

Information Security Policy, 6.01
Chapter 6: Information Technology

Responsible Office: Information Technology**Applies to:** Faculty, Staff, Students, Vendors**BOT Approved:** 11/15/2022

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.

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

While these practices mostly affect IT, some of them will impact diverse areas of the College, including but not limited to Business Services, Student Services, the Office of the Registrar, and many third-party contractors, facilities and building service providers. The goal of this document is to define the College's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the College for likely future privacy and security regulations.

III. Gramm Leach Bliley (GLB) Requirements

GLB mandates that the College appoint an Information Security Plan Coordinator, 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 Information Security Program periodically.

IV. Information Security Plan Coordinator

In order to comply with GLB, IT has designated an Information Security Policy Coordinator. This individual must work closely with the Business Office, the State of Ohio AG, the Networking and Security Administrator in Information Technology, other positions in Information Technology and Information Systems and Services, as well as all relevant academic and administrative Departments throughout the College. The Coordinator is presently the Director of Information Technology.

The Coordinator must help the relevant offices of the College identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program.

V. Compliance

In order to maintain compliance with the Federal NIST Computer Security Resource center see NIST Requirements Handbook.

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:	MM/DD/YY	

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.