



GoToMyPC Corporate Gramm- Leach-Bliley Act Compliance Guide

Protection, privacy and remote access

Protecting the integrity of your company network and the privacy of sensitive data is of utmost concern to any enterprise, especially when extending remote access. Many organizations must also comply with the standards set by the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLB Act, which includes provisions to protect consumers' personal financial information held by financial institutions.

GoToMyPC Corporate is a secure, managed service that provides remote access to the desktop. It reduces the costs and complexities associated with traditional remote-access solutions while offering administrators the highest level of security and centralized control.

GLBA security compliance

The GLB Act applies to financial institutions that offer financial products or services to individuals such as loans, financial or investment advice or insurance. Among the institutions that fall under FTC jurisdiction for purposes of the GLB Act are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services and debt collectors.

The following guide is based upon the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. A copy of the final standard is available here: <http://www.fdic.gov/regulations/information/ebanking/66FR8615.pdf>

This guide was created to assist financial institutions in understanding the various GLB Act requirements and to demonstrate how GoToMyPC Corporate can support GLB Act compliance. General GLB Act questions and answers can be found at the end of this document.

II Standards for safeguarding customer information

A: Information security program: You shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to your size and complexity and the nature and scope of your activities. While all parts of your organization are not required to implement a uniform set of policies, all elements of your information security program must be coordinated.

B: Objectives: Your information security program shall be designed to:

	Applicable sections	Support in GoToMyPC Corporate
B.1	Ensure the security and confidentiality of customer information.	<ul style="list-style-type: none"> • SSL-encrypted website and Advanced Encryption Standard (AES) encryption using 128-bit keys ensure the privacy of all remote connections. • Administrators control the feature set of individual users or groups to restrict such features as file transfer, guest invite and remote printing. • Users accessing their host Macs and PCs with GoToMyPC Corporate have only the same access to services as if they were physically present at their host computers. • Administrators can define day/time during which users may access their host computers.
B.3	Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.	<ul style="list-style-type: none"> • GoToMyPC Corporate can be configured to adhere to your company's established access-control policy. • Secondary authentication via a host-specific access code is required before accessing screen sharing, file transfer or other host services. The access code is never stored anywhere; the SRP (Secure Remote Protocol) protocol allows the host to verify the user's knowledge of the access code while simultaneously establishing end-to-end secrecy and integrity keys. • Additionally, company administrators can require users to use one-time passwords or RSA SecurID for two-factor authentication (PC only). • Administrators can set the host computer screen to be blanked out and the physical keyboard and mouse to be disabled when a user remotely accesses the computer (PC only). This prevents any unauthorized persons physically near the host computer to either see or access the computer. • Administrators can configure GoToMyPC to automatically lock the host computer once the user disconnects from a session to prevent further access without authorized system credentials.

III Development and implementation of customer information security program

C: Manage and control risk: You shall design your information security program to control the identified risks commensurate with the sensitivity of the information as well as the complexity and scope of your activities. You must consider whether the following security measures are appropriate for you and, if so, adopt those measures you conclude are appropriate.

	Applicable sections	Support in GoToMyPC Corporate
C.1.a	Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.	<ul style="list-style-type: none"> • Users are first authenticated at the GoToMyPC website by providing their email addresses and passwords. A secondary password that must be provided is the host computer access code. The host computer access code is the shared secret between users and their host computers. • All desktop access controls remain in place, e.g., the user must still log in through Windows. • Administrators control the feature set of individual users or groups to restrict such features as file transfer, guest invite and remote printing. • Users accessing their host computers with GoToMyPC Corporate have only the same access to services as if they were physically present at their host computers. • Company administrators can require users to use one-time passwords or RSA SecurID for two-factor authentication (PC only).
C.1.c	Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.	<ul style="list-style-type: none"> • An SSL-encrypted website and Advanced Encryption Standard (AES) encryption using 128-bit keys ensure the privacy of all remote connections. AES is a U.S. government standard algorithm and is Federal Information Processing Standard (FIPS) approved. Dual passwords plus end-to-end user authentication provide maximum security.
C.1.f	Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	<ul style="list-style-type: none"> • GoToMyPC Corporate generates usage/connection logs that can be reviewed by the customer for auditing purposes. And in addition, operates an intrusion detection system on its website and networks.

GoToMyPC Corporate product information

Security, control and customization

Users and administrators have the option of assigning users to groups defined by the features to which they are granted access. Some features may be disabled by an IT administrator to customize the level of security that is appropriate for your organization. In addition, GoToMyPC Corporate offers an Authorization Management Service to ensure that only users with approved GoToMyPC Corporate accounts can access your organization's networks. Because the

security features are built in, administrators can rest easy: Security cannot be weakened by inexperienced users.

Encryption

An SSL-encrypted website and Advanced Encryption Standard (AES) encryption using 128-bit keys ensure the privacy of all remote connections. AES is a U.S. government standard algorithm and is Federal Information Processing Standard (FIPS) approved. Dual passwords plus end-to-end user authentication provide maximum security without compromising performance. This multi-level authentication and state-of-the-art encryption keeps your corporate traffic safe.

GoToMyPC Corporate is firewall friendly, yet secure. Because most firewalls are already configured to permit outgoing web traffic, you don't have to bypass or compromise your company firewall to implement secure remote access to the desktop with GoToMyPC Corporate.

Administrator control

End-user settings are controlled by your company's administrator and can be customized as needed. Administration capabilities include: enforcing the use of one-time passwords; requiring client and host authorization; managing availability of remote printing and file transfer; and setting business rules for lockout in the event of multiple failed log-in attempts. Administration reports enable real-time monitoring and management of remote-access traffic.

RSA SecurID integration

GoToMyPC Corporate can be seamlessly integrated with RSA Security's SecurID to provide unparalleled protection for remote desktop access (PC only).

Frequently asked questions

Q: What is the Gramm-Leach-Bliley (GLB) Act?

The GLB Act of 1999 establishes standards for financial institutions relating to administrative, technical and physical safeguards regarding customer records and information.

Q: What is the purpose of this act?

- This act has been established to ensure the security and confidentiality of customer records and information by protecting against potential threat and unauthorized access.

Q: Under which provisions of the act does the GoToMyPC Corporate service apply?

Section II: Standards for Safeguarding Customer Information, Sections A and B.

Section III: Development and Implementation of Customer Information Security Program, Section C.

Q: How does the use of GoToMyPC Corporate affect compliance?

The security architecture of services offered includes policy definition and enforcement mechanisms consistent with the best-practice guidance given for user management and remote access within the act.

Please refer to the table above for a detailed breakdown of how GoToMyPC Corporate addresses the relevant remote-access security points within the standard or review a copy of the standard act.

Q: What is the best way to deploy GoToMyPC Corporate in an environment striving to maintain compliance?

Organizations should carefully review all configurable security features of GoToMyPC Corporate in the context of their security standards and deployed environments to determine which features should be enabled and how best to configure them.

The GoToMyPC Corporate administration center offers companies web-based user management, host/client end-point management and auditing features that can be used to enforce the desired compliance level.