Information Security Policy and Plan

Preamble

In order to protect critical information and data, and to comply with Federal law and New York State law, the College's Information Technology Services (ITS) proposes certain practices in the College information environment and institutional information security procedures. While many of these practices mostly affect ITS, some of them will impact diverse areas of the College including, but not limited to, the Finance Office, the Office of the Registrar, College Relations, Dean of Students Office, the Library, the Bookstore, Admissions, and many third party contractors, including Dining Services. The goal of this document is to define the College's Information Security Policy and Plan, to provide an outline to address ongoing compliance with federal regulations related to the Policy, and to position the College for likely future privacy and security regulations.

Gramm Leach Bliley (GLB) Requirements

GLB mandates that the College appoint an Information Security Plan Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Policy and Plan periodically.

New York State Security Breach and Notification Act

The New York State Security Breach and Notification Act went into effect on December 7, 2005. The act requires an entity which owns or licenses private information to disclose a breach of the security of the system containing such information. Private information is defined as any identifier concerning a natural person (i.e., name or personal mark) plus one or more of the following: Social Security number; driver's license number or non-driver identification; account number; credit or debit card number plus security code, access code, or password which permits access to an individual's financial account.

Information Security Plan Coordinator

In order to comply with GLB, ITS has designated an Information Security Plan Coordinator. This individual will work closely with the College's attorney and Risk Manager. The Interim Information Security Plan Coordinator is presently the Chief Information Officer.

The Coordinator, working with other members of the College administration, must help the relevant offices of the College identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program; and regularly monitor and test the program. In addition, the Coordinator will facilitate notification of any breach in security, restoring the integrity of the system following a breach and working with law enforcement in the event of a criminal breach.

Risk Assessment and Safeguards

The Coordinator will work with all relevant areas of the College to identify potential and actual risks to security and privacy of information. Each Department head, or his/her designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in his/her respective areas that work with covered data and information. In addition, the relevant departments of ITS will conduct an annual review of procedures, incidents, and responses and will publish all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. Publication of these materials is for the purpose of educating the College community on network and information security and privacy issues. ITS will assure that procedures and responses are appropriately reflective of those widely practiced at other national liberal arts colleges.

In order to protect the security and integrity of the College network and its data, ITS will develop and maintain a registry of all computers attached to the College network. This registry will include, where relevant, IP address or subnet; MAC address; physical location; operating system; intended use (server, personal computer, lab machine, etc.); the person, persons, or department primarily responsible for the machine; and whether the machine has, or has special access to, any confidential data covered by relevant external laws or regulations.

ITS assumes the responsibility of assuring that patches for servers and critical systems are reasonably up to date. ITS will review its procedures for patches to operating systems and software and will keep current on potential threats to the network and its data. Risk assessments will be updated annually.

ITS bears primary responsibility for the identification of internal and external risk assessment, but all members of the College community are involved in risk assessment associated with information technology areas. ITS, working in conjunction with the relevant College offices, will conduct regular risk assessments including, but not limited to, the categories listed by GLB.

ITS will work with the relevant offices (Finance, Human Resources, the Registrar, College Relations, and the Library, among others) to develop and maintain a registry of those members of the College community who have access to covered data and information. ITS, in cooperation with Human Resources and Finance, will work to keep this registry up to date.

ITS will oversee the physical security of all servers and terminals which contain or have access to covered data and information. ITS will work with other relevant areas of the College to develop guidelines for physical security of any covered servers in locations outside the ITS machine room. The College will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the College to risks.

One of the largest security risks may be the possible non-standard practices concerning social security numbers. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA). By necessity, student social security numbers are in the College student information system. The College will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover College employees as well as subcontractors such as the food services.

ITS will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

It is recommended that relevant offices of the College decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, for example employees handling confidential financial information.

ITS will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

Notification of Breach

In the event of a suspected or actual breach of the security system containing private information as defined in paragraph III above, the Information Security Plan Coordinator shall be contacted immediately. The Coordinator shall then provide notification to the relevant party or parties in the most expedient time possible, without unreasonable delay, after performing necessary measures to determine the scope of the

breach and restore integrity to the system. Law enforcement shall also be contacted if the breach is suspected to be criminal in nature.

Employee Training and Education

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, ITS and the College attorney will work in cooperation with Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all College data; custodians of data, and those employees who use the data as part of his/her essential job duties.

Oversight of Service Providers and Contracts

GLB requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The Risk Manager and the Coordinator will develop and send form letters to all covered contractors requesting assurances of GLB and New York State Security Breach and Notification Act compliance. While contracts entered into prior to June 24, 2002 are grandfathered until May 2004, the College will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

Evaluation and Revision of the Information Security Plan

GLB mandates that this Information Security Policy and Plan be subject to periodic review and adjustment. The most frequent of these reviews will occur within ITS where constantly changing technology and constantly evolving risks indicate the wisdom of periodic reviews. Processes in other relevant offices of the College such as data access procedures and the training program should undergo regular review. The Policy itself should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

Definitions

Covered data and information for the purpose of this Policy includes student financial information required to be protected under the Gramm Leach Bliley Act (GLB). Covered data and information includes both paper and electronic records.

Student financial information is that information the College has obtained from a student in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers, in both paper and electronic format.