Gramm-Leach-Bliley Act Amendments

GLBA Readiness for Higher Education

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 required by the Department of Education.

The High Level:

Always make sure to write out and keep your information security program documented. It must be appropriate to the size and complexity of your institution, the nature and scope of your activities, and the sensitivity of student financial records.

The Details

Nine (9) 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

1 Designate a qualified individual, an employee or service provider, to implement and supervise your information security program.

2 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.

3 Monitor your service providers contracts that should include security expectations and periodically reassess third-party security.

4 Keep your information security program current.

5 Conduct a risk assessment.
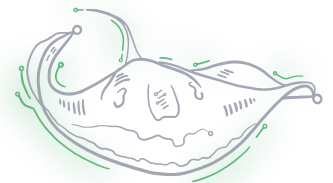
Step 1:

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.

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

1. Implement and periodically review access controls. 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 access.

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

4. Assess your apps (and your third-party apps). 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 your most recent use of it 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.

7 **Train your staff.**

🖊 Teach security awareness training for employees AND specialize training for those with information security responsibilities to ensure awareness of emerging threats.

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

🖊 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, and response overview, and recommendation for changes to the information security program.

9 **Create a written incident response plan.**

🖊 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.

Higher Education GLBA Cybersecurity Readiness Checklist

Requirements	CMMI Rating
Designate a Qualified Individual	
Inventory you Student Financial Records	
Conduct a Risk Assessment	
Implement Access Control Procedures	
Encrypt Student Financial Records at Rest and in Transit	
Assess Security of Apps Storing, Accessing or Transmitting Student Financial Records	
Implement Multi-Factor Authentication for Anyone Accessing Student Financial Records	
Dispose of Student Financial Records by Two (2) Years Following the Last Need to Use	
Implement Ongoing Change Management of Information System or Network	
Log Authorized User Activity	

Continuous Monitoring of Information Systems (OR the following two)
  - Annual Penetration Testing (& the following)
  - Every Six (6) Month Vulnerability Assessment	

Employee Awareness Training	
Information Security Training for Applicable Resources	
Include Security Expectations in Third-Party Contracts	
Create a Written Incident Response Plan	
Written Report to Board of Trustees	
Implement Recurring Risk Assessment	
Implement Ongoing Student Financial Information Inventory Update	
Implement Ongoing Access Control Review	
Implement Ongoing Disposal of Student Financials Records before Two Years of their Last Use	
Implement and Monitor Ongoing Authorized User Activity and Unauthorized Access	
If Continuous Monitoring Not Implemented, Implement Annual Penetration Testing	
If Continuous Monitoring Not Implemented, Implement Six (6) Month Vulnerability Assessment	
Implement Ongoing Employee Awareness Training	
Implement Ongoing Security Training for Applicable Resources	
Implement Monitoring and Periodic Assessment of Third-Party Security Expectations	
Follow through of all Components of Incident Response Plan for any Security Events	
Implement Minimum of Annual Written Report to Board of Trustees	