New Boundary Technologies®
Financial Modernization Act of 1999
(Gramm-Leach-Bliley Act)
Compliance Checklist

GLBA Security Checklist

This GLBA Security Checklist was developed by New Boundary Technologies as a resource for security officers and network administrators charged with meeting the *Standards for Safeguarding Customer Information of the Financial Modernization Act of 1999* or *Gramm-Leach-Bliley Act.*

The checklist is a good starting point to ensure you are asking the right questions within your organization to aid you in the development and implementation of a GLBA Information Security Program.

GLBA Objective	GLBA Elements	Status
Administrative Safeguards		
Objective 501(b)(1)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
	Has a Risk Analysis been completed in accordance with NIST Guidelines?	
	Has the Risk Management process been completed in accordance with NIST Guidelines?	
	Do you have formal sanctions against employees who fail to comply with security policies and procedures?	
	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking?	
	Have you identified the security official who is responsible for the development and implementation of the policies and procedures?	
	Have you published and implement policies and procedures to ensure that all members of your workforce have appropriate access to protected customer information and to prevent those workforce members who do not have access from obtaining access to customer information?	
	Do you check the references and/or conduct background checks on potential employees?	
	Have you implemented procedures for the authorization and/or supervision of employees who work with customer information or in locations where it might be accessed?	

	How do you ensure that employees are knowledgeable about applicable policies and expectations?	
	Have you implemented procedures to determine the access of an employee to customer information is appropriate?	
	Have you implemented procedures for terminating access to customer information when an employee leaves your organization?	
Objective 501(b)(3)	**Information Access Management: Implement policies and procedures for authorizing access to protected customer information.**	
	If you are a service provider that is part of a larger organization, have you implemented policies and procedures to protect customer information from the larger organization?	
	Have you implemented policies and procedures for granting access to customer information, for example, through access to a workstation, transaction, program, or process?	
	Have you implemented policies and procedures that are based upon your access authorization policies that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process?	
	Do those policies limit access to customer information to employees who have a business need or when it is required to conduct departmental activities?	
Objective 501(b)(3)	**Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).**	
	Do you provide periodic information security reminders?	
	Do you have a published GLBA Security Manual? Print or on the company network?	
	Do you conduct scheduled and unscheduled training with employees on your security policies?	
	Are the policies in your manual, which apply to an employees' workstation security, actually installed and automatically enforced on that workstation?	
	Do you have specific policies, procedures and tools for guarding against, detecting, and reporting malicious software?	

	Are the IT personnel trained and proficient in the use of the security solutions used to protect against malicious software?	
	Are end users aware of the security policies being enforced on their workstations?	
	Do you have procedures for monitoring log-in attempts and reporting discrepancies?	
	Do you have procedures for creating, changing, and safeguarding passwords?	
	Do they use password activated screensavers?	
	Do your employees' know to use strong passwords(combination of alphanumeric and letters)?	
Objective 501(b)(3)	**Security Incident Procedures: Implement policies and procedures to address security incidents.**	
	Do you have procedures to identify and respond to suspected or known security incidents; to mitigate them to the extent practicable, measure harmful effects of known security incidents; and document incidents and their outcomes?	
Objective 501(b)(2)	**Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain protected customer information.**	
	Have you established and implemented procedures to create and maintain retrievable exact copies of customer information?	
	Have you established (and implemented as needed) procedures to restore any loss of customer information data stored electronically?	
	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of customer information while operating in the emergency mode?	
	Have you implemented procedures for periodic testing and revision of contingency plans?	
	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components?	

Objective 501(b)(1)	**Evaluation: Have you established a plan for periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of customer information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart?**	
Objective 501(b)(3)	**Service Provider Arrangements: A covered entity may permit a service provider to create, receive, maintain, or transmit customer information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the service provider will appropriately safeguard the information.**	
	Have you established written contracts or other arrangements with your service providers that document satisfactory assurances that meets the applicable security requirements you have established?	

GLBA Objective	GLBA Elements	Status
Physical Safeguards		
Objective 501(b)(2)	**Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**	
	Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan?	
	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft?	
	Do you lock rooms and file cabinets where customer information is kept?	
	Have you implemented procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision?	

	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks)?	
	Have you implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access customer information?	
	Have you implemented physical safeguards for all workstations that access customer information to restrict access to authorized users?	
	Device and Media Controls: Have you implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected customer information into and out of a facility, and the movement of those items within the facility?	
	Have you implemented policies and procedures to address final disposition of customer information, and/or hardware or electronic media on which it is stored?	
	Have you implemented procedures for removal of customer information from electronic media before the media are available for reuse?	
	Have you considered the threat from removable USB storage devices and do you have a policy that addresses their use within the network and on end user workstations?	
	Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement?	
	Do you create a retrievable, exact copy of customer information, when needed, before moving equipment?	

GLBA Objective	GLBA Elements	Status
Technical Safeguards		
Objective 501(b)(3)	**Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected customer information to allow access only to those persons or software programs that have been granted access rights.**	
	Do you centrally manage all of your security tools and do you keep employees informed of security risks and breaches?	
	Have you established a written contingency plan to address breaches of safeguards?	
	Have you assigned a unique name and/or number for identifying and tracking user identity?	
	Have you established (and implemented as needed) procedures for obtaining necessary customer information during an emergency?	
	Have you implemented automated procedures that terminate an electronic session after a predetermined time of inactivity?	
	Do you store electronic customer information on a secure server that is accessible only with a password and is in a physically-secure area	
	Have you implemented a mechanism to encrypt and decrypt customer information?	
	Do you avoid storage of customer information on machines with an Internet connection?	
	Do you have the ability to prevent access to files/folders on workstations and servers from unauthorized users?	
	Have you implemented audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use customer information?	
	Have you implement policies and procedures to protect electronic protected customer information from improper alteration or destruction?	

	Have you implemented electronic mechanisms to corroborate that customer information has not been altered or destroyed in an unauthorized manner?	
	Have you implemented person or entity authentication procedures to verify a person or entity seeking to access customer information is the one claimed?	
	Are you using anti-virus software that updates automatically?	
	Do you regularly scan, obtain and install patches that resolve software vulnerabilities?	
	Do you apply industry standard security configuration policies (Microsoft, NSA, NIST) that will “lock down” those computer systems and servers handling customer information?	
	Do you maintain up-to-date firewalls (perimeter and host based), particularly if you use broadband Internet access or allow staff to connect to the network from home?	
	Have you developed and do you automatically enforce remote network access security policies on staff that connects to the network from home or remote locations?	
	Do you have procedures and controls to maintain a secure backup of media and to secure archived data?	
	Have you implement technical security measures to guard against unauthorized access to electronic protected customer information that is being transmitted over an electronic communications network.	
	Have you implemented security measures to ensure electronically transmitted customer information is not improperly modified without detection until disposed of?	
	Have you implemented a mechanism to encrypt customer information whenever deemed appropriate?	