



Policy and Procedures on Safeguarding Customer Information under GLBA

Author	Compliance Program Manager; IT Director
Policy Title	Policy and Procedures on Safeguarding Customer Information under GLBA
Policy Purpose	Safeguarding Customer Information
Policy Effective Date	January 1, 2025
Area Information is located	
Responsible Office	The following departments have GLBA responsibilities for customer information: All units with access to customer information, including but not limited to: Admissions; Information Technology; Registrar's Office, Finance; and Advancement.
Related Policies	GDPR Privacy Notice; Data Governance Policy and Plan
History	
Date Document was last updated	December 10, 2024

I. *Policy Statement:* The Gramm-Leach Bliley Act ("[GLBA](#)") and the Title IV of the Higher Education Act of 1965 require institutions of higher education, as financial institutions, to take steps to safeguard customers' nonpublic personal information.

II. *Purpose:* Principia College, as an Institution of higher education, is required to comply with the Federal Trade Commission Standards for Safeguarding Customer Information (Safeguards Rule) as outlined in 16 C.F.R. Part 314. These requirements are additional to those of the Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation and are required under 34 CFR 668.14(c)(2)(i).

III. *Definitions/ Acronyms:*

Customer Information: The customer information nonpublic personal information protected in the GLBA is typically gathered while obtaining a financial product or service. This information obtained by Principia as a result of providing financial services such as Title IV programs; making institutional loans or scholarships. Customer information is limited to financial information connected to student and parent finances such as student and parent loans, bank account information and income tax information for financial aid packages. It may include, but is not

limited to:

- Address and phone number
- Bank account numbers
- Credit card numbers
- Credit history
- Income history
- Social Security numbers

Data Custodians: Any department or unit with critical tasks of storing, managing and/or securing customer information for The Principia.

GDPR: General Data Protection Regulation

GLBA: Gramm-Leach Bliley Act

ITSD: Technology Security Director

IV. Procedure

The GLBA Safeguards Rule mandates that an institution of higher education's GLBA written information security program includes the elements outlined in this procedure:

Element 1: Designates a qualified individual responsible for overseeing and implementing the institution's or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a))

Principia's Information Technology Security Director ("ITSD") is responsible for this GLBA procedure and is designated as the Qualified Individual for The Principia Corporation.

Element 2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to the institution or servicer) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 C.F.R. 314.4(b)).

The designated units and the ITSD work together to identify and assess risks to customer information including but not limited to:

- Unauthorized access to customer information;
- Compromised system security as a result of system access by an unauthorized person;
- Interception of customer information during transmission;
- Loss of data integrity;
- Physical loss of customer information in a disaster;
- Errors introduced into the system;
- Corruption of data or systems;
- Unauthorized requests for customer information;
- Unauthorized access to hard copy files or reports containing customer information;
- Unauthorized transfer or release of customer information by third parties contracted by Principia;
- Unauthorized disposal of customer information; and
- Unsecured disposal of customer information.

Principia recognizes that the above list of risks may not be a complete list of risks associated with the protection of customer information. Since technology changes over time, the possibility of new risks may arise. The data custodians will seek to identify and address technology security risks

associated with customer information. Additionally, the IT Department shall incorporate continuous monitoring and identification of security risks and controls into its regular internal control review process.

Element 3: Provides for the design and implementation of safeguards to control the risks the institution or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8).

The minimum safeguards that Principia will implement and maintain to protect customer information include:

- Encryption: Implementation of strong encryption protocols to protect customer information in servers. VPN (Virtual Private Network) is used to encrypt off campus remote employees access to data.
- Access Controls: Maintain the multi-factor authentication approved by the ITSD for information systems where customer information is held. Ensure that access to sensitive information is restricted to authorized personnel only. Implement and periodically review access controls, including technical and as appropriate, physical controls to authenticate authorized users and limit users' access only to customer information needed to perform duties or functions.
- Incident Response: Develop and execute a robust incident response plan to address potential data breaches or security incidents. Principia will follow the corresponding review process to recover any potential loss of information.
- Regular Audits: Conduct annual internal and external audits to identify vulnerabilities and ensure compliance with GLBA. Monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information.
- Require all in-house and external developed applications used by units subject to GLBA to ensure customer information is collected, stored, used and known, and secured in approved ways;
- Follow ITSD approved secure disposal procedures for any system with customer information or retain records in accordance with state and federal laws. Remove all information from hard drives before recycling or selling hardware.

Element 4: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

The ITSD will follow regular procedures to test the technical safeguards for GLB customer information. For example, security exercises where a cyber security expert attempts to find and expose vulnerabilities -penetration testing- to Principia's system are executed once a year.

Element 5: Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 C.F.R. 314.4(e)).

Both the Policy on Safeguarding Customer Information under GLBA and the GDPR are associated with Principia's commitment to information security and customer data integrity. Data custodians are responsible for facilitating and enforcing compliance with all information security policies and practices applicable to their unit/department.

The IT department is responsible for ensuring employees are properly trained as an essential component of a collaborative effort to safeguard customer information.

Element 6: Addresses how the institution or servicer will oversee its information system service providers (16 C.F.R. 314.4(f)).

Principia will take reasonable steps to select and retain service providers who maintain appropriate safeguards for customer information.

Element 7: Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the information security program (16 C.F.R. 314.4(g)).

The GLBA Information Security Procedure will follow the requirements of this document with respect to evaluation of the information security program, periodic updates, and improvements.

Element 8: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the establishment of an incident response plan (16 C.F.R. 314.4(h)).

The Principia's Continuity of Operations Plan includes a written incident response plan to respond to a data security incident. The IT Team is responsible for conducting response operations to a breach of IT systems or an unauthorized release data. The team is comprised of IT professionals, Head of School or President, the CFO/COO, CE and others as needed to resolve the incident. A security breach must be reported within 24 hours to the US Department of Education.

Element 9: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the requirement for its Qualified Individual to report regularly and at least annually to those with control over the institution on the institution's information security program (16 C.F.R. 314.4(i)).

The ITSD will collaborate with other Principia officers to submit a report on the overall status of Principia information security program to the Leadership group and/or Principia's Board of Trustees annually on the current security program.

Note: Principia's policy has been adapted from [Illinois State University's Policies and Procedures](#)

Other Resources

<https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

<https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements>

<https://privacy.gwu.edu/glba>



PRINCIPIA COLLEGE

One Maybeck Place
Elsah, IL 62028

618.374.2131
www.principiacollege.edu

Policy Approval & Executive Summary

Author:	Compliance Program Manager; IT Director
Policy Title	Policy and Procedures on Safeguarding Customer Information under GLBA
Policy Location (URL)	
Policy Effective Date	01/01/2025
Responsible Office	The following departments have GLBA responsibilities for customer information: All units with access to customer information, including but not limited to: Admissions; Information Technology; Registrar's Office, Finance; and Advancement.
Related Policies	GDPR Privacy Notice; Data Governance Policy and Plan
History	
Executive Summary	The Gramm-Leach Bliley Act (" <u>GLBA</u> ") and the Title IV of the Higher Education Act of 1965 require institutions of higher education, as financial institutions, to take steps to safeguard customers' nonpublic personal information. Principia College, as an Institution of higher education, is required to comply with the Federal Trade Commission Standards for Safeguarding Customer Information (Safeguards Rule) as outlined in 16 C.F.R. Part 314 (GLBA). These requirements are additional to those of the Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation and are required under 34 CFR 668.14(c)(2)(i).

With my signature, I acknowledge and accept the creation and/or revision of the attached policy.

Required Signatures:

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Jim Huddleston
Director of Information Technology
Signature

Jim Huddleston 04/03/2025
Printed Name, Date



PRINCIPIA COLLEGE

One Maybeck Place
Elsah, IL 62028

618.374.2131
www.principiacollege.edu

Policy Approval & Executive Summary

Author:	Compliance Program Manager; IT Director
Policy Title	Policy and Procedures on Safeguarding Customer Information under GLBA
Policy Location (URL)	
Policy Effective Date	01/01/2025
Responsible Office	The following departments have GLBA responsibilities for customer information: All units with access to customer information, including but not limited to: Admissions; Information Technology; Registrar's Office, Finance; and Advancement.
Related Policies	GDPR Privacy Notice; Data Governance Policy and Plan
History	
Executive Summary	The Gramm-Leach Bliley Act ("GLBA") and the Title IV of the Higher Education Act of 1965 require institutions of higher education, as financial institutions, to take steps to safeguard customers' nonpublic personal information. Principia College, as an Institution of higher education, is required to comply with the Federal Trade Commission Standards for Safeguarding Customer Information (Safeguards Rule) as outlined in 16 C.F.R. Part 314 (GLBA). These requirements are additional to those of the Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation and are required under 34 CFR 668.14(c)(2)(i).

With my signature, I acknowledge and accept the creation and/or revision of the attached policy.

Required Signatures:

Tom Nickell

Tom Nickell, CFO 06/19/2025

Printed Name, Title

Printed Name, Date

Director of Information Technology Signature

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Printed Name, Title

Printed Name, Date

Principia College Policy Approval GLBA_Fillable_unsigned

Final Audit Report

2025-06-19

Created:	2025-06-19
By:	Gloria Burgert (gloria.burgert@principia.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAAKcJdVkCMBpQ_I-Yyp-U4EaXkKwQkA6Qc

"Principia College Policy Approval GLBA_Fillable_unsigned" History

-  Document created by Gloria Burgert (gloria.burgert@principia.edu)
2025-06-19 - 6:16:38 PM GMT
-  Document emailed to Tom Nickell (tom.nickell@principia.edu) for signature
2025-06-19 - 6:17:21 PM GMT
-  Email viewed by Tom Nickell (tom.nickell@principia.edu)
2025-06-19 - 6:21:46 PM GMT
-  Document e-signed by Tom Nickell (tom.nickell@principia.edu)
Signature Date: 2025-06-19 - 6:23:05 PM GMT - Time Source: server
-  Agreement completed.
2025-06-19 - 6:23:05 PM GMT



Adobe Acrobat Sign