# Higher Education GLBA Checklist

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 required by the Department of Education.

### The High Level:

Always 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 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 for your Information Security Program

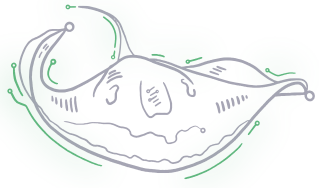
1. **Designate a qualified individual, an employee or service provider, to implement and supervise your information security program.**

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 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 and document them.

**Step 3:**

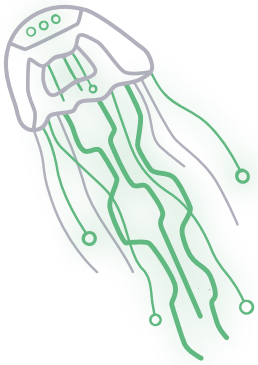
Assessments should reoccur in line with changes to the institution or threat landscape.

## 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. Information should be disposed of no later than two years following your 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.

## 7 Train your staff.

- Provide security awareness training for employees, including specialized 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.

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

## 9 Create a written incident response plan.

- Include:
  - Goals
  - Information sharing guidelines internal and external to your institution
  - Roles
  - Responsibilities
  - Levels of decision-making authority
  - Communication
  - Internal processes to a security event
  - A process to fix any identified system and control weaknesses
  - Procedures for documenting and reporting security events and response
  - 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

*refer to CMMI maturity levels chart

| Requirements | CMMI Rating* |
|---|---|
| Designate a qualified individual. | |
| Inventory your student financial records. | |
| Conduct a risk assessment. | |
| Implement access control procedures. | |
| Encrypt student financial records at rest and in transit. | |
| Assess the security of your 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 years following the last need to use. | |
| Implement ongoing change management of information system or network. | |
| Log authorized user activity. | |
| Conduct continuous monitoring of information systems or complete annual penetration testing along with a vulnerability assessment every six months. | |
| Conduct employee awareness training. | |
| Conduct information security training for applicable resources. | |
| Include security expectations in third-party contracts. | |
| Create a written incident response plan. | |
| Create a written report for the Board of Trustees. | |
| Implement a recurring risk assessment. | |
| Implement an ongoing student financial information inventory update. | |
| Implement an 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 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. | |