Southern Methodist University

Policy and Procedure for the Protection of Non-Public Personal Information and for Compliance with the Gramm-Leach-Bliley Act (GLBA)

BACKGROUND

GLBA is another name for the Financial Services Modernization Act of 1999 which regulates the disclosure of non-public personal information by financial institutions. SMU is considered to be a financial institution because we participate in financial activities, such as the Federal Perkins Loan Program. Therefore we must ensure the security and confidentiality of customer personal information. The University's focus is to protect all private data rather than to identify which particular law applies (GLBA, HIPAA, FERPA), in any given situation. Our emphasis applies to any record containing nonpublic 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.

The Federal Trade Commission implemented GLBA by issuing two rules: The Privacy Rule and the Safeguards Rule. Colleges and universities are deemed in compliance with the Privacy Rule if they already comply with the FERPA. The Safeguards Rule has five required components:

1. Designate a Security Program Coordinator responsible for coordinating the program.
2. Conduct a risk assessment to identify reasonably foreseeable security and privacy risks (which we have completed).
3. Ensure that safeguards are employed to control the identified risks; regularly test and monitor the effectiveness of these safeguards.
4. Oversee service providers, including selection of appropriate service providers and use of contract language to protect customer information handled by service providers.
5. Evaluate and adjust the program in light of relevant circumstances and changes in the business.

The SMU Program to comply with GLBA applies to any record containing nonpublic 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, nonpublic information includes, but is not limited to, information pertaining to a student or other third party:

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

For purposes of this program, covered data and nonpublic 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 SMU. In addition to nonpublic financial information, data such as names, addresses, phone numbers, credit card numbers, social security numbers and credit histories are covered under GLBA.

Customer information is any record containing nonpublic personal information about a customer obtained in connection with offering a "financial product or service". This includes paper, electronic or other form that is handled or maintained by or on behalf of the financial institutions or its affiliates. Examples include:

1. Social Security Numbers
2. Bank Account Numbers
3. Credit Card Account numbers
4. Date and/or location of birth
5. Account balances; payment histories; credit ratings, income histories
6. Drivers License Information
7. ACH (Automated Clearing House) numbers
8. Tax Return Information

REQUIRED ACTIONS

All University departments are responsible for identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer nonpublic information; evaluating the effectiveness of the current safeguards for controlling these risks; designing and implementing a safeguards program; and regularly monitoring and testing the program. 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.

Relevant SMU policies that already exist 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

SAFEGUARDS

There are three types of safeguards that must be considered and that departments must assume responsibility that adequate safeguards are in place within their areas of responsibility:

- Administrative
- Physical
- Technical

Administrative Safeguards

These are generally within the direct control of a department and include:

- Checking references on potential employees
- Training employees on basic steps as they must take to protect customer information
- Ensuring that employees are knowledgeable about applicable policies and expectations
- Limiting access to customer information to employees who have a business need
- Reducing exposure to the GLBA by requesting customer information only when it is required to conduct departmental activities
- Imposing disciplinary measures where appropriate

Physical Safeguards

These are generally within a department's control and include:

- Locking rooms and file cabinets where customer information is kept
- Using password activated screensavers
- Using strong passwords
- Changing passwords periodically and not sharing or writing them down
- Encrypting sensitive customer information transmitted electronically
- Referring calls or requests for customer information to staff trained to respond to such requests
- Being alert to fraudulent attempts to obtain customer information and reporting these to management for referral to appropriate law enforcement agencies
- Ensuring that storage areas are protected against destruction or potential damage from physical hazards, such as fire or floods
- Storing records in a secure area and limiting access to authorized employees
- Disposing of customer information appropriately:
    - Designate a trained staff member to supervise the disposal of records containing customer personal information
    - Shred or recycle customer information recorded on paper and store it in a secure area until the recycling service picks it up
    - Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information

- Promptly dispose of outdated customer information within record retention policies

Technical Safeguards

This is generally the responsibility of central IT personnel or departmental computing staff. Departments, however, should be knowledgeable about how their electronic customer information is safeguarded. If additional controls are warranted, departments should work with IT to improve safeguards. Departments are also responsible for alerting IT to the existence of customer information networks. Examples of technical safeguards include:

- Storing electronic customer information on a secure server that is accessible only with a password, or has other security protections, and is kept in a physically secure area.
- Avoiding storage of customer information on machines with an Internet connection
- Maintaining secure backup media and securing archived data
- Using anti-virus software that updates automatically
- Obtaining and installing patches that resolve software vulnerabilities
- Following written contingency plans to address breaches of safeguards
- Maintaining up-to-date firewalls particularly if the institution uses broadband Internet access or allows staff to connect to the network from home
- Providing central management of security tools and keeping employees informed of security risks breaches
- If credit card information or other sensitive financial data is collected, use a secure connection so that the information is encrypted in transit.
- If information is collected directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail.
- If you must transmit sensitive data by electronic mail, encryption is necessary.

Effective security management includes the prevention, detection and response to attacks, intrusions and other system failures, including steps mentioned above and the following:

- Backing up data regularly and storing back-up information offsite
- Imaging documents
- Shredding paper copies after imaging
- Other reasonable measure to protect the integrity and safety of information systems

SUMMARIZATION OF DEPARTMENT AND SCHOOL RESPONSIBILITIES

The responsibilities of all departments and schools are the following:

- Designate a key contact to work with the Security Program Coordinator on all GLBA matters

- Ensure that the key contact carries out periodic risk assessments and monitors the identified risks
- Adhere to policies, standards and guidelines for the safeguarding of private data, and ensure the employees with access to covered data do the same
- Ensure that new employees are made aware of the GLBA and its safeguarding requirements
- Ensure that companies that have access to University customers' nonpublic personal information on behalf of the University comply wit hthe privacy and safeguards requirements of GLBA.
- Review with the Budgets and Information Technology Services department changes to or any new software, networks or electronic service providers that include access or processing nonpublic personal information protected by GLBA to ensure that the technology in place includes appropriate safeguards.