GLBA: Safeguarding of Confidential Financial and Personal Information

Contents

Introduction

Wright State University (the "University") is committed to the ongoing protection of confidential financial information that it may collect from faculty, staff, students, alumni and others. The Gramm-Leach-Bliley Act* ("GLBA") addresses the privacy of non-public identifying information and describes the necessity for administrative, technical and physical safeguarding of that type of information. GLBA mandates that the University develop, implement and maintain a comprehensive information security program (the "Plan") to insure the safeguarding of Confidential Financial Information ("CFI"). The University obtains CFI from students, faculty, staff and others that may include, but is not limited to:

- Names
- Social Security Numbers
- Date and location of birth
- Gender
- Credit card numbers
- Drivers license information
- Salary history
- Personal check information
- Tax or financial information from a student or a student's parents

Specific Authority

The GLBA is implemented by 16 CFR Part 314 and the Federal Trade Commission (FTC) Rules on "Standards for Safeguarding Customer Information". This policy statement sets the University's policy to ensure ongoing protection of CFI and serves as written evidence of a Security Plan in compliance with 16 CFR Part 314.3(a). The GLBA uses the term "customer" to describe persons whose information is to be protected under the Act.

GLBA Objectives and Requirements

The objectives of GLBA are to:

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

"Customers" of the University include, but are not limited to faculty, staff, students, alumni and others. To comply with safeguarding confidential financial records and related personal information and achieve these objectives, the University is required to:

- Designate one or more employees to coordinate the safeguards

- Identify and assess risks to customer information and evaluate the effectiveness of the current safeguards
- Designate and implement a safeguards program that includes regular compliance monitoring and evaluation
- Select appropriate service providers and ensure that contracts with those providers include adequate safeguards for customer information
- Provide for evaluating and adjusting the program in light of relevant circumstances
- Ensure that all new and existing employees who are involved in activities covered under the Act receive safeguarding training

Who Receives Information and Why?

As required by GLBA, the University does not disclose any non-public financial information about our students/customers, or former student/customers, to anyone, except as permitted by law. The University may exchange such information with its affiliates and certain nonaffiliated third parties (under limited circumstances) to the extent permissible under law to service accounts, report to credit bureaus, provide loan services, or provide other financial services related activities.

Upon request, a student/customer shall be informed of the existence, use and disclosure of their information, and shall be given access to it. Students/customers may verify the accuracy and completeness of their information, and may request that it be amended, if appropriate. Each department/unit is responsible for obtaining and presenting information when requested by a customer.

*15 U.S.C. §6801

Scope of This Policy

This policy applies to all University personnel who administer, manage, maintain or use CFI. It also applies to the supervisors and unit administrators of those individuals. It applies to all locations of this information, whether on campus or from remote locations.

CFI includes any paper or electronic record containing non-public personal information about a customer that the University, or its affiliates, handle and maintain. CFI includes any personally identifiable information provided by students or others (such as loan applications, credit card numbers, account histories, and related consumer information) in order to obtain a financial product or service from the University (such as financial aid).

Information Security Officer

The department that is responsible for the implementation and execution of the Plan at the University is the Office of Information Security). All correspondence and inquiries should be directed to the Information Security Officer at Computing and Telecommunications Services. The Office of General Counsel will coordinate with the Information Security Officer to maintain the Plan.

The ISO should assist the various offices of the University that have access to CFI to identify and reasonably foresee internal and external risks to the security of CFI. University Offices likely to be

affected are the University Bursar, the Registrar's Office, the Admissions Office, the Student Financial Aid Office, Graduate Studies, the Office of Residence Services, and the University Center for International Education, Career Services and CaTS. Further, the ISO should (1) evaluate the effectiveness of the current safeguards for controlling these risks; (2) regularly monitor and test the Plan; and (3) design and implement any necessary changes to the Plan. The ISO should also work with other relevant Schools and Departments to identify third-party providers who have access to CFI so that the University secures contracts with those third party providers to ensure the protection of CFI.

Identification of Risks and Risk Assessments

Each University department or office that handles or maintains CFI is responsible for identifying the type and form of the CFI within their departments or offices and taking appropriate measures to mitigate those risks. Examples of relevant areas to be considered when assessing the risks of unauthorized customer information disclosures includes, but is not limited to:

- Unauthorized access to CFI by employees, third-parties or through requests
- Compromised system security as a result of "hacking" or other unauthorized access
- Failure to properly protect passwords (e.g. posting passwords in publicly viewable places)
- Interception of data during transmission
- Physical loss of data in a disaster
- Corruption of data or systems
- Paper forms containing CFI that are not restricted to authorized employees
- Paper forms and computer systems vulnerable to break-in after hours
- Paper forms and computer systems left unattended during business hours, and
- Errors introduced into the system by authorized or unauthorized persons

The University recognizes that this may not be a complete list of the risks associated with the protection of CFI. Since technology growth is not static, new risks are created regularly. Accordingly, the ISO will monitor for the development of new risks.

Implementation of Policy

Wright State University's Safeguarding Program has six key components:

- Employee Training and Management
- Information System Security
- Detecting, Preventing and Responding to Attacks, Intrusions and Other System Failures
- Physical Security of Paper Records
- Disposal of Records
- Oversight of Service Providers and Contracts

Employee Training and Management

All University employees that will have access to CFI shall receive proper training on the importance of confidentiality of certain records, such as student records, student financial information, credit card numbers, credit checks, bank accounts, tax records and any other CFI maintained by the University, and the proper storage of CFI materials. All University employees with access to computers shall be trained in the proper use of CFI and the use of passwords to prevent the transmission or communication of CFI to unauthorized persons. Protecting Financial Privacy in the New Millenium Training Module.

Information System Security

Access to CFI through the University's computer network shall be limited to those University employees who have a valid legitimate reason to have such information. All CFI that may be accessed through the University's computer network shall be protected by, and each University employee that needs to have access to CFI shall be assigned, a user name and password. Such user names and passwords shall expire periodically and shall not be posted in public spaces. The University will take all reasonable and appropriate steps consistent with current technological development to ensure that all CFI remains secure.

Information systems include network and software design, information processing, storage, transmission, retrieval, and disposal.

Network and software systems will reasonably limit the risk of unauthorized access to covered data.

Safeguards for information processing, storage, transmission, retrieval and disposal may include:

- requiring electronic data (covered by the GLBA) be entered into a secure, password-protected system
- using secure connections to transmit data outside the University; using secure servers
- ensuring data is not stored on transportable media (floppy drives, zip drives, etc.)
- permanently erasing covered data from computers, diskettes, magnetic tapes, hard drives, or other or other electronic media before re-selling, transferring, recycling, or disposing of them
- storing physical records in a secure area and limiting access to that area; providing safeguards to protect covered data and systems from physical hazards such as fire or water damage
- disposing of outdated records under a document disposal policy; shredding confidential paper records before disposal
- other reasonable measures to secure data during its life cycle in the University’s possession or control

Detecting, Preventing, and Responding to Attacks, Intrusions, and Other System Failures

The University will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and installing patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies;

backing up data regularly and storing back up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

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, and to quickly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits, and any other reasonable measures adequate to verify that information security's controls, systems and procedures are working.

Physical Security of Paper Records

Only employees who have a legitimate and valid reason to have CFI shall have access to any physical paper records. The records should be kept in a secure place, such as a locked office or file drawer, to prevent unauthorized access. Such records should be secured in locked cabinets whenever an authorized employee is not present with the records, particularly overnight.

Disposal of Records

The University should only keep physical paper records and electronic documents for as long as they are being actively used by the University, or as necessary to comply with state, federal or local law, or the University's document retention policy. Paper documents containing CFI should be shredded at the time of disposal. Electronic records should be deleted and magnetic media should be erased.

Oversight of Service Providers and Contracts

GLBA requires that the University take reasonable steps to select and retain service providers that will maintain safeguards necessary to protect CFI. Contracts entered into with such service providers after the effective date of this policy should include a commitment by such service providers to the safeguarding of CFI. The ISO will work with the General Counsel to put such agreements in place, being mindful of the 2-year grandfathering of service contracts entered into not later than June 24, 2002.*

*16 C.F.R. Part §314.5(b)

Review & Revision of the Plan

GLBA mandates that the Plan be subject to periodic review and adjustment. The Plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the University's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be done at the joint discretion of the University's Internal Auditor and the Information Security Officer, but no less often than annually.