The Gramm Leach Bliley Act addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions. This GLBA Information Security Program describes safeguards implemented by the University of West Georgia (UWG) to protect covered data and information in compliance with the FTC’s Safeguards Rule of the Gramm Leach Billey Act (GLBA). These safeguards are provided to:

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

This GLBA Supplement also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by UWG;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the program; and
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Policy Statement:

GLBA mandates that the institution appoint GLBA information security program coordinator(s), conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the GLBA Information Security Program periodically.

GLBA Program Coordinator

The President (or designee) is responsible for the development of the GLBA Program at UWG. The Information Technology Services (ITS) Information Security Officer, the Director of Financial Aid, and the Director of the Bursar Office are considered the GLBA program coordinators for their respective areas.

Each program coordinator is responsible for assessing the risks associated with unauthorized transfers of covered data and information, and implementing procedures to minimize those risks, instituting a training program for covered employees, and overseeing assigned service providers and contracts. Internal Audit personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security policies and practices delineated in this program.

Covered Data and Information

For the purpose of this program, covered data includes student financial information that is protected under the GLBA. UWG considers student financial information to be that which UWG has obtained from a student or customer in the process of offering a financial product or service, or such information provided to UWG by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student or a parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.
**Departments Covered by GLBA**

The following table illustrates the mapping of department and data that fall under the GLBA.

<table>
<thead>
<tr>
<th>Department</th>
<th>Types of Covered Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bursar</td>
<td>Loans, Payment Plans, 1098Ts.</td>
</tr>
<tr>
<td></td>
<td>PII (SSN, billing information, credit card info, bank account info, date of birth, driver’s license number)</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>Loans, Payment Plans, financial aid disbursement information, tax returns.</td>
</tr>
<tr>
<td></td>
<td>PII (SSN, billing information, credit card info, banking account info, date of birth, driver’s license number)</td>
</tr>
<tr>
<td>ITS</td>
<td>Responsible for storage of covered data.</td>
</tr>
</tbody>
</table>

**Identification and Assessment of Risks to Customer Information**

UWG recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, information security program coordinators will ensure periodic risk assessments are conducted. The UWG ITS Risk Assessment Procedure will be used to ensure risk assessments and subsequent remediation actions are conducted.

**Employee Management and Training**

References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information (e.g. Cashier’s Office, Financial Aid, Bursar, Information Technology Services) are checked/performed. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information.
Department heads are responsible for ensuring that new employee training and annual refresher training occurs and is documented. Information security program coordinators are responsible for reviewing the training material for completeness.

**Physical Security**

Physical security of covered data and information is available to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to employees with an appropriate business need for such information. Furthermore, each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. UWG Procedure 8.2.2 Data Storage and Use as well as UWG Procedure 8.2.7 Media Hardware Disposal support the GLBA program.

**Information Systems**

Access to covered data and information via UWG’s computer information systems is limited to those employees and faculty who have a legitimate business reason to access such information. UWG has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security to the information systems. These policies and procedures are listed in the “Related Documentation” section below.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, UWG has discontinued the use of social security numbers as student identifiers in favor of the student 917 number as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

**Monitoring of Information Systems**

UWG ITS has an outsourced system monitoring service and a Cybersecurity Incident Response Plan which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This document is available upon request from the Information Security Officer.

**Oversight of Service Providers**

GLBA requires the institution to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. UWG ITS has a Third Party Agreement that defines how service providers may store, use, and dispose of University data. ITS, Purchasing Services and UWG Legal Counsel work together to ensure service providers contracts contain appropriate terms to protect the security of covered data.

**Continuing Evaluation and Adjustment**

This document will be managed by the ITS Document Development process to ensure it is periodically reviewed and remains current.

**Communication**

Upon approval, this policy shall be published on the UWG Policy website. The following offices and individuals shall be notified via email upon approval of the program and upon any subsequent revisions or amendments made to the original document:

- Bursar
- Financial Aid
- Information Technology Services

**Related Information:**
**Document Revision History**

Periodic review of this document is managed by the ITS Document Development and Document Management Procedure. See that document for details.

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision Notes</th>
<th>Revision Number (one up number)</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2019</td>
<td>Creation</td>
<td>0</td>
</tr>
</tbody>
</table>