New Information Technology Security Procedures

As you know in October 2005 the University successfully completed its search and appointed its first Information Technology Security Officer, Carl Cammarata. Mr. Cammarata immediately began to evaluate our current IT security procedures with the goal to update and develop new procedures where needed. As a result of Mr. Cammarata's work with each of the colleges and the Security sub-committee of the IT Steering Committee, it is my recommendation that the procedures listed below be immediately promulgated to the all University offices and campuses. These procedures should be communicated to your campus governance.

IT SECURITY PROCEDURES: - (August 30, 2006)

All users with access to University information, whether in computerized or printed form, are continually responsible for information integrity, accuracy and privacy. Loss of data integrity, theft of data, and inadvertent disclosure could lead to a significant exposure to the University and our constituents as well to those directly responsible for the loss or disclosure. Non-compliance with New York State or Federal laws could lead to direct financial loss to the University. We are directed by the following University Information Security procedures covering all University networks and systems containing non-public University data:

Access to Sensitive or Non-Public University Data/Systems – Access to non-public University data must be limited to a strict need to know, consistent with the user's job responsibilities, and be specifically approved by the Vice President of Administration or equivalent. Data that is considered to be sensitive or private University data must be severely limited. All users given access to non-public University data must attest to reading and understanding the University's Computer Use Policy.

Authentication – Users of computerized systems must use an individually assigned user ID to gain access to all networks and applications containing sensitive or non-public University data.

User IDs – Users of computerized systems should have no more than one individually assigned user ID. The user ID must be of a format consistent with University naming standards, clearly identifiable to a user, and not shared. Generic-named or group user IDs are not permitted. Each University entity (e.g., College, Central Office department) must maintain an accurate record of the person to whom the user ID has been assigned including name, title, level of access, office, department and phone number.

Severance of Computer Accounts – Access to computerized systems must be severed prior to or upon the 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 computerized systems must be removed no later than the last date in the old position and established no sooner than the 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 the University entity's Vice President of Administration and University Information Security Officer. Such arrangements, if approved, will be for a fixed duration of time, determined on a case-by-case basis.

Review of Computer Access – Each respective University entity (e.g., College, Central Office department) must review, at least once a semester, those having any type of access to sensitive or non-public University data and removing user IDs and access capabilities that are no longer current. This review includes, but is not limited to, access to networks, applications, sensitive transactions, databases, or specialized data access utilities.

Attestation of such review must be completed by the University entity's Vice President of Administration or equivalent and submitted to the University Information Security Officer. It is the responsibility of the University entity for maintaining the integrity and privacy of non-public University data.

Students, Part-time Employees, Contractor User IDs – Students, part-time employees or contractors must not be given access to update permanent student record information including but not limited to all student demographic and term information, admissions, registration, grades, attendance, immunization, testing and financial aid.

Passwords – All passwords must be treated as sensitive and private University data and as such, are not to be shared with anyone. Users must manually enter their password when prompted and passwords must not be scripted or stored.

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 must 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..

Privileged Access – In some circumstances, individuals within IT departments may be allowed broad access to University data to support the ongoing operations of administrative systems. These individuals must not alter any University data unless given specific approval by the Vice President of Administration or equivalent, in order to restore a system to a normal state of operation. A record of the data change including evidence of approval must be retained in the Office of Administration or equivalent Central Office department.

Users with privileged or broad access to data must sign an agreement stating they understand their responsibility in maintaining the integrity and privacy of sensitive or non-public University data.

Mobile Devices – Sensitive or non-public University data must not be stored, transported, taken home on portable devices of any type without specific approval of the Vice President of Administration or equivalent and the University Information Security Officer. Where approval is granted, additional password protection and encryption of data is required.

Incident Response and Reporting – A report of all security incidents must be made to the University Chief Information Officer and University Information Security Officer on a timely basis. The report will include root cause identification, explanation of the remediation plan and extent of data loss.

When sensitive or non-public data has been disclosed, the Breach of Private Information procedure must be followed. All reasonable efforts will be taken to contain the disclosure including immediate disconnection of the device from the network.

Change of Data in Permanent Records – Any changes to student data in administrative systems must be done from a College or Central Office location. No form of remote access to alter student data is allowed.

Centralized Data Management –Data (e.g., CPE, skill scores) that are acquired or managed by Central University offices shall be loaded into University systems and will not be modified by University colleges at the local level. Colleges will be able to view the data and through an exception process be able to request changes based upon developed criteria. Each College is responsible for reviewing a data edit report for accuracy and completeness whenever data is uploaded to their respective student systems.

Grade Changes – Any system that allows for grade changes will 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 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 severely limited and only available to full time employees of the University.

Changes in Information Systems – Existing and new information systems must comply with these information security procedures, where possible. Modifications to existing information systems may be required to maintain compliance. Ghost (copies of data from master systems) information systems must also comply with these procedures. Ghost systems should be eliminated to minimize the number of copies and access points to private or sensitive University data. Where systems cannot be modified to comply with these procedures, the University entity (College, Central Office department, etc) must notify in writing the University Chief Information Officer and University Information Security Officer.

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 upon operating system configuration and software patch level vulnerabilities and unprotected data. The University Central Office may initiate vulnerability testing at its discretion. Regular reporting of test results must be made available to the University Information Security Officer.

Web Accessible Data – Non-public University data, including private and sensitive information, must not be made accessible to the general public. All web pages must be programmed with a parameter to prevent the caching of data 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.

Management Responsibility – College and Central Office management must be responsible for maintaining and overseeing compliance with information security procedures within their line responsibilities.

Information Security Procedure Governance – The University will establish working groups and/or leverage existing Councils to identify and author procedures and other areas of change that may be instituted to further protect the integrity of University systems and data.

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

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

All appeals or exceptions to Information Security procedures must be directed to the University Information Security Officer prior to the action introducing a non-compliance situation.