01/02/2013

University of Evansville Privacy and Safeguarding Guidelines

Background:

The Federal Trade Commission rule related to the safeguarding of customer financial information stemming from the Gramm-Leach-Bliley Act (Act) enacted on November 12, 1999 applies to colleges and universities and we must now comply with the requirements. The Act reforms the financial services industry and addresses concerns related to consumer financial privacy including the safeguarding of consumer information. The Act addresses the privacy of non-public customer information and describes the necessity for administrative, technical, and physical safeguarding of customer information. The Act broadly defines "financial institution" as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including "making, acquiring, brokering, or servicing loans" and "collection agency services." Because higher education institutions participate in financial activities such as making Federal Perkins Loans, FTC regulations consider them financial institutions for purposes of compliance with the Act. Due to the efforts of NACUBO and other higher education associations, under regulations promulgated in May 2000, colleges and universities are deemed to be in compliance with the privacy provision of the Act if they are in compliance with the Family Educational Rights and Privacy Act (FERPA).

General Standards for Safeguarding Customer Information:

The University of Evansville must meet a general standard in order to comply with the "to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards" for non-public customer information. A customer is a type of consumer, namely, an individual who has an ongoing relationship with an institution that provides a financial product or service. Therefore, our main customers are the students of University of Evansville.

Safeguarding objectives are:

- To ensure the security and confidentiality of customer information
- To protect against any anticipated threats to the security or integrity of such information; and
- To guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

The required elements of the security program are:

- Designate an employee(s) to coordinate the information security program
    - The 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

    - Identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks
- At a minimum, such a risk assessment should include consideration of risks in each of the following operational areas:
    - Employee training and management
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
    - Detecting, preventing and responding to attacks, intrusions, or other systems failures
- Oversee service providers by taking steps to select and retain providers that are capable of maintaining appropriate safeguards for customer information
- Contractually require service providers to implement and maintain appropriate safeguards
- Periodically evaluate and adjust the information security program based on the results of testing and monitoring

In order to address the requirements, we have drafted a set of guidelines that will provide a draft framework for the design and implementation of an information security program.

University of Evansville Financial Information Privacy and Safeguarding Guidelines

Background

Adequately securing customer information is not only the law, it makes good business sense. Above all, it is our ethical responsibility to you, our customer as your fiduciary agent for this information, to ensure its safeguarding while in our possession. When we show you, our customer, that we care about the security of your personal information, we increase your level of confidence in our institution. Poorly managed customer data can lead to identity theft. Identity theft occurs when someone steals a consumer's personal identifying information to open new charge accounts, order merchandise or borrow money.

Information Collected and Stored

As an educational institution, the University of Evansville collects, retains, and uses non-public financial information about individual customers, as allowed by law, to provide services. Non-public financial information is collected from sources such as:

- Applications and/or other forms;
- Financial transactions (Checks, credit cards, and ACH)
- Information about your transactions with us, our affiliates, or others;
- Information we receive from consumer reporting agencies; and
- Information from governmental agencies.

Information Shared

The University of Evansville may disclose nonpublic financial information about you with our business affiliates and other affiliated third parties under certain circumstances to provide services. Any non-public financial information sharing is conducted in strict adherence to applicable law. The University of Evansville will not disclose any non-public personal information about you to anyone except as permitted under law.

Who Receives Information and Why

The University of Evansville does not disclose any non-public financial information about our students/customers, or former student/customers, to anyone, except as permitted by law. We may exchange such information with our 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.

How Your Information Is Protected

The University of Evansville understands that the protection of your non-public financial information is of the utmost importance. Providing for administrative, technical and physical safeguarding of your privacy is our obligation. We restrict employee access to customer information only to those who have a legitimate business reason to know such information, and we educate our employees about the importance of confidentiality and customer privacy. As a part of this commitment, we provide the following Privacy and Safeguarding guidelines:

Guideline 1 - Accountability

The University of Evansville is responsible for maintaining and protecting the customer financial information under its control. In fulfilling this mandate, each functional area of The University of Evansville is required to educate their employees and comply with these guidelines. For each functional area dealing with non-public information, specific The University of Evansville employees in each functional area must be identified as the Financial Information Privacy Custodian. This custodian is responsible for ensuring the following policies and procedures are fulfilled for their area:

The Office of Technology Services (OTS) will perform and maintain an inventory of all information that requires protection. Custodians will contact OTS as new systems or data is being stored or if any relevant changes occur to the collection, storage or disposal of information.

Guideline 2 – Purpose

The purposes for which student/customer financial information is collected shall be identified before or at the time the information is collected. If any financial information is maintained in a University of Evansville area, a written statement must be held in the department, stating the purpose of the information, how it is being used, the length of time it will be held and how the information will be destroyed. Example: If the department maintains files with copies of checks

or credit card information, the department must have a departmental policy on hand which states why copies are maintained, how long they are to be held and how they will be destroyed when no longer needed. The Accounting and Auditing department and OTS will work with the Custodians to help identify and state the purpose of the information collected.

Guideline 3 – Collection

The student/customer information collected must be limited to those details necessary for the purposes identified by the University of Evansville. Information must be collected by fair and lawful means. The University of Evansville departments may only collect the information, which is needed to perform the task at hand. Example: A department may not collect a driver's license number without a policy on hand that addresses the specific purpose and use of this information.

Guideline 4 - Use, Disclosure and Retention

Student/customer information may only be used or disclosed for the purpose for which it was collected unless the student/customer has otherwise consented, or when it is required or permitted by law. Student/customer information may only be retained for the period of time required to fulfill the purpose for which it was collected and will be disposed of in a secure manner when the purpose has been fulfilled. If the information is to be used for another purpose, consent must be obtained from the customer prior to use. When obtaining consent, either initially or for a revised purpose, the length of retention must be stated and how the information will be disposed must be disclosed to the customer. Example: If a department, on a given application, maintains a driver's license number, but the department now wishes to use this information to process another application, the customer must give new consent. In the new consent, the length of time this information will be held and how the information will be destroyed must be stated. The University of Evansville will manage private non-public information in accordance with all applicable state and federal laws relating to the use, disclosure and retention of private non-public information.

Guideline 5 – Safeguarding

Customer information must be protected by security safeguards that are appropriate to the sensitivity level of the information obtained. Each functional area must review the information being retained and establish appropriate physical safeguards for the data. Physical paper data such as copies of checks must be kept in locking rooms and file cabinets. Computer stored data can be protected with password-activated screensavers, by utilizing strong passwords of at least eight characters, by changing passwords periodically and not posting passwords near employees' computers, by encrypting sensitive customer information when it is transmitted electronically over networks, by referring calls or other requests for customer information to a designated individual who has been trained, and recognizing any fraudulent attempt to obtain customer information and reporting it to Audit Services for evaluation. Data custodians in conjunction with OTS will provide the training and oversight necessary to insure the appropriate safeguarding of customer information.

Guideline 6 - Openness

The University of Evansville is required to make information available to customers concerning the policies and practices that apply to the management of their information. Each functional area is responsible for maintaining a policy and practice document which details the financial information obtained by the department, and their adherence to these guidelines.

Guideline 7 - Access

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.

Guideline 8 - Handling Customer Complaints and Suggestions

Students/customers may direct any questions or inquires with respect to the privacy principles outlined above or about our practices by contacting the designated person(s) accountable for privacy in each University of Evansville Department. Each department/unit is responsible for dealing with customer complaints and suggestions.

Guideline 9 – Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Security must be maintained throughout the life cycle of customer information.

- Storage of information
- Secure data transmission
- Disposal of customer information
- Erase all data when disposing of computers, or destroy hard drives containing sensitive information
- Responding to system failure

The University of Evansville (UE) maintains centralized control of public and non-public data through various applications. These applications maintain their own internal security measures which are administered by the assigned data custodian for these applications. Furthermore, for system access to data, an initial password is required to gain access to the applications. This layer is known as AceNet Access. A small number of AceNet administrators in the Office of Technology Services have the ability to control access to the AceNet accounts. Hence, a two-tier access control is maintained for normal operation of these applications. Physical access to the centralized computers is controlled by keyed access to the data center. We use a localized security monitoring review access to the data center. Access to this facility is restricted to those who have a demonstrated need. All access is granted by the Assistant Vice-President of Technology Services.

OTS maintains secure, offsite storage of institutional data for disaster recovery purposes. This facility is located in a separate, secure location. The data tapes are kept in a locked vault inside the facility, which is set up with continuous intrusion and fire detection systems.

Data transmission of institutional data is routed through the University of Evansville AceNet infrastructure, which is currently a switched 10/100/1000 Ethernet network. For the most part, no encryption of data is made when transmitting institutional data across AceNet to communication distribution areas. Where possible, data transmission is encrypted. For example, web based services that have non-public, authenticated data, are usually encrypted using SSL.

It is our desire that all or our data be encrypted during transmission. We also have a goal that all institutional data that leaves our network be encrypted using encryption methods like PGP. We anticipate in the near future that we will require such transactions to help safeguard our data from third party intervention.

Institutional data transferred to PCs is the responsibility of the end user. All users who have access to institutional data are required to sign a document outlining their responsibility to that data. End users are responsible for ensuring that institutional data is securely maintained and properly destroyed.

The University of Evansville maintains a policy for deleting all data on computers that are sold or disposed of.

OTS monitors for intrusions or other security violations. OTS has an assigned person to be the primary contact for such occurrences. OTS maintains a log of incidents and resolutions of all security violations.

Guideline 10 – Monitoring and Testing of Security

The information security program will need periodic evaluation and adjustment based on the result of the testing and monitoring any material changes to operation, or any other circumstances that are known to have or that may have a material impact on the information security program. Audit Services will provide the oversight to insure the success of this plan.