

Business Affairs Financial Information Security Plan

Effective May 23, 2003

I. Purpose

The Gramm-Leach Bliley Act (GLBA) requires financial institutions, including colleges and universities, to develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information issue. The scope of this act covers primarily financial institutions but also organizations containing financial functions including colleges and universities. This purpose of this plan is to assure that the Business Affairs Office of the University of Houston-Downtown is in compliance with the GLBA.

II. Definitions

- *Customer information* means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or another form, that is handled or maintained by or on behalf of you or your affiliates.
- *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- *Nonpublic personal information* means 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 information that is not publicly available.
- *Service provider* means any person or entity that receives, maintains, processes or otherwise is permitted access to customer information through its direct provision of services to a financial institution.

III. Objectives

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats to the security or integrity of such records
- Protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer

IV. Risk Assessment

The following is a list of threats to customer financial information that will be mitigated through the implementation of this plan:

- Unauthorized access to data through software application
- Unauthorized use of another user's account and password
- Unauthorized viewing of printed or computer displayed financial data
- Release of customer financial information to unauthorized persons
- Improper storage of printed financial data
- Unprotected documentation usable by intruders to access data
- Improper destruction of printed material

V. Financial Information Security Plan

- Electronic access to customer financial information is protected by user names and passwords. Each major area within the department has a Director that serves as the security officer for that area. The security officers are responsible for determining the level of access granted, granting and removing access for all employees within their area. The appendix includes forms used by security officers to grant and remove access to their data and a policy statement regarding the use of this access.
- All passwords are kept confidential and are not shared by other users.
- All users are required to log off or lock their computer terminals when they are away from their work area.
- Computer monitors used to display customer financial information are not to be left unattended with customer information still displayed.
- Computer monitors are placed in such a way as to prevent casual viewing by unauthorized persons.
- A locked door secures access to all work areas during non-business hours. Only authorized individuals are given keys. A key request form must be completed by the employee and approved by the security officer before the Physical Plant Office will issue a key. The Physical Plant is responsible for maintaining the key log for all employees. Lost or stolen keys are reported immediately to the Physical Plant Office.
- Printed copies of customer financial information are handled only by authorized personnel and kept in areas with restricted access. They are not left in the open or in unattended areas. All printed records containing customer financial information are shredded when they are no longer needed.
- Printed copies of customer financial information that are kept for record retention requirements are maintained in a secured location and shredded at the end of the retention period.
- Requests for information from third parties are handled in accordance with the Family Educational Rights and Privacy Act (FERPA).
- All outside service providers will be required to provide UHD with a copy of their financial information security plan and will be expected to operate within the guidelines imposed by the GLBA.

VI. Employee Training

- Training of all employees includes an explanation of the purpose of the GLBA and a copy of this plan. Each employee, including student workers, will sign that they have received a copy of this plan and that they understand their responsibilities under this plan. This statement will be on file in the security officer's office.
- Additional training will be conducted as needed to train employees on all new issues or modifications to this plan. Annual refresher training for all employees will be held.

VII. Appendix

- University of Houston-Downtown, Division of Information Technology, Computer Account Request Form
- University of Houston-Downtown, Policy Statement PS 08.A.04
- University of Houston-Downtown, Policy Statement PS 08.A.05

I, _____, hereby acknowledge that I have received a copy of the Business Affairs Financial Information Security Plan. I have read this plan and fully understand my responsibilities under this plan.

Employee Signature

Date