Southern Methodist University
Program for the Security of Non-Public Personal Information

Overview

The Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act or "GLB") regulates the disclosure of non-public personal information by financial institutions. Institutions of higher education such as Southern Methodist University are considered to be financial institutions because they participate in financial activities, such as the Federal Perkins Loan Program.

The goal of this document is to set forth the University's program to (i) ensure the security and confidentiality of non-public information covered by GLB, (ii) protect against anticipated threats or hazards to the security of such information, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in harm or inconvenience to consumers. This document will define the University's Program for the Security of Non-Public Personal Information, designate employees responsible for the coordination and administration of the Program, and provide an outline to assure ongoing compliance with federal regulations related to the Program and other privacy and security considerations.

In order to protect critical information and data as required by GLB, this program documents certain practices in the University information environment and institutional information security procedures. These practices cover both paper and electronic information and data and impact diverse areas of the University. Since safeguarding non-public information is a good business practice irrespective of legislative requirements, the University has expanded the Program to cover areas handling both GLB-protected information and other information protected by state and other federal privacy laws, including, but not limited to:

- Information Technology Services
- Business Services
- Enrollment Services
- Development and External Affairs
- Residence Life and Student Housing
- Health Center
- Other Student Affairs offices
- Libraries
- Athletics
- Police Department
- Copy Center
- Impressions

- Computer Center
- Payroll
- Risk Management
- Division of Education and Lifelong Learning
- Advanced Computer Education Centers
- Student Association
- Hart eCenter
- Other, including ticket offices, short courses and seminars, law clinic, summer camps, Upward Bound, and the International Office
- Various third party contractors, including dining services and the bookstore

Designation of Representatives

The University considers compliance with GLB to be an institution-wide responsibility. It has designated three representatives to be responsible for coordinating compliance. The University Information Security Officer, empowered in University Policy 12.5 is responsible for coordinating and overseeing the Program pertaining to electronic data. The University Information Security Officer is responsible for ensuring adherence to the University's policies and procedures related to electronic data, and that the elements of this program are in place to safeguard electronic information described in Scope of Program, below. The Associate Provost for Educational Programs is responsible for coordinating and overseeing the Program protecting printed data pertaining to students. The Associate Provost is responsible for ensuring adherence to the University's policies and procedures related to printed data pertaining to students, and that the elements of this program are in place to safeguard printed information described in Scope of Program, below. The Business and Finance designee is responsible for coordinating and overseeing the Program protecting all other printed data. The Business and Finance designee is responsible for ensuring adherence to the University's policies and procedures related to this printed data, and that the elements of this program are in place to safeguard printed information described in Scope of Program, below. These individuals, hereinafter referred to as Program Officers, will work with the appropriate vice presidents to designate representatives to oversee, coordinate and carry out various requirements of this program for r related to print

- Provided in order to obtain a financial service from the University
- Resulting from any transaction involving a financial service provided by the University
- Resulting from providing financial services to a student, faculty, staff or other third party.

Further, for purposes of this program, covered data and non-public information includes, but is not limited to bank and credit card information, income and credit histories and tax information, in both paper and electronic format, received directly or indirectly in the course of business by the University. In addition to non-public financial information, data such as names, addresses, phone numbers, credit card numbers, social security numbers and credit histories are covered under GLB.

Ri

12.5 Information Security
12.6 Password Management
13.8 Policy for Service of Subpoenas and Responding to Subpoenas or Other Requests for Records of Current or Former Students and Employees

Elements of the University's program to safeguard non-public financial information include, but are not limited to:

Evaluation and Revision of the Program

GLB mandates that this Program for the Security of Non-Public Personal Information be subject to periodic review and adjustment. Generally, review requirements of elements of this program are no less frequently than annually. However, some reviews, such as those in Information Technology Services, will occur more frequently than annually, due to constantly changing technology and constantly evolving risks. Further, the Program and associated policies are subject to regular review and modification, as appropriate, to assure ongoing compliance with existing and future laws and regulations.

Southern Methodist University
Information Security Program Addendum I
Information Technology Services Responsibilities

In order to protect the security and integrity of the University network and its data registry of all computers attached to the University network will be developed and maintained. The University operates under a distributed technology support model. Information Technology Services (ITS) will work with the appropriate areas of the University to ensure proper registry records are maintained for those systems under the direct responsibility of those areas. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, residence hall machine, etc.), and the person, persons, or department primarily responsible for the machine

ITS assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date for those systems under their direct responsibility. ITS will work with the other support organizations to ensure proper processes and procedures are in place for maintaining software patch currency. All support organizations 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 regularly, but no less frequently than annually.

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

The University Information Security Officer, working in cooperation with relevant University offices, will develop and maintain a data handbook, listing those persons or offices responsible for each non-public financial data field in relevant software systems (Financials, Student Administration, Advancement, and Human Resources). The University's Internal Auditor, ITS and the relevant offices will conduct ongoing audits of activity and will report any significant questionable activities.

The University Information Officer will work with the relevant offices (Human Resources, the Division of Enrollment Services, Development and External Affairs, and the Controller's Office) to develop and maintain a registry of those members of the University community who have access to non-public financial information. The University Information Officer, in cooperation with the various offices noted above, will work to keep this registry rigorously up to date.

ITS will ensure the physical security of all servers and terminals which contain or have access to non-public financial information. ITS will work with appropriate 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, which may expose the University to risks.

While the University has discontinued use of social security numbers as student identifiers,