

Information Security Policy, 6.01
Chapter 6: Information Technology

Responsible Office: Information Technology**Applies to:** Faculty, Staff, Students, Vendors**BOT Approved:** 11/18/2025

Policy: In order to protect personal critical information and data, Rhodes State College will comply with the Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley (GLB) 15 U.S.C. §6801) and incorporate equitable access to resources and facilities.

I. Definitions

- a. **Covered Data and Information:** All student, employee, and financial data collected by the College, especially data that contains Personal Identifying Information (PII) and is individually identifiable.

II. Background

This policy defines the College's Information Security Program, outlining compliance with federal regulations related to security and integrating equitable access principles. It positions the College for ongoing and future privacy regulations while maintaining transparency for users of College resources.

III. Gramm Leach Bliley (GLB) Requirements

GLB mandates the appointment of an Information Security Plan Coordinator, risk assessments, employee training, oversight of service providers and contracts, and periodic evaluation of the Information Security Program.

IV. Information Security Plan Coordinator

The Information Technology Department Administrator serves as the Information Security Plan Coordinator, working with the Business Office, State of Ohio Attorney General's Office, Networking and Security Administrator, and other academic and administrative departments. Responsibilities include:

- Identifying risks to the security, confidentiality, and integrity of information.
- Evaluating safeguards.
- Designing and monitoring the safeguards program.
- Conducting regular policy reviews.

V. Compliance and User Accountability

To ensure adherence to this policy and maintain a secure and equitable technology environment, the following measures are mandatory:

1. **Equitable Access:** All faculty, staff, students, vendors, and other authorized users must have fair and need-based access to computing resources. Authorization for access will be strictly managed by designated personnel based on clear, documented protocols.

2. **User Accountability:** Unauthorized activities, such as accessing restricted data, interfering with network operations, or misusing College resources, are strictly prohibited. All incidents of non-compliance must be reported to the Information Technology Department Help Desk immediately. Investigations will be conducted to determine the severity of the violation. Disciplinary actions, including user restrictions, retraining, or termination, will follow the guidelines in Policy 5.5. All violations will be documented.
3. **Privacy Disclaimers:** Users must acknowledge that no privacy is implied or guaranteed for activities conducted on College systems. This disclaimer will be communicated during onboarding, through training sessions, and via acknowledgment forms. Exceptions to this rule, such as privileged communications protected under applicable laws, will be addressed on a case-by-case basis.
4. **Periodic Reviews:** Compliance with the Federal NIST Computer Security Resource Center guidelines and internal policies will be reviewed biannually. Departments must collaborate with the Information Security Coordinator to ensure ongoing adherence to established safeguards.

Related Policies or Procedures:

[Information Security Procedure 6.01\(a\)](#)
NIST Requirements Handbook

Compliance References:

The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley (GLB)
15 U.S.C. §6801

History:

	Date:	Reason:
Issued:	11/15/2022	Original policy was reviewed and approved by Board of Trustees
Revised:	11/18/2025	Updated Section V - Compliance and User Accountability for included coverage and to allow for retirement of outdated Computer Resources & Facilities policy 6.14.

This policy and / or procedure provides operating principles for Information Technology Security and compliance with GLBA and other security standards at Rhodes State College. It supersedes any prior policy covering this specific subject. This policy and/or procedure may be suspended, modified, or cancelled as determined by the College. This policy and/or procedure does not create a contract of employment, nor is it a condition of employment between the College and its employees.