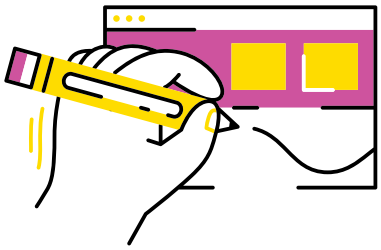
Updated GLBA Safeguards Rule

Although organizations still have the flexibility to design their information security programs with relation to the size/complexity of their institutions and the sensitivity of the customer information, the more prescriptive requirements of the updated Safeguards Rule may have an impact on programs that had been previously considered compliant. Updates to the Safeguards Rule include:

Written Information Security Program

A comprehensive, written program that includes administrative, technical, and physical safeguards as appropriate to the institution's size and complexity, and the sensitivity of the customer information being handled.

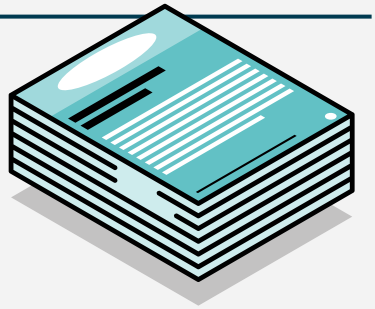


Designation of a Qualified Individual

An individual appointed to oversee, implement, and enforce the information security program.

Written Reports to the Board of Directors

At least annually, the Qualified Individual must create a written report outlining the overall status of the information security program and submit it to the board of directors.



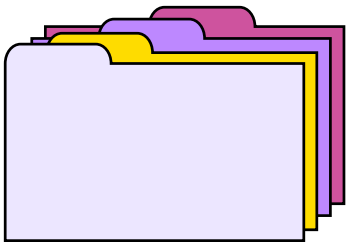
Periodic Risk Assessments

Requirements for performing documented risk assessments, evaluating and categorizing security risks and threats, assessing the confidentiality, integrity, and availability of the institution's information systems and customer information, and requirements for mitigating or accepting identified risks.

CAMPUSGUARD®

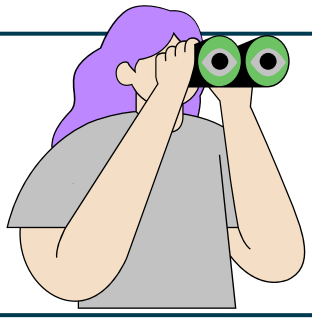
Data Inventorying and Classification

Identify and manage customer data and identify all systems on which that data is collected, stored, or transmitted.



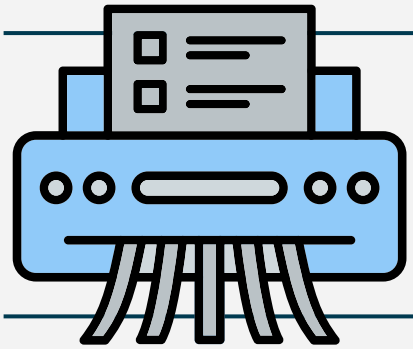
Access/Authentication Controls

Implement, and periodically review, access and authentication controls to limit access by unauthorized individuals and prevent unauthorized access.



System Monitoring

Procedures to monitor and log the activity of authorized users and detect unauthorized access or use of customer information.

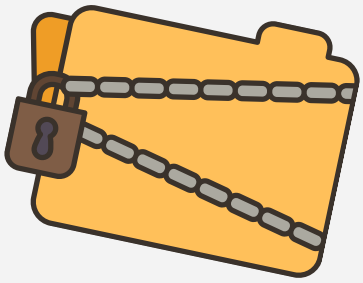


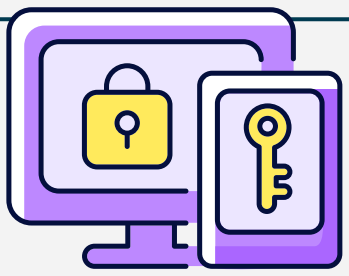
Data Retention and Disposal

Secure disposal of customer information no later than 2 years after the last date of use unless retention is necessary for a legitimate business purpose.

Encryption of Customer Information at Rest and in Transit

Organizations can still adopt effective compensating controls if they are unable to implement encryption that can sufficiently prevent the deciphering of information in most circumstances.

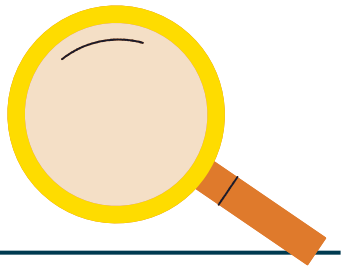




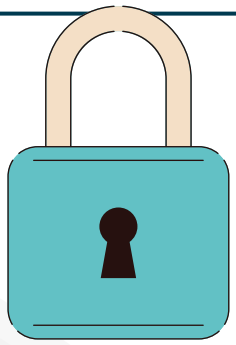
Multifactor Authentication

MFA must be implemented for any individual accessing systems that contain customer information, for both internal and external users accessing the system.

Penetration Testing and Vulnerability Scanning



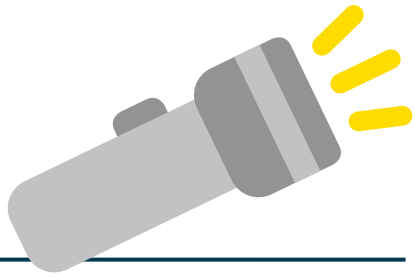
Requirements to perform annual penetration testing and bi-annual vulnerability scanning for those systems that contain customer information or are connected to systems that contain customer information.



Secure Development Practices

Adopt secure development practices for in-house developed applications used for transmitting, accessing, or storing customer information, and implement requirements for evaluating and testing the security of externally developed applications when third-party applications are used to handle customer information.

Change Management Procedures



Requirement to develop procedures to assess the security of devices, networks or other systems added to the environment, or the effect of removing such items or otherwise modifying the information systems.

Incident Response Plan (IRP)

Development of a written IRP that addresses internal response processes, clearly defined roles and responsibilities, as well as decision making authority, external and internal communications, and the evaluation and revision of the IRP following a security event, and specifically called out ransomware attacks.

Employee Training

Provide personnel with security awareness training that has been updated to reflect the evolving risks identified by the risk assessment.

Vendor Management

Institutions must take "reasonable" steps to ensure vendors maintain proper safeguards: have appropriate contract language in place to ensure all third-party service providers have instituted such safeguards, and periodically evaluate selected providers on the adequacy of their safeguards based on perceived risk.

Reach out to CampusGuard to assist with your GLBA Compliance Program.

www.campusguard.com/glba

CAMPUSGUARD®