The GLB Act: Guidelines for Faculty and Staff Relating to Customers' Nonpublic Personal Information

---

1. Introduction:

The Gramm-Leach-Bliley Act ("GLB Act"), also known as the Financial Modernization Act of 1999, is a federal law that requires organizations that are significantly engaged in providing financial services to protect the privacy and security of customers' nonpublic personal information. 15 USCA § 6801(a). As directed by the Federal Trade Commission ("FTC"), universities must develop information security programs that include administrative, technical and physical safeguards that, in general, will be used to collect, access, maintain, transmit and dispose of customer information. 16 CFR § 314.2(c). Implementation of the GLB Act's safeguarding rules through effective information security programs is intended to ensure the confidentiality of customer information, to protect against hazards to the integrity of the information and to protect against unauthorized access, use or theft of the information. 16 CFR § 314.3(b)(1-3).

Customer information is defined as "any record containing nonpublic personal information as defined in 16 CFR § 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates." 16 CFR § 314.2(b).

Nonpublic personal information is defined as:

- "Personally identifiable financial information; and
- Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." 16 CFR § 313.3(n)(1)(i-ii).

A list of nonpublic personal information includes "any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers." 16 CFR § 313.3(n)(3)(i).

Please review the University's online GLB Act training for more information regarding the University's practice with regard to the GLB Act.

2. Additional Guidelines for Faculty and Staff:

2.1 The successful implementation of the University's information security plan depends on the training and awareness of those employees who handle customer information in paper, electronic or other forms. References should be checked for potential new hires that will have access to customer information. All employees who could potentially handle customer information should be trained in the proper handling of customer information.

2.2 Access to customer information should be limited to only those employees who have a business reason for viewing it. When a business reason for viewing customer information exists, access should be allowed only to the extent that an employee needs to do his/her job. Requests for customer information should be referred to staff authorized and trained to handle such requests.

2.3 Records containing customer information should be stored in a physically secure area that is protected against theft and damage or destruction from physical hazards such as fire or floods. Rooms and file cabinets that contain customer information should be locked, and access should be limited to authorized employees. Computers should be locked or password activated screensavers should be used when employees are away from their computers. Sensitive customer information should be encrypted when it is electronically transmitted or stored online.

2.4 A secure connection should be used when customer information is collected or transmitted electronically. Consumers should be warned against transmitting sensitive data via electronic mail. If sensitive data is transmitted via electronic mail, then it should be encrypted to limit access to only authorized recipients. There are several ways to encrypt data (depending upon the system being used and the type of data that is being transmitted, etc.). Contact Information Technology at www.uh.edu/infotech for assistance.

2.5 Records containing customer information should be disposed of in a secure manner. Promptly dispose of outdated customer information in accordance with university record retention policies. Dispose of paper records by shredding them and storing them in a secure area until discarded. Dispose of data on electronic media by securely erasing the data and/or effectively destroying the hardware.

2.6 Data systems should be managed in such a way that unauthorized intrusions or attacks can be promptly detected and addressed. Systems should be properly maintained with regularly updated l patches that address software weaknesses, up to date anti-virus software and current firewalls. Customer data should be backed up regularly. Employees should use strong passwords and regularly change passwords for accounts used to access customer data.

2.7 Customers should be promptly alerted if their nonpublic personal information is subjected to unauthorized access or damage. Employees should be alert to fraudulent attempts to obtain customer information and report those attempts to management or appropriate law enforcement agencies.

2.8 Failure to comply with the requirements of the GLB Act could lead to damage, loss and unauthorized access and use of customers' nonpublic personal information. Disciplinary procedures may be imposed for security policy violations.