# GLBA SECURITY POLICY

***Division: Information Technology***

## *Policy Statement*

This policy is designed to protect and mitigate threats to the information security and privacy of stakeholder data and information at Terra State Community College (TSCC). This policy provides an outline of Terra State Community College's comprehensive written security policy in compliance with Gram-Leach-Bliley Act (GLBA).

## *Policy Details*

The GLBA along with the more recent Standards for Safeguarding Customer Information (Final Rule) addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions. Colleges and Universities are subject to GLBA because they collect and maintain financial information through student lending and alumni processes. Primary objectives of GLBA include:

- Ensuring the security and confidentiality of customer financial information
- Protecting against any anticipated risks or threats to the security and integrity of covered data
- Protecting against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer.

This policy applies to customer financial information Terra State Community College receives in the course of business as required by GLBA and the Federal Trade Commission's (FTC) updated Safeguards Rule, as well as other confidential information the institution has chosen to include within its scope.

This IT security framework is based on the National Institute of Standards Technology Special Publication 800-171 (NIST 800-171) which provides a set of baseline security controls and is used to meet multiple compliance requirements. The FTC uses NIST 800-171 framework to assess the security posture of an organization. Further, the Federal Student Aid (FSA) recommends the use of NIST 800-171 controls as GLBA safeguards. Using the NIST 800-171 allows an organization to assess and evaluate its specific environment and determine what security controls are necessary to best protect its organizational operations and assets. The NIST 800-171 prescribes different sets of controls for systems that are considered low, medium or high impact and is continuously updated to respond to newly discovered threats or breaches.

The practices set forth in this document will be carried out by and impact diverse areas of Terra State Community College.

Terra State Community College is committed to the ongoing protection of confidential financial information it collects from faculty, staff, students, alumni and others. GLBA and the updated Safeguards Rules are enforced by the Federal Trade Commission. A data security breach that results from non-compliance is a violation of federal law. Failure to protect customer information may result in financial loss for customers, fines imposed on the institution, as well as related reputational damage.

## Information Security Program

The GLBA establishes a Safeguards Rule that requires Terra State Community College to develop, implement, and maintain a comprehensive information security program with appropriate administrative, technical, and physical safeguards to protect customer information. This Information Security Program has five components:

1. Designating one employee responsible for coordinating the program

2. Conducting risk assessments to identify reasonably foreseeable security and privacy risks
3. Ensuring that safeguards are implemented to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored
4. Overseeing service providers
5. Maintaining and adjusting the Information Security Program periodically to include updates based on outcomes of investigations, incidents, and assessments

## Scope/Applicability

The Terra State Community College GLBA Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with handling, collecting, maintaining, processing, sharing, or transmitting covered data, and/or any other persons for, or on behalf of Terra State Community College. This includes transmission, storage, and/or processing of data, in any form (electronic or paper), for or on behalf of Terra State Community College.

## GLBA Compliance Program Coordinator

Terra State Community College's GLBA Compliance Coordinator (hereafter referred to as the Coordinator) will be responsible for implementing the Information Security Program.

The Coordinator will consult with responsible offices to identify units and areas of Terra State Community College with access to covered data. The Coordinator will conduct an audit, or utilize other reasonable measures, to confirm that all areas with covered information are included within the scope of this Information Security Program. The Coordinator will maintain a list of areas across the College with access to covered data.

The Coordinator will ensure that risk assessments and monitoring are carried out for each area that has covered data and that appropriate controls are in place for the identified risks. The Coordinator will work with responsible parties to ensure adequate training and education is developed and delivered for all employees and third-parties with access to covered data. The Coordinator will, in consultation with other College offices, verify that existing policies, standards and guidelines that provide for the security of covered data are reviewed and adequate. The Coordinator will make recommendations for revisions to policy, or the development of new policy, as appropriate.

The Coordinator will update the Information Security Program, including the GLBA Policy and related documents, at least annually to the Board of Trustees. The Coordinator will maintain a written security plan and make the plan available to the Terra State Community College community.

## Risk Assessment

The Information Security Program will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data 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.

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 covered data by employees, third-parties, or through requests
- Compromised system security as a result of criminal hacking or any unauthorized access
- Failure to properly protect passwords
- Interception of data during transmission
- Physical loss of data in a disaster
- Corruption of data or systems
- Paper forms containing covered data 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
- Errors introduced into the system by authorized or unauthorized persons

The Coordinator will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks, as well as risks unique to each area with covered data. The risk analysis methodology and approach will be conducted using guidelines in the NIST Special Publication 800-30 (Revision 1), Guide for Conducting Risk Assessments.

## Information Safeguards and Monitoring

The Information Security Program will verify that information safeguards are designed and implemented to control the risks identified in the risk assessments. The Information Security Program will create a comprehensive IT security framework, based on NIST 800-171.

The Coordinator will ensure that reasonable safeguards and monitoring are implemented and cover each area that has access to covered data. Such safeguards and monitoring will include the following:

**Employee Management and Training**

The Coordinator will, working with other responsible offices and units, identify those individuals and roles who have access to covered data, and advise them of their responsibilities to protect customer information and systems from compromise.

Comprehensive policies, programs, procedures, and recommendations for protecting covered data will be implemented. Training for all individuals with authorized access to covered data will include physical handling and disposal of non-electronic information, as well as procedures for processing and storing electronic information.

**Information Systems**

The Coordinator will maintain inventories of all computer systems accessing or controlling covered data. Information systems include network and software systems, as well as information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing role-based access through use of system IDs and passwords, regularly expiring and updating passwords, maintaining appropriate screening programs to detect criminal hackers and viruses, and implementing security patches within a defined time period.

Security Access will be designed to provide access only to those that are authorized and have a legitimate need for the data.

**Managing System Failures**

The College will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures.

Such systems may include maintaining and implementing current endpoint protection software, application of critical patches, appropriate filtering or firewall technologies, maintaining system logs, vulnerability scanning, alerting those with access to covered data of potential threats to security, shredding paper documents, backing up data regularly and storing back up information at a secondary site, as well as other reasonable measures to protect the integrity and safety of information systems.

**Monitoring and Testing**

Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards.

Monitoring will be conducted to ensure that safeguards are being followed, and to quickly detect and correct gaps 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.

**Identity Management**
The College will assign a unique account to each user that is granted access to the college systems. All user accounts will be unique and identifiable to an individual person or entity. Before any user is granted a system login ID and credentials, their identities must be validated based on procedures within the departments responsible; Enrollment Services for students, Human Resources for employees and patrons, and Information Technology for third party service providers.

The college assigned account with password is the default authentication factor for access to college systems. The Information Technology office will define and enforce minimum standards for password strength, lockout policy, and change interval for passwords. Multi-Factor authentication will be implemented for anyone accessing customer information on the systems. Any user may be required to re-validate their identity before recovering authentication credentials. Any exceptions or substitution of equivalent forms of access control must be approved in writing by the Coordinator.

Access to data and information on college systems will not be available to all system users. A system of role-based access will be implemented for any system that contains private or sensitive information. All role-based access must undergo periodic evaluation to re-evaluate current access needs and to adjust users as necessary. Procedures for access to systems must ensure termination of access for any user no longer affiliated with the college.

**Service Providers**
In the course of business, Terra State Community College may share covered data with third parties. Such activities may include collection activities, transmission of documents, transfer of funds, destruction of documents or equipment, or other similar services. Terra State Community College will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for protecting customer information. All third-party contracts must also incorporate specific language requiring that service providers implement and maintain such safeguards.

**Physical Security of Paper Records**
Only Terra State Community College employees who have a legitimate and valid reason to have covered data shall have access to 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.

**Information Disposal**
Terra State Community College should only keep physical paper records and electronic documents for as long as they are being actively used by the College, or as necessary to comply with retention requirements. Paper documents containing covered data will be shredded with a cross-cut shredder at the time of disposal. Electronic records will be deleted, and media will be erased and/or destroyed. Refer to Terra State Community College's Record Retention Policy.

**Incident Response**
It is the responsibility of all employees of Terra State Community College to promptly report any suspected compromise or confirmed breach of covered data. Please refer to the institution's Incident Response plan.

**Notification and Reporting**
Terra State Community College will follow the institution's Incident Response procedures for promptly notifying customers if their non-public personal information is compromised. The Coordinator will deliver an annual written report to the Board of Trustees. The report should contain an overall assessment of the College's compliance to the Information Security Program, information covering specifics topics under the scope of the Program and recommendations for changes to the program as appropriate.

## Program Maintenance

The Coordinator, working with responsible units and offices, will evaluate and adjust the Information Security Program based on the risk assessments, monitoring, and testing, as well as in response to any material changes to operations and any other circumstances which may reasonably have an impact on the Information Security Program.

## Non-Compliance

Any Terra State Community College employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination.

## *Procedures*

NA

## *Resources*

National Institute of Standards Technology Special Publication 800-171 (NIST 800-171)

NIST Special Publication 800-30 (Revision 1), Guide for Conducting Risk Assessments

Federal Trade Commission Gramm-Leach-Bliley Act

Standards for Safeguarding Customer Information (Final Rule)

Terra State Community College Records Retention Policy

## Documentation

## Definitions

| *Term* | **Definition** |
|---|---|
| *Customer* | Any individual who receives a financial service from Terra State Community College. Customers may include students, parents, spouses, faculty, staff, alumni, and third parties. |
| *Non-public personal information* | Any personally identifiable financial or other personal information, not otherwise publicly available, that Terra State Community College has obtained from a customer in the process of offering or providing a financial product or service; such information provided to the College by another financial institution; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include, but are not limited to:<br>▪ Names<br>▪ Addresses<br>▪ Telephone numbers<br>▪ Date of birth<br>▪ Bank and payment card numbers<br>▪ Income tax returns<br>▪ Paystubs<br>▪ Income and credit histories<br>▪ Social security numbers<br>▪ Health information |

| | |
|---|---|
| | ▪ Institution assigned ID numbers (Tnumber)<br>▪ State issued driver's license or identification number<br>▪ Government passport number<br>▪ Alien registration number |
| *Financial product or service* | Student loans, employee loans, activities related to extending credit, financial and investment advisory activities, management consulting and counseling activities, community development activities, and other miscellaneous financial services. |
| *Covered data and information* | Non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the College chooses as a matter of policy to also define covered data and information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers (SSNs) received in the course of business by the College, whether or not such financial information is covered by GLBA. As a general rule, Terra State Community College should avoid using Social Security numbers as a primary identification number. Covered data and information includes both paper and electronic records. |

## Contacts

| | **Department/Division** | **Email** | **Phone/Ext** |
|---|---|---|---|
| | IT | glbacoordinator@terra.edu | |

## *Approval History*

| *Date* | Policy/Procedure or Entire Document | Notes (Types of Actions) | **Approved by |
|---|---|---|---|
| 10/06/2023 | Policy | Issued | Wayne Yerdon, Chief Information Officer |
| | | | |
| | | | |

**Full name of CASA Committee Chair, signatory, or designee

**Effective Date: 10/06/2023**

**Next Review Date: 10/31/2026**