Texas Christian University
Gramm-Leach-Bliley Financial Services Modernization Act
Information Security Plan and Policy (1.1)

I. Introduction

In order to protect critical information and data, and to comply with Federal Law[1], Texas Christian University (TCU) proposes certain practices in the information technology environment and institutional information security procedures. These practices primarily affect Information Services (TCU IS) but some of them will impact diverse areas of the University, including but not limited to Financial Services, the Office of the Registrar, Institutional Advancement, Student Life, Athletics, Financial Aid, the Library, and many third party contractors, including food services, the bookstore and other such vendors who have access to protected information through contracts with TCU. This policy applies to both electronic and paper information.

The goal of this document is to define the University's Institutional Information Security Program, to outline ongoing compliance with federal regulations and to position the University for future privacy and security regulation compliance. Existing University policies including, but not limited to, the TCU Computing Resources Policy, the TCU Privacy Policy and the University Standards for Wireless Access are made a part of this policy. The TCU Information Security Plan Policy is intended to extend the privacy and safeguards already in place at the University.

II. Financial Services Modernization Act (Gramm Leach Bliley (GLB) Requirements

The Financial Services Modernization Act, also known as GLB Act, has two significant sections. These sections in combination provide privacy and safeguard the security of non-directory customer financial information. The first, Section 313, provides privacy of information collected on *customers* as defined by the Act. The second, Section 314, provides that such nonpublic information be administratively, technically and physically safeguarded.

The University's compliance with the Family Education Rights and Privacy Act of 1974 (FERPA)[2] and the Health Insurance Portability and Accountability Act of 1996 (HIPPA) provides *de facto* compliance with Section 313 of the GLB requirements. However, Section 314, regulations mandate that the University 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 Institutional Information Security Program periodically.

---

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

2 20 U.S.C. § 1232g

The Federal Trade Commission (FTC) will enforce compliance with the regulations of the GLB Act. The effective date for compliance is May 23, 2003.

III. Information Security Plan Coordinator

In order to comply with GLB, The University has designated an Information Security Plan Coordinator and a Deputy Plan Coordinator. These individuals, but primarily the Plan Coordinator and the Information Services Security Administrator, must work closely with the University legal counsel, other positions in Information Services (TCU IS), as well as all relevant academic and administrative offices throughout the University. The Information Security Plan Coordinator (ISPC) is presently the Assistant Provost. The Deputy Coordinator is currently the Associate Vice Chancellor for Administrative Services. These two individuals will serve until further notice.

The ISPC must assist the relevant offices of the University in identifying 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.

IV. Definitions

Customer for the purposes of this policy shall be anyone with whom the TCU has a consumer relationship or who has obtained a financial product or service from the University. While students are clearly customers under this definition, the University has taken a broader approach and considers it prudent to cover donors, those who purchase tickets for University events and other such individuals who might from time to time share financial information with TCU. The University does not consider employees or vendors as customers under the definition of the act; however, the same safeguards will apply wherever feasible.

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, whether in the PeopleSoft Centralized system or any other system maintained by a University Office.

In addition to the coverage that is required by federal law, TCU also chooses, as a matter of policy, to define *covered data and information* to include any credit card or bank account information received in the course of business by the University, whether or not such information is covered by GLB.

Constituent financial information is information TCU has obtained from a student, or his/her parents if applicable, 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 constituent 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.

Other constituent data and information for purposes of this policy is any nonpublic information collected on anyone (employees, donors, vendors, etc.) that is not essential to the business operation of the University. TCU will strive to effectively eliminate use of social security numbers, or to consider them protected and institute appropriate safeguards, in all its dealings with individuals and businesses. Likewise, bank account information on employees and vendors, while not specifically covered by GLB, will be omitted from paper records, used only when imperative in electronic records and encrypted in transmission over the network involving web access.

Institutional information security means any administrative, technical or physical safeguards the University uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle constituent information.

Service provider is any person or entity that receives, maintains, processes or otherwise is permitted access to constituent information through its direct provision of services to TCU.

V. Risk Assessment and Safeguards

TCU has chosen to take a distributed, decentralized approach to insuring compliance with GLB. To that end, the ISPC will work with all relevant areas of the University to identify potential and actual risks to security and privacy of information. The Chancellor and Vice Chancellors will identify one or more individuals from their areas who will serve as Division Security Liaisons (DSL) to monitor and implement the regulations of the GLB Act within their specific area. Working in concert with the Coordinator and the Deputy Coordinator, the DSLs will be trained to assist in identifying individuals and operations within their units where access to either electronic or paper copies of covered information exist. The Division Security Liaisons, with the help of the ISPC, will assist each school or department in conducting an annual data security review.

TCU Information Services will assume major responsibility for the security of electronic data available to the TCU community. As such, several measures fall to the TCU IS staff to ensure compliance with implementation of safeguards. The Coordinator or Deputy Coordinator will be apprised as to the status of each measure, and may from time to time audit the respective systems for compliance with this policy.

The Security Council of TCU IS will conduct a quarterly review of procedures, incidents, and responses taken to ensure security, and will make available to the ISPC all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. The IS Security Council meetings, notes and reports will serves as evidence of compliance with this requirement. Publication shall be solely for the purpose of educating the University community on network security and privacy issues. TCU IS will assure that procedures and responses are appropriately reflective of those widely practiced at other national research Universities, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

In order to protect the security and integrity of the University network and its data, TCU IS will maintain a current registry of all TCU computers that are eligible to attach to the University network. This registry will include, where relevant, IP address or subnet, MAC address, original physical location, operating system, intended use (server, personal computer, lab machine, etc.).

TCU IS 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. TCU IS 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 semi-annually.

TCU IS bears primary responsibility for the identification of internal and external risk assessment regarding electronic access to restricted information, but all members of the University community are involved in risk assessment. The Information Security Plan Coordinator and TCU IS, working in conjunction with the relevant University offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB. While considerable risks are the result of technological assess, paper copies of information may prove greater security risk due to availability and easy access.

The ISPC, working with TCU IS and relevant University departments, will develop and maintain a data handbook, listing those persons or offices responsible for each relevant software systems (financial, student administration, development, athletics, etc.). The ISPC and the relevant departments will conduct ongoing (at least biannual) audits of activity and will report any significant questionable activities.

TCU IS will work with the ISPC and relevant offices (Financial Services, Human Resources, the Registrar, Institutional Advancement, and the Library, among others) to develop and maintain a registry of those members of the TCU community who have access to covered data and information. The Plan Coordinator and TCU IS Security Officer, in cooperation with Division Security Liaisons and the Offices of Human Resources and Financial Services will work to keep this registry rigorously up to date.

TCU IS will assure the physical security of all servers and terminals that contain or have access to covered data and information. TCU IS 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. Any non-centralized computer system developed by a University Office or individual must be reported and be in compliance with the provisions of this policy.

While TCU has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some employees, offices and systems on the use of 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 still remain in the University student information system.[3] Use of social security numbers in other University databases and systems where they are a convenience, rather than a legal requirements, will be evaluated for possible conversion to a non-financial identifier. The University 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 university employees as well as subcontractors such as the bookstore and food services, and consortiums to which the University belongs.

3 Social Security Numbers are kept both for historical purposes and due to the requirements of 26 U.S.C. § 6050S, the tuition payment credit reporting requirements.

TCU IS will develop a plan to ensure that all electronic covered information that is accessible via the web is encrypted in transit and that the central databases are strongly protected from security risks. TCU IS 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. Incidents will be promptly reported to the ISPC.

TCU employment policy requires a criminal background check of all new hires. It is recommended that relevant offices of the University decide whether background or reference checks are prudent for current employees (including faculty) who handling confidential financial information. Students who have access to financial information in University Offices will be subject to the same background screening.

TCU will ask all employees who have access to protected information, or who might have access to protected information, to sign a confidentiality agreement. Failure to comply with such confidentiality will be grounds for immediate dismissal.

The Information Security Plan Coordinator will periodically review the University's disaster recovery program and data-retention policies and present a report to the Provost.

VI. Employee training and education

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, TCU IS and the ISPC 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. New employees who have access to secure information will receive training immediately. All employees who have access to secure information must attend periodic training to keep abreast of changes in laws pertaining to covered information. Compliance with federal and state laws will be a part of all training for TCU employees.

VII. 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. The ISPC in cooperation with the University legal counsel and Financial Services, 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, where possible, an Addendum to existing contracts will be executed. The University will ensure that all relevant future contracts include a privacy clause that is in compliance with GLB.

VIII. 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 TCU IS 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 whenever significant changes are made to systems or personnel changes occur, but at least annually. The plan itself as well as the related data retention policy also should be reevaluated annually to assure ongoing compliance with existing and pending laws and regulations.