

UNE Information Security Plan

I. Preamble

In order to protect critical information and data, and to comply with Federal Law¹, the Information Security FTC/GLB Compliance Committee, in alliance with the Vice President of Business and Finance proposes certain practices in the University information environment and institutional information security procedures. These practices impact diverse areas of the University, including but not limited to the Business Office, the Office of the Registrar, University Relations, Student Life, the Library, Admissions and Financial Aid, and many third party contractors, including food services and the bookstore. The purpose of this document is to define the University's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the University for likely future privacy and security regulations.

II. Gramm Leach Bliley (GLB) Requirements

GLB mandates that the University appoint an Information Security Plan FTC/GLB Compliance Committee, 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 Program periodically.

III. Information Security Plan FTC/GLB Compliance Committee

In order to comply with GLB, UNE has designated an Information Security Policy FTC/GLB Compliance Committee. These individuals must work closely with the Vice President of Business and Finance. The FTC/GLB Compliance Committee is presently the Director of Financial Aid, Director of Information Technology Services, Oracle Database and Project Manager, Registrar, Controller, Associate Controller/Director of Internal Audit, Assistant Director of Human Resources, and University Relations Database Coordinator.

The FTC/GLB Compliance Committee must help the relevant offices of the University 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.

¹ The Financial Services Modernization Act of 1999 (also known as Gramm Leach Biley (GLB) 15 U.S.C. §6801

IV. Risk Assessment and Safeguards

The FTC/GLB Compliance Committee must work with all relevant areas of the University to identify potential and actual risks to security and privacy of information. Each College or Department head, or her designee, will conduct an annual data security review, with guidance from the FTC/GLB Compliance Committee. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. In addition, the relevant departments of UNE will conduct a quarterly 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 University community on network security and privacy issues.

Information Technology Services (ITS) assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date, and will keep records of patching activity. 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 quarterly.

The Information Security FTC/GLB Compliance Committee bears primary responsibility for the identification of internal and external risk assessment, but all members of the University community are involved in risk assessment. The Information Security FTC/GLB Compliance Committee, working in conjunction with the relevant University offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB.

ITS, working in cooperation with relevant University departments, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development, etc.). The Information Security FTC/GLB Compliance Committee and the relevant departments will conduct ongoing (at least biannual) audits of activity, and will report any significant questionable activities.

The Information Security FTC/GLB Compliance Committee will work with the relevant offices (Business Office, Human Resources, the Registrar, Financial Aid, University Relations, and the Library, among others) to develop and maintain a database of those members of the University community who have access to covered data and information. The Information Security FTC/GLB Compliance Committee in cooperation with Human Resources and the Business Office will work to keep this data rigorously up to date.

ITS will assure 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 university to develop guidelines for physical security of any covered servers in locations outside the central server area. The University will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures that may expose the University to risks.

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

It is recommended that relevant offices of the University 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.

The Information Security FTC/GLB Compliance Committee will periodically review the University's disaster recovery program and data-retention policies and present a report to the Vice President of Business and Finance.

V. Employee training and education

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, the Information Security FTC/GLB Compliance Committee and the Vice President of Business and Finance will work in cooperation with the Office of 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 university data; custodians of data as identified in the data handbook, and those employees who use the data as part of their essential job duties.

VI. Oversight of Service Providers and Contracts

GLB requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Business Office, in cooperation with the Vice President of Business and Finance, will develop and send form letters to all covered contractors requesting assurances of GLB compliance. While contracts entered into prior to June 24, 2002 are grandfathered until May 2004, the Vice President of Business and Finance will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

VII. Evaluation and Revision of the Information Security Plan

GLB mandates that this Information Security 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 quarterly reviews. Processes in other relevant offices of the University such as data access procedures and the training program should undergo regular review. The plan itself as

well as the related data retention policy should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

VIII. 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). In addition to this coverage which is required by federal law, UNE chooses as a matter of policy to also define *covered data and information* to include any credit card information received in the course of business by the university, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

Student financial information is that information the university has obtained from a student in the process of offering a financial product or service, or such information provided to the university 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.

Information Security FTC/GLB Compliance Committee consists of the Director of Financial Aid, Director of Information Technology Services, Oracle Database and Project Manager, Registrar, Controller, Associate Controller/Director of Internal Audit, Assistant Director of Human Resources, University Relations, and Vice President of Business and Finance.