POLICY

9-05 Gramm-Leach-Bliley Act Compliance Plan

Approval
LT Approved: 5/29/18
Effective Date: 5/29/18
Revised: 5/29/18
Responsible Party: Executive Director, Information Technology

Policy Statement

Purpose:

This compliance plan ("Plan") describes WSU Tech's safeguards to protect non-public, financial-related personal information ("covered information") in accordance with the requirements of the Gramm-Leach-Bliley Act of 1999 (GLBA). The Safeguards Rule of the GLBA, as defined by the Federal Trade Commission (FTC), requires financial institutions, which the FTC explicitly indicated includes higher education institutions, to have an information security program to protect the confidentiality and integrity of personal information.

These safeguards are provided to:

A. Ensure the security and confidentiality of covered information.
B. Protect against anticipated threats or hazards to the security or integrity of such information.
C. Protect against unauthorized access to or use of covered information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

A. Designate an employee or employees to coordinate the information security program.
B. Identify and assess the internal and external risks that may threaten covered information maintained by WSU Tech.
C. Design and implement safeguards to control the identified risks.

D. Oversee service providers, including third party contractors, to ensure appropriate safeguards for covered information are maintained.
E. Periodically evaluate and adjust the information security program as circumstances change.

Scope:

This policy applies to all WSU Tech divisions, departments, affiliated organizations and third party contractors that create, access, store or manage covered information.

Definitions:

Covered Information:

Information that WSU Tech has obtained from a customer (e.g., a student) in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Service Providers:

Any person or entity that receives, maintains, processes, or otherwise is permitted access to covered information through its direct provision of services to the College.

Information Security Program:

A. Responsibilities

The Executive Director, Technology is responsible for coordinating and overseeing all elements of WSU Tech's information security program. The Executive Director will work with appropriate personnel from other offices as needed (such as the Registrar's Office, Financial Aid, Enrollment Management, and Finance) to ensure protection of covered information.

B. Risk Identification and Assessment

Under the direction of the Executive Director, risk and privacy assessments are performed for all information systems that house or access covered information. These risk and privacy assessments shall address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

Internal and external risks include, but are not limited to:

1. Unauthorized access of covered information by persons within or outside the College.
2. Compromised system security as a result of human error, vulnerabilities, infection by malicious software, or unauthorized system access
3. Interception of data during transmission
4. Loss of data integrity
5. Physical loss of data in a disaster
6. Errors introduced into the system
7. Corruption of data or systems
8. Unauthorized access through hardcopy files or reports
9. Unauthorized disclosure of covered information through third parties

Risk and privacy assessments are used to determine the likelihood and magnitude of harm that could come to an information system, the affected individual(s), and ultimately the College itself in the event of a security breach. By determining the amount of risk that exists, the College shall determine how much of the risk should be mitigated and what controls should be used to achieve that mitigation.

Both risk and privacy assessments shall be performed prior to, or if not practical, immediately after acquisition of an information system (in the event that the information system is owned/operated by the College) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of the College). Further, the risk and privacy assessments shall be reviewed and, where required, updated after three years or whenever a significant change is made to the information system, whichever comes first.

Risk assessment should include consideration of risks in each of the following operational areas, in accordance with the requirements of the GLBA:

1. Employee training and management

Prior to being granted access to covered information, new employees in positions that require access to covered information (e.g., Academic Advisors, Registrar staff, Financial Aid staff, etc…) will receive training on the importance of confidentiality of student records, student financial information, and other types of covered information, and the risks of not providing appropriate protection. Furthermore, all employees receive annual training in general information technology security. Training also covers controls and procedures to prevent employees from providing confidential information to an unauthorized individual through social engineering or improper disposal of documents that contain covered information. All training will be reviewed and, where needed, updated at least annually.

All new employees with access to covered information must pass a criminal background check as a condition of employment.

2. Information systems

Including network and software design, as well as information processing, storage, transmission, and disposal.

3. **Incident management**

Including detecting, preventing and responding to attacks, intrusions, or other systems failures.

Designing and Implementing Safeguards

The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Executive Director will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers

In the process of choosing a service provider that will maintain or regularly access covered information, the selection and retention processes shall ensure the ability of the service provider to implement and maintain appropriate safeguards for covered information. In addition, contracts with service providers may include contractual protections which will require such providers to implement and maintain appropriate safeguards.

Program Evaluation and Adjustment

The Executive Director will periodically review and adjust the information security program as it relates to the GLBA requirements, with input from relevant stakeholders. Program evaluation should be based on results of testing and monitoring of security safeguard effectiveness and reflect changes in technology and/or operations, evolving internal and external threats, and any other circumstances that have a material impact on the information security program.