GreyCastle SECURITY

Gramm-Leach-Bliley Act Amendments

GLBA

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, many require specific components to be included.

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*

GreyCastle SECURITY

greycastlesecurity.com
sales@greycastlesecurity.com

@greycastlesec

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

Higher Education GLBA Cybersecurity Readiness Checklist

Refer to CMMI maturity levels chart on previous page for definitions of each rating.

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 - 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 Financial 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 –