Title: OIT0300 - Graham-Leach-Bliley Policy

Policy Owner: Chief Information Officer

Responsible Department: Office of Information Technology

I. Purpose

This document establishes the University's policy to meet the requirements of the Graham-Leach-Bliley Act (GLBA). The University community is based on principles of honesty, academic integrity, respect for others, and respect for others' privacy and property; thus, The University seeks to:

1. Protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under federal and state law; and
2. Ensure that the use of all digital records complies with the provisions of University policy and state and federal law; and
3. Allow for the free exchange of ideas and support of academic freedom.
4. This Information Security Plan ("Plan") describes safeguards implemented by St. Thomas University (STU) to protect covered data and information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA). Covered data includes customer financial information as well as other confidential financial information the University has voluntarily chosen as a matter of policy to include within its scope. These safeguards are provided to:
    - Ensure the security and confidentiality of covered data and information;
    - Protect against anticipated threats or hazards to the security or integrity of such information; and
    - Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.
5. This Information Security Program also identifies mechanisms to:
    - Identify and assess the risks that may threaten covered data and information maintained by STU;
    - Develop written policies and procedures to manage and control these risks;

- Implement and review the program; and
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information, and internal or external threats to information security.

II. Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by STU including its campus, institutes, and administration.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

III. Definitions:

A. **Unit:** An operational entity such as a Campus, Institute, division, or department.

B. **Sensitive Information:** Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical, privacy, or proprietary considerations. Sensitive information includes all data which contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or any other information that is protected by applicable laws, regulations, or policies.

IV. Procedures:

The University adopted the policy principles as established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Vice President for Administration has designated the Chief Information Officer (CIO) as the position responsible for information security at the University.

The University must develop or adopt and adhere to a program which demonstrates compliance with this policy and related standards. This program is the responsibility of the Chief Information Officer.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.

V. Policy:

A. User Privacy

- There should be no expectation of privacy on the part of the User.
- Users should be aware that any activity on University systems and networks may be monitored, logged, and reviewed by university approved personnel or may be discovered in legal proceedings. All documents created, stored, transmitted, or received on university computers and networks may be subject to monitoring by systems administrators.

B. GLBA mandates that the University appoint an Information Security Program Coordinator; conduct a risk assessment of likely security and privacy risks; administer a university wide training program for all employees who have access to covered data and information; oversee and monitor third party service providers and contracts; and evaluate and adjust the Information Security Program periodically.

C. Information Security Program Coordinator(s)

The Chief Information Officer has been appointed as the coordinator of this Program at STU. The CIO is responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to the University.

The CIO will consult with and identify units and areas of the University with access to covered data and will maintain a list of areas and units with such access.

D. **Covered data and information** for the purpose of this program includes all information required to be protected under the GLBA. Covered data includes information obtained from a student in the course of offering a financial product or service. In addition to this coverage, which is required under federal law, STU chooses as a matter of policy to include in this definition any and all sensitive data, including credit card information and checking/banking account information received in the course of business by the University, whether or not such information is covered by GLBA. Covered data and information include both paper and electronic records.

E. **Pretext calling** occurs when an individual attempts to improperly obtain personal information of STU customers so as to be able to commit identity theft. It is accomplished by contacting the University, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit (sometimes referred to as social engineering), convincing an employee of the University to release customer-identifying information.

F. **Student financial information** is that information that STU has obtained from a student or customer 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 and/or parent when offering a financial aid package, and other miscellaneous financial services. 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.

G. Identification and Assessment of Risks to Customer Information

The CIO and STU Cyber Security will conduct random assessments to continually identify and update potential risks. These risk assessments will include but are not limited to, consideration of employee training; information systems, including network and software design; information processing, storage, transmission, and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other systems.

STU recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, STU Cyber Security will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks.

Current and future safeguards implemented, monitored, and maintained by STU Cyber

Security are reasonable, and in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the University. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

H. Employee Management and Training

Background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information (e.g. Finance, Financial Aid, Business Office, Registrar) are performed. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts help minimize risk and safeguard covered data and information.

All employees will also undergo annual data security and privacy, FERPA, and other relevant trainings to ensure continued protection of covered data.

I. Physical Security

STU has addressed the physical security of covered data and information by limiting access to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to STU employees with an appropriate business need for such information. Furthermore, each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

J. Information Systems

Access to covered data and information via STU computer information systems is limited to those employees and faculty who have a legitimate business reason to access such information. Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data.

The University has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security to STU information systems. These policies and procedures, listed in Section 3 below, are available upon request from the Chief Information Officer.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, STU has discontinued the use of social security numbers as student identifiers in favor of the student ID number as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

K. Management of System Failures

Follow the Incident Response Plan that outlines procedures for responding to an actual or attempted unauthorized access to covered data and information.

The University will maintain effective systems and procedures to prevent, detect, and respond to attacks, intrusions, and other system failures. Such systems may include maintaining and implementing current anti-virus software; verification with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting users of covered data of potential threats and risks; backing up data regularly; and other reasonable measures to protect the integrity and safety of information systems.

L. Oversight of Service Providers

a. GLBA requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue, by contractually requiring service providers to implement and maintain such safeguards. The Security Program Coordinator will identify service providers who have or will have access to covered data and will work with the Finance Office and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data.

M. Monitoring and Testing

a. Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards. Monitoring will be conducted to reasonably ensure that safeguards are being followed. The level of monitoring will be appropriate based on the potential impact and probability of risks identified, as well as the sensitivity of the information provided.

N. Continuing Evaluation and Adjustment

a. This Information Security Program will be subject to periodic review and adjustment, at least annually. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Program Coordinator, who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate. The Information Security Program Coordinator, in consultation with the Technology Advisory Committee, will review the standards set forth in this program and recommend updates and revisions as necessary; it may be necessary to adjust the program to reflect changes in technology, the sensitivity of student/customer data, and/or internal or external threats to information security.

O. Related Policies, Standards, and Guidelines

a. STU has adopted comprehensive policies, standards, and guidelines relating to information security, which are incorporated by reference into this Information Security Program. They include:

   i. **Policies**

      i. Password Policy

      ii. Acceptable Use Policy

      iii. Email Policy

   ii. **Standards**

      i. Data Protection Safeguards

P. Communication

a. Upon approval, this policy shall be published on the STU website. The following offices and individuals shall be notified via email and/or in writing upon approval of the program and upon any subsequent revisions or amendments made to the original document:

   i. Vice President for Administrative Affairs

   ii. Chief of Staff

   iii. Provost

   iv. Faculty

   v. Staff

Q. Users WILL

a. Comply with all University policies to ensure confidentiality, integrity, and availability of university resources under their control.

b. Only use University resources for which the User has authorization.

c. Be responsible for using University-approved resources for electronic data and understanding the back up and retention policies associated with those resources.

d. Control and secure physical and network access to University resources, including data.

e. Properly log out ofsessions.

f. Monitor access to their accounts. If a User suspects unauthorized activity or that their account has been compromised, they must report the compromise to the Central Help Desk (CHD), and change passwords immediately (stuhelpdesk@stu.edu)

g. Install, use, and regularly update virus protection software, as directed by the IT team.

h. Use only supported and patched applications and operating systems on University-owned devices. Exceptions must be documented and approved by the CIO or their designee.

i. Where technically possible, abide by the password protection best practices specified for each University resource.

j. Use only the passwords and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose.

k. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of University resources.

l. Use University provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license.

R. Users WILL NOT

a. Share access codes or passwords.

b. Use accounts, access codes, privileges or IT resources for which they are not authorized.

c. Tamper, modify, or alter any restrictions or protections placed on their accounts, the University’s system, or network facilities.

d. Physically damage or vandalize University resources.

e. Commit copyright infringement, including file sharing of video, audio, or data without permission from the copyright owner.

f. Use University resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan horses, or other malicious code.

g. Obtain extra University resources or gain access to accounts for which they are not authorized.

h. Eavesdrop on or intercept other Users’ transmissions.

i. Attempt to degrade the performance or availability of any system or to deprive authorized Users access to any University resources.

j. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering.

k. Send email chain letters or mass mailings for purposes other than official University business.

l. Use University resources as an email relay between non-university email systems (routing email through university email systems between two non-university systems).

m. Engage in activities that violate state or federal law, a University contractual obligation, or another University policy or rule including but not limited to Human Resources policies and Standards of Conduct for students.

n. Comment or act on behalf of the University over the Internet without authorization.

o. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) to the network without prior approval from the Office of Information Technology (OIT).

p. Use of any device or application that consumes a disproportionate amount of network bandwidth without prior authorization.

q. Include or request Sensitive Information be included in unprotected electronic communication (email, instant message, text message, etc.).

S. University Rights

a. The University reserves the right to access, monitor, review, and release the contents and activity of an individual User’s account(s) as well as that of personal Internet account(s) used for University business. The University reserves the right to access any University owned resources and any non-University owned resources on University property, connected to University networks, or containing University data. This action may be taken to maintain the network’s integrity and the rights of other authorized Users. Additionally, this action may be taken if the security of a computer or network system is threatened, misuse of University resources is suspected, or the University has a legitimate business need to review activity or data. This action will be taken only after obtaining approval from the CIO, an authorized University office (e.g. Office of the Vice President for Administration, or Office of Human Resources), or in response to a subpoena or court order.

T. Copyrights and Licenses

a. Violation of copyright law or infringement is prohibited by University policy and state and federal law. Any unauthorized use of copyrighted material, may subject the User to disciplinary action as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct in the Human Resources Policy and Procedures.

b. Software may not be copied, installed, or used on University resources, except as permitted by OIT, the owner of the software, and the law.

c. Users will use properly licensed software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license.

d. All copyrighted information, such as text and images, retrieved from University resources or stored, transmitted, accessed, or maintained with University resources must be used in compliance with applicable copyright and other laws.

e. Copied material must be properly credited using applicable legal and professional standards.

f. Each Unit is responsible and accountable for maintaining records of purchased software licensure. The providing organization is responsible for maintaining records and information related to centrally provided software. These records are subject to internal audit for compliance.

U. Personal Use

a. University Resources are provided for use in conducting authorized University business. All users are prohibited from using these resources for personal gain, illegal activities, or obscene activities.

b. The prohibition against using the University's IT resources for personal gain does not apply to:
   i. Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members.
   ii. Consulting and other activities that relate to a faculty member's professional development or as permitted under University policy.
   iii. Incidental or casual personal use of these resources is permitted by this policy, except when such use:
   iv. Is excessive or interferes with the performance of the User's University responsibilities.
   v. Results in additional incremental cost or burden to the University's resources.
   vi. Violates any state or federal law or is otherwise in violation of this or any other University policy.
   vii. Results in additional risk to the confidentiality, integrity, and availability to the University's resources.

c. University IT resources may not be used for commercial purposes, except as specifically permitted under other written university policies or with the written approval of the CIO.

d. Any commercial use of University IT resources must be properly related to University activities and provide for appropriate reimbursement of taxes and other costs the University may incur by reason of such use.

e. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use.

f. Activities not appropriate for the ".edu" domain but otherwise permissible using University resources must use other domain designations.

V. Misuse of IT Resources

a. Users must report all suspected or observed illegal activities to the appropriate University or Campus administrative office. Examples include theft, fraud, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and viewing or distribution of child pornography.

b. Abuse of networks or computers at other sites through the use of University resources will be treated as an abuse of resource privileges.

W. Sunset Review

a. This policy will be reviewed every three (3) years to ensure continued best practices are utilized.

Last Reviewed: