UTC GLBA Information Security Program Standard

This document outlines the University's **GLBA Information Security Program Standard**. The University of Tennessee at Chattanooga is required by the Gramm-Leach-Bliley Act (GLBA) and its implementing regulation called the Safeguards Rule (the Rule) (16 CFR Part 314) to develop, implement, and maintain a comprehensive written Information Security Program (ISP) to safeguard customer information in the University's care.

The objectives of the ISP are to

1. Ensure the security and confidentiality of customer information
2. Protect against anticipated threats or hazards to the security or integrity of such information
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

Scope of Customer Information

The ISP applies to any record containing nonpublic personal information in paper, electronic or other form, about a student or other third party who has a continuing relationship with the University, where such information *is* ***obtained in connection with the provision of a financial service or product by the University***, and that is maintained by the University or on the University's behalf.

Nonpublic personal information means information:

1. A student or other third party provides in order to obtain a financial service or product from the University
2. About a student or other third party resulting from any transaction with the University involving a financial service or product, or
3. Otherwise obtained about a student or other third party in connection with providing a financial service or product to that person.

For example, nonpublic personal information includes bank and credit card account numbers, income and credit histories, as well as names, addresses, and social security numbers associated with financial information. Customer information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases.

Related Policies and Programs

The University has adopted comprehensive policies and practices to protect the privacy and security of information in its care. The University maintains a mandatory data protection training program for all employees. The ISP also includes all security standards found on the Information Security page:

https://www.utc.edu/information-technology/security/policies-guides-plans.php

Elements of the UTC Information Security Program

1. Information Security Program Coordinator(s).

The University has designated the University CISO as its ISP Coordinator (Coordinator). The Coordinator may designate others to oversee particular elements of the ISP. Questions regarding the ISP should be directed to the CISO or the designees.

2. Risk Identification and Assessment.

The CISO will identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. Further, the CISO will assess the sufficiency of any safeguards in place to control these risks. This applies to information in any format, whether electronic, paper, or other form.

The CISO will assess:

- *Employee training and management*: evaluate the effectiveness of current employee training and management procedures relating to the access and use of covered records.

- *Information systems, information processing, and disposal*: assess the risks to covered information associated with the University's information systems, including network and software design, as well as information processing, storage, transmission, and disposal.

- *Detecting, preventing and responding to attacks and system failures*: evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions, or other system failures.

3. Designing and Implementing Safeguards.

The CISO will design and implement safeguards to control the risks identified in assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Testing and monitoring may be accomplished through existing network monitoring, problem escalation procedures, and other data management practices.

4. Overseeing Service Providers.

The CISO will work with the Procurement and Contract Services unit to develop and incorporate standard contractual provisions for service providers that will require providers to implement and maintain appropriate safeguards. In conjunction with the Procurement and Contract Services unit, the CISO will assist in instituting methods to select and retain only those service providers capable of maintaining appropriate safeguards for customer information to which they will have access.

5. Adjustments to Program.

The CISO will evaluate and adjust the ISP as needed, based on risk identification and assessment activities and when material changes to the University's operations or other circumstances may have a material impact on the ISP.