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 Corner
- 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 departments in their areas handling or maintaining non-public financial data covered within the scope of this program.

The Program Officers assist University departments to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer non-public 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. Any questions regarding the Program or this document should be directed to a Program Officer.

Scope of Program

The Program applies to any record containing non-public information about students, faculty, staff or other third parties who have a relationship with the University, whether it is in paper, electronic or other form that is collected, handled or maintained by or on behalf of the University. For these purposes, non-public information includes, but is not limited to information pertaining to a student or other third party:

- 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.

Risk Identification and Assessment

The Program Officers must work with all relevant areas of the University to identify potential and actual risks to security and privacy of information, assessing external and internal risks to the security, confidentiality, and integrity of non-public financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. Risk identification and assessment will include evaluation of (i) employee training and management; (ii) adequacy of information systems, information processing, storage, transmission and disposal; and (iii) detection, prevention and response to attack on systems. The Program Officers will establish procedures to reassess risks and monitor compliance at the University no less frequently than annually. In addition, the department representatives designated by the vice presidents will document departmental procedures to safeguard non-public financial information in their areas, any incidents of breach of procedures, and responses thereto. The Program Officers will review this documentation no less frequently than annually and implement corrective actions, as necessary.

Safeguards

The University has or will implement policies and procedures to safeguard the non-public financial information covered herein. Existing policies address the privacy and confidentiality of personal information handled or maintained at the University. To the extent that non-public financial information is included with the records referenced in those policies, the privacy and confidentiality requirements of those policies also applies to non-public financial information. Further, to the extent that current policies address a standard of conduct and responsibility pertaining to one type of data or media (e.g., electronic), the same standard of conduct and responsibility also pertains to other types (e.g., printed). Relevant policies include:

1.12 Policy on Privacy of Health Information

1.18 Family Educational Rights and Privacy Act ("FERPA") Policy

12.3 Computing and Communications Policy
12.4 Electronic Payment Processing

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:

Employment training and management. The Program Officers will arrange appropriate training and communication through Human Resources' Professional Development Program. Through training and communication, faculty and staff handling or responsible for maintaining non-public financial information will be educated about the confidentiality and privacy requirements pertaining to the non-public financial data to which they have access. Review of the adequacy of training and communication as well as compliance with these requirements will be no less frequently that annually.

Information Systems and Information Processing and Disposal. This program requires the University to establish and maintain requirements to control access to University and third party systems to minimize the risk of a system breach, including, but not limited to password requirements, firewall and router specifications and encryption requirements. In addition, the Program requires each department to establish and maintain controls pertaining to the processing, storage, transmission and disposal of non-public financial data it manages or handles, including, but not limited to password requirements, deletion procedures, document shredding and the use of locked offices and file cabinets. The adequacy of and compliance with these requirements and specifications should be reviewed regularly, but no less frequently than annually.

Detecting, Preventing and Responding to Attacks. The University Information Security Officer is responsible for assessing the risks to non-public financial information associated with the University's electronic information systems, including network and software design, information processing, and the storage, transmission and disposal of non-public financial information. This evaluation will include assessing the Institution's current polices and procedures relating to University's network and network security, document retention and destruction. The University Information Security Officer will also assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

Service Providers and Contracts

The University will select and retain service providers who maintain appropriate safeguards for covered data and information. Vice Presidents will provide the Program Officers with a list of all service providers that have access to non-public financial information pursuant to their business relationship with the University. The Program Officers will work with University contacts of those service providers and Legal Affairs to develop appropriate addenda to all current service provider contracts requiring GLB compliance. Further, Legal Affairs 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 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 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 University employees 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. However, 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.

ITS will utilize software programs and tools with written 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 University Internal Auditor will periodically review the University's disaster recovery program and data-retention policies and present a report to the Vice President for Business and Finance, et al.