GreyCastle SECURITY

Gramm-Leach-Bliley Act Amendments

GLBA

The Federal Trade Commission (FTC) issued final regulations to amend the Standards for Safeguarding Customer Information, a component of the GLBA. This guide will help you achieve compliance by the Department of Education's June 9th, 2023 enforcement date.

The High Level:

You must have a written information security program appropriate to the size and complexity of your institution, the nature and scope of your activities, and the sensitivity of the information at issue (e.g. student financial records).

The Details:

Nine required elements of your institution's information security program require specific components to be included. GLBA requires you to apply these requirements to how you collect, store, and use student financial records.

Required Elements to Include in Your Information Security Program

Designate a qualified individual (can be an employee or service provider) to implement and supervise your information security program.

Regularly monitor and test the effectiveness of your safeguards.

- Accomplished through continuous monitoring of information systems OR must conduct annual Penetration Testing as well as Vulnerability Assessments every six (6) months.

Monitor your service providers.

- Contracts must include security expectations, and you must monitor and periodically reassess third parties' security.

Keep your information security program current.

Conduct a risk assessment.

Step 1:
Log inventory on what student record information you have and where it is currently stored.

Step 2:
Assess your risks based on the inventory you were able to come up with and put it in writing.

Step 3:
Assessments should be reoccurring in line with changes to the institution or threat landscape.

Design and implement safeguards to control the risks identified in your risk assessment.

1: Implement and periodically review access controls, evaluating who has access to your student financial records, and is there a legitimate reason for that access.

2: Know what you have and where you have it (same as Step 2 under Risk Assessment) and maintain that information inventory to ensure safeguards are applied appropriately on an ongoing basis.

3: Encrypt student financial information on your system and when it's in transit.

4: Assess your apps (and your third-party apps) and implement procedures for evaluating the security of apps that store, access, or transmit student financial information.

5: Implement multi-factor authentication for anyone accessing student financial information on your system.

6: Dispose of student financial information securely no later than two years following the most recent use to service that student.

7: Anticipate and evaluate changes to your information system or network. Build change management into your information security program to ensure visibility into new additions or changes to your system or network.

8: Maintain a log of authorized user activity and review for unauthorized access.

Train your staff.

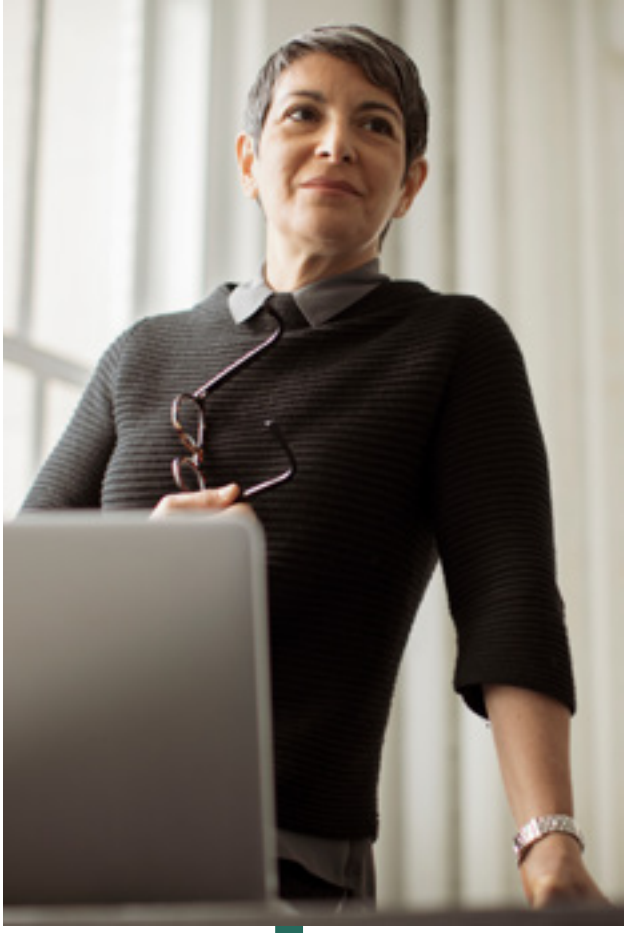
- Provide security awareness training for employees **and** specialized training for those with information security responsibilities to ensure awareness of emerging threats.

Require your qualified individual to report to your board of trustees.

- Provide a report in writing at least annually, including an overall assessment of your institution's compliance with your information security program, as well as specific topics, including risk assessment, risk management and control decisions, service provider arrangements, test results, security events, response overview, and recommendation for changes to the information security program.

Create a written incident response plan.

- Written plan must include your goals, internal processes to a security event, roles, responsibilities, levels of decision-making authority, communication, information sharing guidelines internal and external to your institution, a process to fix any identified system and control weaknesses, procedures for documenting and reporting security events and response, and a postmortem that includes updating your plan.



CMMI
Maturity Levels

Refer to this chart for the table on the next page.

Maturity Level 0: Incomplete
Ad hoc and unknown. Work may or may not get completed.

Maturity Level 1: Initial
Unpredictable and reactive. Work gets completed but is often delayed and over budget.

Maturity Level 2: Managed
Managed on the project level. Projects are planned, performed, measured and controlled.

Maturity Level 3: Defined
Proactive rather than reactive. Organization-wide standards provide guidance across projects, programs and portfolios.

Maturity Level 4: Quantitatively Managed
Measured and controlled. Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.

Maturity Level 5: Optimizing
Stable and flexible. Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.

source: *(ISACA, 2023) Federal Trade Commission, 2022*

Higher Education GLBA Cybersecurity Readiness Checklist

refer to CMMI maturity levels chart***

Requirements	CMMI Rating
Designate a Qualified Individual	– Choose Rating –
Inventory your Student Financial Records	– Choose Rating –
Conduct a Risk Assessment	– Choose Rating –
Implement Access Control Procedures	– Choose Rating –
Encrypt Student Financial Records at Rest and in Transit	– Choose Rating –
Assess Security of Apps Storing, Accessing or Transmitting Student Financial Records	– Choose Rating –
Implement Multi-Factor Authentication for Anyone Accessing Student Financial Records	– Choose Rating –
Dispose of Student Financial Records by Two (2) Years Following the Last Need to Use	– Choose Rating –
Implement Ongoing Change Management of Information System or Network	– Choose Rating –
Log Authorized User Activity	– Choose Rating –
Continuous Monitoring of Information Systems (OR the following two) - Annual Penetration Testing (& the following) - Every Six (6) Month Vulnerability Assessment	– Choose Rating –
Employee Awareness Training	– Choose Rating –
Information Security Training for Applicable Resources	– Choose Rating –
Include Security Expectations in Third-Party Contracts	– Choose Rating –
Create a Written Incident Response Plan	– Choose Rating –
Written Report to Board of Trustees	– Choose Rating –
Implement Recurring Risk Assessment	– Choose Rating –
Implement Ongoing Student Financial Information Inventory Update	– Choose Rating –
Implement Ongoing Access Control Review	– Choose Rating –
Implement Ongoing Disposal of Student Financials Records before Two Years of their Last Use	– Choose Rating –
Implement and Monitor Ongoing Authorized User Activity and Unauthorized Access	– Choose Rating –
If Continuous Monitoring Not Implemented, Implement Annual Penetration Testing	– Choose Rating –
If Continuous Monitoring Not Implemented, Implement Six (6) Month Vulnerability Assessment	– Choose Rating –
Implement Ongoing Employee Awareness Training	– Choose Rating –
Implement Ongoing Security Training for Applicable Resources	– Choose Rating –
Implement Monitoring and Periodic Assessment of Third-Party Security Expectations	– Choose Rating –
Follow through of all Components of Incident Response Plan for any Security Events	– Choose Rating –
Implement Minimum of Annual Written Report to Board of Trustees	– Choose Rating –