New Boundary Technologies®
Financial Modernization Act of 1999
(Gramm-Leach-Bliley Act)
Security Guide

A New Boundary Technologies
GLBA Security Configuration Guide
Based on NIST Special Publication 800-68

CONTENTS

1.0 Executive Summary

This GLBA Security Guide was developed by New Boundary Technologies to provide insight and recommended computer security configurations for security officers and network administrators charged with meeting the *Standards for Safeguarding Customer Information of the Financial Modernization Act of 1999* (aka *the Gramm-Leach-Bliley Act or GLBA*).

The Financial Modernization Act, better known as the Gramm-Leach-Bliley Act (GLBA), became law in 1999 and is designed to protect consumers' personal financial information held by financial institutions. The Act not only applies to banks, but to securities firms, insurance companies, and also to financial institutions such as credit reporting agencies that receive customer information from other financial institutions.

There are three principal parts to the privacy requirements: the Financial Privacy Rule, Pretexting provisions, and the Safeguards Rule. The Financial Privacy Rule seeks the protection of customers' personal financial information by financial institutions, while the pretexting provision seeks to protect consumers from individuals and companies obtaining personal financial information under false pretenses.

The key part for network administrators to focus on is the Safeguards Rule, which requires all financial institutions to design, implement and maintain safeguards to protect customer information. What is key to understand with all the regulatory compliance legislation imposed on the industry is that to truly meet the requirements one must not only show proof of the presence of controls that are regulated (usually through auditing and reporting), but you also need to show auditors the actual presence of the controls that are mandated.

To assist companies with meeting the GLBA requirements, the Federal Trade Commission has published a Safeguards Rule that is applicable for all financial institutions that need to comply with GLBA. The Safeguards Rule requires financial institutions to develop a written Information Security Program that describes their methodology to protect customer information. *The development and implementation of an Information Security Program is the key to complying with GLBA.*

A critical part of any GLBA Information Security Program is the development of a security configuration baseline that will "lock down" computer systems handling customer information. To ensure our customers are provided with proven security configuration policies and guidance, this guide is based on the Specialized Security-Limited Functionality recommendations from the National Institute of Standards and Technology (NIST) Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.* The complete version of 800-68 is available from NIST at: http://csrc.nist.gov/

Additional information and resources on GLBA are available in our GLBA Resource Guide available at http://www.newboundary.com/solutions/glba_form.htm.
When an IT security configuration template (e.g., hardening or lockdown guide) is applied to a system, in combination with trained system administrators and a sound and

effective security program, a substantial reduction in vulnerability exposure can be achieved. In fact, actual testing by the NSA and NIST of these security templates on workstations and servers has shown that they will reduce the vulnerabilities on systems from 80% to 90%.

In the past, applying any security policy was a complex and time-consuming task that required use of numerous complex and separate tools for workstations and servers. Furthermore, once a system was "locked down" with a template or security baseline configuration, it was extremely hard to:
1) Detect when a system became "unlocked" or non-compliant;
2) Remediate the system and bring it back into compliance.
For these reasons and others network administrators tended to avoid applying security templates to their systems and thus missed an opportunity to eliminate up to 90% of their system vulnerabilities.

To address the complexity of customizing, deploying, managing and maintaining security configurations and policies on desktops and servers, New Boundary Technologies developed Policy Commander™. Policy Commander is a ***single solution*** that contains scores of security policies that can be applied to both workstations and servers. It is no longer necessary to learn how to use separate tools and scripting languages for different versions of Windows workstations and servers. To further simplify the process of testing and applying the NIST security templates, Policy Commander has reduced the numerous individual security settings contained in the NIST templates to a smaller, more manageable collection of security policies. Thus, from a central web console and database, Policy Commander can quickly deploy a complete Microsoft, NSA or NIST security template or a single policy to one or all of your systems. Policy Commander then will continuously monitor the state of computers and security policies, notify administrators of any instances of non-compliance, and automatically remediate those non-compliant computers. Policy Commander is a solution that significantly reduces the complexity, time and effort to package, test, deploy, monitor, and enforce any security policy on any Windows-based server or workstation located anywhere in your network worldwide.

To see how Policy Commander helps you meet the GLBA Security Safeguard Rule, see Appendix A. It provides an overview of the GLBA requirements and outlines a GLBA Information Security Program with recommendations on how Policy Commander supports key parts of the plan.

Appendix B provides a list of the New Boundary Technologies' GLBA security policies for workstations. Appendix C provides a list of the New Boundary Technologies GLBA security policies for servers.

To download a full Policy Commander Evaluation version please visit the New Boundary Technologies Website at:
http://www.newboundary.com/products/policycommander/index.htm

2.0 Standards for Safeguarding Customer Information.

2.1 GLBA Objectives

There are three main objectives of GLBA 501(b) that companies need to meet.

· **501(b)(1):** Ensure the security and confidentiality of customer records and information

· **501(b)(2):** Protect against any anticipated threats or hazards to the security or integrity of such records.

· **501(b)(3):** Protect against unauthorized access or use of such records or information which could result in substantial harm or inconvenience to any customer.

In order to meet these objectives, a company will need to develop an Information Security Program and Plan.

2.2 Information Security Program

Section 314.3 (a) of the GLBA Act requires that you shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in Section 314.4 and shall be reasonably designed to achieve the objectives below.

2.3 FTC Safeguard Rule Guidance

To help financial institutions meet the above objectives the Federal Trade Commission, one of the primary enforcement agencies for both the Privacy and Safeguards Regulations, has published a Safeguards Rule that is applicable for all financial institutions that need to comply with GLBA.

As with similar regulatory laws passed, such as Sarbanes-Oxley and the Healthcare Insurance Portability and Accountability Act (HIPAA), the Safeguards Rule is designed to be flexible so that each financial institution can implement the safeguards appropriate to its own circumstances.

The Safeguards Rule applies to businesses, regardless of size, that are “significantly engaged” in providing financial products or services to consumers. This includes check-cashing businesses, data processors, mortgage brokers, non-bank lenders, personal property or real estate appraisers, professional tax prepares, courier services, and retailers that issue credit cards to consumers. The Safeguards Rule also applies to financial companies, like credit reporting agencies and ATM operators, which receive information from other financial institutions about their customers. In addition to developing their

own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

As mentioned earlier in this guide, the Safeguards Rule requires financial institutions to develop a written Information Security Program that describes their processes and controls to protect customer information. The program must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its program, each financial institution must include the following elements outlined in Section 314.4

314.4(a): Designate one or more employees to coordinate the safeguards;

314.4(b): Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;

314.4(c): Design and implement a safeguards program, and regularly monitor and test it;

314.4(d): Select appropriate service providers and contract with them to implement safeguards;

314.4(e): Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

The Information Security Program must address the elements above with respect to three safeguards. Those safeguards are: Administrative, Physical and Technical. Below is a brief discussion of what each of the safeguards might include. It is not an all-inclusive list. For a more detailed example of an Information Security Program that covers these three Safeguards see Appendix A.

A. Administrative safeguards might include:

- Checking references on potential employees.
- Training employees on basic steps they must take to protect customer information.
- Ensuring that employees are knowledgeable about applicable policies and expectations.
- Limiting access to customer information to employees who have a business need.
- Reducing exposure to the GLBA by requesting customer information only when it is required to conduct departmental activities.
- Imposing disciplinary measures where appropriate

B. Physical safeguards might include

- Locking rooms and file cabinets where customer information is kept.
- Using password activated screensavers.
- Using strong passwords.
- Changing passwords periodically and not sharing or writing them down.
- Encrypting sensitive customer information transmitted electronically.

- Referring calls/requests for customer information to trained staff.
- Being alert to fraudulent attempts to obtain customer information and reporting these to management for referral to appropriate law enforcement agencies.
- Ensuring that storage areas are protected against destruction or potential damage from physical hazards like fire or floods.
- Storing records in a secure area and limiting access to authorized employees.
- Disposing of customer information appropriately.

C. Technical safeguards might include

- Storing electronic customer information on a secure server that is accessible only with a password and is in a physically-secure area.
- Applying security configuration policies that will "lock down" those computer systems handling customer information.
- Avoid storage of customer information on machines with an Internet connection
- Maintaining secure backup media and securing archived data.
- Using anti-virus software that updates automatically.
- Obtaining and installing patches that resolve software vulnerabilities.
- Following written contingency plans to address breaches of safeguards.
- Maintaining up-to-date firewalls particularly if the institution uses broadband Internet access or allows staff to connect to the network from home.
- Providing central management of security tools and keeping employees informed of security risks and breaches.

3.0 GLBA Security Guidance

The purpose of this guide is to provide security officers and network administrators with a template for a GLBA Information Security Program. It is also intended to show how Policy Commander plays an integral part in applying security configuration policies that will "lock down" Windows XP workstations and Windows servers handling customer information without negatively impacting operations and organizational productivity. The NIST Specialized Security-Limited Functionality security template modifies several key areas of a Windows XP system, including password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings, and file permissions. The template is based on security templates previously developed by the National Security Agency (NSA), Defense Information Systems Agency (DISA), and Microsoft. Most of the settings in the template represent consensus best practices recommendations as proposed by various security experts from the Center for Internet Security (CIS), DISA, NSA, Microsoft, and NIST.

While NIST has developed different security templates with settings for use in Small Office/Home Office (SOHO), Legacy, Enterprise and High Security environments, NIST has recommended that any company that has to comply with GLBA should use the XP Specialized Security-Limited Functionality security template discussed in this guide. Therefore, New Boundary Technologies recommends that any systems (workstations or servers) that will handle sensitive customer information use or be migrated to the Windows XP operating system. This will not only provide the highest level of security

but also significantly ease the task of testing, applying and maintaining the Specialized Security-Limited Functionality security template for Windows XP.

3.1 High Security Environment

A high security environment is any environment, networked or standalone, which is at high risk of attack or data exposure. This environment encompasses computers that contain highly confidential information (e.g., personnel records, medical records, financial information) and perform vital organizational functions (e.g., accounting, payroll processing, air traffic control). These computers might be targeted by external parties for exploitation, but also might be targeted by trusted parties inside the organization. A high security environment could be a subset of a SOHO or Enterprise environment. For example, three desktops or a server in an enterprise environment that hold confidential customer information could be thought of as a high security environment within an enterprise environment. In addition, a laptop used by a mobile worker might be a high security environment within a SOHO environment. A high security environment might also be a self-contained environment outside any other environment; for instance, a government security installation dealing in sensitive data.

Systems in high security environments face threats from both insiders and external parties. Because of the risks and possible consequences of a compromise in a high security environment, it usually is the most restrictive and secure configuration. The suggested configuration provides the greatest protection at the expense of ease of use, functionality, and remote system management. In a high security environment, this guide is targeted at experienced security specialists and seasoned system administrators who understand the impact of implementing these strict requirements.

3.2 Best Practices for Analysis and Testing of Security Policies

Although the NIST security settings have undergone considerable testing and are recommended for companies dealing with GLBA security, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST Windows XP Specialized Security-Limited Functionality Template was driven by the need to create a more secure Windows XP workstation configuration. Because some settings in the templates may reduce the functionality or usability of the system, it is not recommended that the complete template be used as a baseline security configuration. Specific settings in the templates should be modified as needed so that the settings conform to local policies and support required system functionality. New Boundary Technologies strongly recommends that organizations fully test the GLBA policies contained in Policy Commander on representative systems before widespread deployment. Some settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile.

NBT recommends the following steps be taken to test the policies:

1) Analyze: Conduct a risk assessment of the assets in your network that will handle customer financial information. Use Policy Commander as part of the risk assessment to

compare the current security policies of the local workstation/servers to the policies required to meet the GLBA Security Rule.

2) Test: When new security settings or policies are applied, they can interfere with the operation of existing software applications and other operations on the target computers. We strongly recommend testing each new policy thoroughly in the test environment before moving it to the production environment. Our recommended testing methodology includes the following steps:

- System administrators build their systems from a clean formatted state to begin the process of securing Windows XP workstations.
- System administrators should perform the installation and test process on a secure network segment or off the organization's network until the security configuration is completed.
- All patches, service packs, hotfixes and rollups for XP should be applied.
- All desktop or server applications should be installed, operational and have all upgrades/patches applied.
- Strong passwords should be set for all accounts.

3) Assign: Use Policy Commander to install the New Boundary Technologies security policies derived from the NIST security template in the test mode. In the past, network administrators would have to apply the entire NIST security template and then spend hours troubleshooting the dozens of settings to see which ones caused a problem on the test workstation. By reducing the NIST security template to a small collection of key policies, network administrators now can individually apply each policy, modify it as necessary, and then add the next policy. This will significantly decrease the time required to test and configure the GLBA security configuration that best fits your environment.

The New Boundary Technologies GLBA security policies are organized based on the nine categories identified by NIST. Those categories are:

1) Account Policies
2) Local Policies
3) Event Log Policies
4) Restricted Groups
5) System Services
6) File Permissions
7) Registry Permissions
8) Registry Values
9) File and Registry Auditing

Appendix B provides an overview of these nine categories and which New Boundary Technologies GLBA security policies are in each category. Appendix C is an overview of the Windows Server security policies contained in Policy Commander that can used to lock down the security configuration of servers based on their role.

4) Enforce: Save your final security configuration baseline, use Policy Commander to organize your key GLBA workstations and servers, and then deploy the GLBA security configuration baseline. New Boundary Technologies recommends that the automatic enforcement feature be utilized to ensure complete 24x7 enforcement of the GLBA security configuration.

For a complete overview of how Policy Commander works, download a fully functional 30 day trial version at:
http://www.newboundary.com/products/policycommander.index.htm

4.0 Summary of Recommendations

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.
- Reduce the opportunities that attackers have to breach a system by limiting functionality according to the principle of least privilege and resolving security weaknesses.
- Select security controls that provide a reasonably secure solution while supporting the functionality and usability that users require.
- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.
- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide what additional measures (if any) should be implemented.
- Document procedures for implementing and maintaining security controls. Maintain other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications, such as acceptable use policy, configuration management policy, and IT contingency plans.
- Test all security controls, including the settings in the NIST security templates, to determine what impact they have on system security, functionality, and usability. Take appropriate steps to address any significant issues.
- Monitor and maintain systems on a regular basis so that security issues can be identified and mitigated promptly. Actions include acquiring and installing software updates, monitoring event logs, providing remote system administration and assistance, monitoring changes to OS and software settings, protecting and sanitizing media, responding promptly to suspected incidents, performing vulnerability assessments, disabling and deleting unused user accounts, and maintaining hardware.

  Note: Policy Commander automates security policy management to streamline the processes noted above and significantly improve IT efficiency while promoting security best practices.

Appendix A

GLBA Information Security Plan

Appendix A provides a draft of a GLBA Information Security Guide. It is based on the NIST recommendations for meeting other regulatory requirements such as HIPAA. Table 1 provides a crosswalk between the GLBA Objectives and the GLBA Elements that comprise the Safeguards. Table 2 is a suggested outline of a GLBA Information Security Plan. It is based on New Boundary Technologies' work in the HIPAA regulatory market and on the National Institute of Standards and Technology (NIST) publication SP800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*. This outline is a good starting point for the development of a final GLBA Information Security Program tailored for your particular company's needs and requirements.

Table 1

GLBA Element Section	GLBA Elements	GLBA Objective
314.4(a)	**Assign Security Responsibility: Identify the security official who is responsible to develop, implement, and maintain your information security program.**	**501(b)(1)**
314.4(b)	**Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: 314.4(b)(1), 314.4(b)(2) and 314.4(b)(3)**	**501(b)(2)**
314.4(b)(1)	Employee training and management	**501(b)(3)**
314.4(b)(2)	Information systems, including network and software design, as well as information processing, storage, transmission and disposal	**501(b)(2)**
314.4(b)(3)	Detecting, preventing and responding to attacks, intrusions, or other systems failures	**501(b)(2)**

314.4(c)	**Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.**	**501(b)(2)**
314.4(d)	**Oversee service providers by:**	**501(b)(1)**
314.4(d)(1)	Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;	**501(b)(3)**
314.4(d)(2)	Requiring your service providers by contract to implement and maintain such safeguards.	**501(b)(3)**
314.4(e)	**Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.**	**501(b)(1)**

Table 2		
GLBA Sections	**Information Security Program GLBA Element**	**Policy Commander Capabilities**
Administrative Safeguards		
Objective 501(b)(1)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
314.4(a)	Assign Security Responsibility: Identify the security official who is responsible to develop, implement, and maintain your information security program.	
314.4(b)	Risk Analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of customer information held by the company or service providers.	Use Policy Commander to assess current security policy configuration and risk.
314.4(b)	Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Objective 501(b)(2)	Use Policy Commander to apply the GLBA Policy Library based on the NIST Security Templates in NIST Special Publication 800-68.
314.4(b)(3)	Sanction Policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	N/A
314.4(c)	Information System Activity Review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Policy Commander continuously reviews and maintains audit logs, access reports, and security incident tracking reports.
314.4(b)(1)	Authorization and/or Supervision: Implement procedures for the authorization and/or supervision of workforce members who work with customer information or in locations where it might be accessed.	Policy Commander can restrict access to workstations and servers to only authorized workforce members.
314.4(b)(3)	Workforce Clearance Procedure: Implement procedures to determine that the access of a workforce member to customer information is appropriate.	N/A

314.4(b)(3)	Termination Procedure: Implement procedures for terminating access to customer information when the employment of a workforce member ends or as required by determinations made by management.	N/A
Objective 501(b)(3)	**Information Access Management: Implement policies and procedures for authorizing access to customer information that are consistent with the applicable requirements of Objective 501(b)(3)**	
314.4(d)(2)	Isolating Service Provider Functions: If a Service Provider is part of a larger organization, the Service Provider must implement policies and procedures that protect the customer information of the Service Provider from unauthorized access by the larger organization.	A Service Provider can use Policy Commander to implement the same security policies as the larger organization.
314.4(b)(2)	Access Authorization: Implement policies and procedures for granting access to customer information, for example, through access to a workstation, transaction, program, process, or other mechanism.	The Policy Commander GLBA Policy Library contains recommended security policies that secure access to customer information. Policy Commander can also be used as a Secure Access Gateway for mobile or remote users. Use the Policy Editor to create access policies that will be checked and remediated on all user systems before they are allowed access to the internal network. This can also be applied to all Service Providers who have access to the internal network.
314.4(b)(2)	Access Establishment and Modification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program, or process.	The Policy Commander GLBA Policy Library contains recommended security policies that will establish access control to workstations that contain customer information.
Objective 501(b)(3)	**Security Awareness and Training: Implement a security awareness and training program for all members of the workforce (including management).**	

314.4(b)(1)	Security Reminders: Periodic security updates.	Policy Commander automatically provides security updates to workstations and servers.
314.4(b)(1)	Protection from Malicious Software: Train employees about the processes and procedures that the company is using to guard against, detect and report malicious software.	Applying the GLBA Policy Library will reduce system vulnerabilities by over 90%, minimizing the need for extensive employee training, and is key to complying with the GLBA Security Rule.
314.4(b)(1)	Log-in Monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	N/A
314.4(b)(1)	Password Management: Procedures for creating, changing, and safeguarding passwords.	N/A
Objective 501(b)(3)	**Security Incident Procedures: Implement policies and procedures to address security incidents.**	
314.4(c)	Response and Reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Policy Commander will automatically identify, respond and correct suspected and known security policy incidents. Policy Commander will document/log security incidents and provide full reports.
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 customer information.**	
314.4(b)(3)	Data Backup Plan: Establish and implement procedures to create and maintain retrievable exact copies of customer information.	N/A
314.4(b)(3)	Disaster Recovery Plan: Establish (and implement as needed) procedures to restore any loss of data.	N/A
314.4(b)(3)	Emergency Mode Operation Plan: Establish procedures to enable continuation of critical business processes for protection of the security of customer information while operating in emergency mode.	N/A

314.4(c)	Testing and Revision Procedure: Implement procedures for periodic testing and revision of contingency plans.	N/A
314.4(c)	Applications and Data Criticality Analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.	N/A
Objective 501(b)(1)	**Evaluation: Perform a 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 314.4(e) and Objective 501(b)(1)**	Policy Commander continuously provides real-time evaluation, enforcement and reporting of the GLBA security configuration selected.
Objective 501(b)(3)	**Service Provider Contracts and Other Arrangements: A covered entity, in accordance with 314.4(d), 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, in accordance with 314.4(d)(2), that the Service Provider will appropriately safeguard the information.**	A Service Provider can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on Service Provider's workstations requesting access to the network.
314.4(d)(1)&(2)	Written Contract or Other Arrangement: Document the satisfactory assurances through a written contract or other arrangement with the Service Provider that meets the applicable requirements of 314.4(d)	N/A

Table 3		
GLBA Sections	**Information Security Program GLBA Element**	**Policy Commander Capabilities**
Physical Safeguards		
Objective 501(b)(3)	**Facility Access Controls: Implement policies and procedures to limit physical access to customer information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**	
314.4(b)(3)	Contingency Operations: Establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	N/A
314.4(b)(3)	Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.	N/A
314.4(b)(3)	Access Control and Validation Procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	N/A
314.4(b)(3)	Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks.	N/A
314.4 (c)	Workstation Use: Implement 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 that can access customer information.	Use Policy Commander to create custom security policies that will restrict improper functions, such as unauthorized applications, changes to admin rights, access to files, etc from being executed on the workstation by end users.
314.4 (c)	Workstation Security: Implement physical safeguards for all workstations that access customer information to restrict access to authorized users.	N/A

314.4 (c)	Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain customer information into and out of a facility, and the movement of those items within the facility.	
314.4 (c)	Disposal: Implement policies and procedures to address the final disposition of customer information, and/or the hardware or electronic media on which it is stored.	N/A
314.4 (c)	Media Re-Use: Implement procedures for removal of customer information from electronic media before the media are made available for reuse.	Policy Commander contains policies that will prevent the attachment and/or use of portable USB storage devices.
314.4 (c)	Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible thereof.	N/A
314.4 (c)	Data Backup and Storage: Create a retrievable, exact copy of customer information, when needed, before movement of equipment.	N/A

GLBA Sections	Information Security Program GLBA Element	Policy Commander Capabilities
Technical Safeguards		
Objective 501(b)(3)	**Access Control: Implement technical policies and procedures for electronic information systems that maintain customer information to allow access only to those persons or software programs that have been granted access.**	
314.4 (b)(3)	Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.	N/A
314.4 (b)(3)	Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary customer information during an emergency.	N/A

314.4 (b)(3)	Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Policy Commander contains a policy that can be set to automatically log off a user after a set time limit.
314.4 (b)(3)	Workstation Security: Implement physical and technical safeguards for all workstations that access customer information to restrict access to authorized users.	N/A
314.4 (b)(3)	Encryption and Decryption: Implement a mechanism to encrypt and decrypt customer information on all Laptops and PDA's.	N/A
314.4 (b)(3)	Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use customer information.	
314.4 (b)(3)	Mechanism to Authenticate Customer information: Implement electronic mechanisms to corroborate that customer information has not been altered or destroyed in any unauthorized manner.	Policy Commander contains a policy that can restrict access to files or folders that contain customer information to only those with authorized access.
314.4 (b)(3)	Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to customer information is the one claimed.	Use the above File/Folder Access policy to help verify access to files or folders containing customer information.
314.4 (b)(3)	Transmission Security: Implement technical security measures to guard against unauthorized access to customer information that is being transmitted over an electronic communications network.	N/A
314.4 (b)(3)	Integrity Controls: Implement security measures to ensure that electronically transmitted customer information is not improperly modified without detection until disposed of.	The policy that restricts access to files or folders that contain customer information can also ensure that the information is not improperly modified without detection until disposed of.
314.4 (b)(3)	Encryption: Implement a mechanism to encrypt customer information whenever deemed appropriate.(Mandatory Policy on all Laptops)	N/A

GLBA Sections	Information Security Program GLBA Element	Policy Commander Capabilities
Service Provider Contracts		
Objective 501(b)(3)	**Service Provider Contracts or Other Arrangements: (i) The contract or other arrangement between the covered entity and its Service Provider required by Section 314.4(d) must ensure that the Service Provider meets the requirements of the covered entity Information Security Program(ii) A covered entity is not in compliance with the standards in 314.4(d) and sub-paragraphs 314.4(d)(1) and (2) if the covered entity knew of a pattern of an activity or practice of the Service Provider that constituted a material breach or violation of the Service Provider's obligation under the contract or other agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful Terminate the contract or arrangement, if feasible.**	
314.4 (d)(2)	**Service Provider Contracts:** The contract between a covered entity and a Service Provider must provide that the Service Provider will – (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of customer information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the Service Provider has violated a material term of the contract.	A Service Provider can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on the Service Provider's workstations requesting access to the network.

Objective 501(b)(1)	**Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.**	Policy Commander complements other GLBA solutions designed to create the covered entity's GLBA Security Policy Manual. Policy Commander deploys, monitors, and automatically remediates those specific GLBA security policies that apply to workstation and server security.
314.4 (e)	Documentation: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Policy Commander continuously maintains electronically the security policies and procedures implemented to meet the GLBA Security Rule. Policy Commander also maintains a printable record of any action, activity, or assessment conducted on the security configuration established by the covered entity. This record can be provided to any GLBA auditor.
314.4 (e)	Time Limit: Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	N/A
314.4 (e)	Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Available with Policy Commander.
314.4 (e)	Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the customer information.	Available with Policy Commander.

Appendix B

New Boundary Technologies' GLBA Workstation Policies

This chart describes the **workstation** security policies contained in the New Boundary Technologies GLBA Windows XP High Security Template. These policies are organized into nine key security categories based on the National Institute of Standards and Technology (NIST) Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*.

Category 9 contains custom policies developed by New Boundary Technologies to meet other GLBA security requirements.

Security Categories	Policy Commander Policies
1.0 Account Policies	• Harden account lockout settings
2.0 Local Policies 2.1 Audit Policies 2.2 User Rights Assignment 2.3 Security Options	• Control the System Audit Policy settings • Harden the User Rights Assignment settings • Disable the Guest Account • Limit local account use of blank passwords to console only • Harden Device settings • Harden Domain Member settings • Harden Interactive Logon settings • Harden Microsoft network server settings • Harden network access settings • Harden network security settings • Harden Recovery Console settings • Harden Shutdown settings • Enforce FIPS Certified Cryptography • Harden System Objects settings • Shut down immediately if unable to log security audits • Disallow anonymous SID_Name translation • Force logoff when logon hours expire
3.0 Event Log Policies	• Control Event Log settings
4.0 Restricted Groups	• Remove all users from the Remote Desktop Users and Power Users groups.
5.0 System Services	• Alerter • Clip book • FTP Publishing • HS Admin Service • Messenger • NetMeeting Remote Desktop Sharing • Routing and Remote Access • Simple Mail Transfer Protocol (SMTP) • Simple Network Management Protocol (SNMP) Service • SNMP Trap • Telnet

	• World Wide Web Publishing Services • Computer Browser • Remote Registry • Task Scheduler • Terminal Services • Fax Service • Indexing Service • Remote Desktop Help Session Manager • Universal Plug & Play Device Host • Net logon
6.0 File Permissions	• Harden security permissions for critical files
7.0 Registry Permissions	• Harden security permissions for critical registry keys
8.0 Registry Values 8.1 Debugging 8.2 Automatic Functions 8.3 Networking	• Disable the Dr. Watson debugger and memory dump file • Disable automatically running CD-ROMs • Disable automatic administrator logon • Disable automatic reboot • Strengthen miscellaneous networking settings • Harden the Microsoft TCP/IP stack settings
9.0 Custom GLBA Policies 9.1 Automatic Logoff 9.2 Customer File Protection 9.3 USB Removable Device	• Meets GLBA Technical Safeguard 314.4(b)(3) • Meets GLBA Technical Safeguard 314.4(b)(3) • Meets GLBA Physical Safeguards 314.4(c)

Appendix C

New Boundary Technologies' GLBA Server Policies

This chart describes the **server** security policies contained in Policy Commander that can be used to secure your servers to meet GLBA requirements.

For further information, refer to the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at: *http://www.microsoft.com/technet/security/topics/serversecurity/tcg/tcgch00.mspx*

Server Role	Policy Commander Policies
1.0 Domain Controller	• Windows Server 2003: High Security - Domain Controller • Windows Server 2003: Enterprise Client - Domain Controller • Windows Server 2003: Legacy Client - Domain Controller • Windows 2000 Server: Domain Controller
2.0 File Server	• Windows Server 2003: High Security - File Server • Windows Server 2003: Enterprise Client - File Server • Windows Server 2003: Legacy Client - File Server • Windows 2000 Server: File Server
3.0 IIS Server	• Windows Server 2003: High Security - IIS Server • Windows Server 2003: Enterprise Client - IIS Server • Windows Server 2003: Legacy Client - IIS Server • Windows 2000 Server: IIS Server
4.0 Infrastructure Server	• Windows Server 2003: High Security - Infrastructure Server • Windows Server 2003: Enterprise Client - Infrastructure Server • Windows Server 2003: Legacy Client - Infrastructure Server • Windows 2000 Server: Infrastructure Server
5.0 Member Servers	• Windows Server 2003: High Security - Member Server • Windows Server 2003: Enterprise Client - Member Server • Windows Server 2003: Legacy Client - Member Server • Windows 2000 Server: Member Server
6.0 Print Servers	• Windows Server 2003: High Security - Print Server • Windows Server 2003: Enterprise Client - Print Server • Windows Server 2003: Legacy Client - Print Server • Windows 2000 Server: Print Server

6.0 Certificate Services Server	• Windows Server 2003: Enterprise Client - Cert Services Server
7.0 IAS Server	• Windows Server 2003: Enterprise Client - IAS Server