GoToAssist 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 receiving remote support. 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.

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.occ.treas.gov/fr/cfrparts/12CFR30.htm

Citrix Online created this guide to assist financial institutions in understanding the various GLB Act requirements and to demonstrate how Citrix® GoToAssist® Corporate can support GLB Act compliance.

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 Citrix GoToAssist Corporate
B.1	Ensure the security and confidentiality of customer information.	• Secure Sockets Layer (SSL) 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. • Administrators can define day/time during which representatives may provide remote support service.
B.3	Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.	• GoToAssist Corporate can be configured to adhere to your company's established access-control policy. • Representatives and managers must log in to GoToAssist Corporate using unique user IDs and strong passwords. • GoToAssist Corporate includes a configurable failed log-in lockout threshold. • Technicians running GoToAssist Corporate as a service must log in with the proper credentials of a local or domain administrator. • PC access is 100% permission based and the client receiving support retains overriding control at all times.

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 Citrix GoToAssist Corporate
C.1a	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.	• Support reps and managers are first authenticated at the GoToAssist Web site by providing their email addresses and passwords. • PC access is 100% permission based and the client receiving support retains overriding control at all times. • Administrators control the feature set of individual users or groups to restrict such features as File Transfer. • Representatives must be approved and set up by an administrator before they can access client computers.
C.1c	Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.	• SSL and 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.
C.1f	Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	• GoToAssist Corporate generates usage/connection logs that can be reviewed by the customer for auditing purposes. In addition, Citrix Online operates an intrusion detection system on its Web site and networks.

GoToAssist Corporate product information

GoToAssist Corporate is a secure, managed solution that allows support agents to remotely view and optionally control a customer's PC when technical help is requested. A complete online Management Center enables administrators to monitor and control remote-support activity, to ensure compliance with your organization's security requirements

Security, control and customization

Support 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 administrator to customize the level of security that is appropriate for your organization. Administration reports enable real-time monitoring and management of remote-support activity. Because the security features are built in, administrators can rest easy: Security cannot be weakened by inexperienced users.

Encryption

Secure Sockets Layer (SSL) 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. Strong 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.

GoToAssist 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 GoToAssist Corporate.

100% Permission based

Support representatives can only remotely access a customer's PC upon receiving permission from the customer, and the customer retains overriding control of all screen-sharing, keyboard and mouse activity at all times. Technicians running GoToAssist Corporate as a service must also log in with the proper credentials of a local or domain administrator.

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 GoToAssist 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 GoToAssist Corporate affect compliance?

The security architecture of services offered by Citrix Online 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 GLB Act Compliance Guide for a detailed breakdown of how GoToAssist 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 GoToAssist Corporate in an environment striving to maintain compliance?

Organizations should carefully review all configurable security features of GoToAssist 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 GoToAssist Corporate Management Center offers companies Web-based user management and auditing features that can be used to enforce the desired compliance level.

Need more information?

Contact us to discuss how GoToAssist Corporate can be configured to securely meet the needs of your unique remote support environment. If you're currently a customer, call your individual account manager. If you're considering purchasing GoToAssist Corporate, call us toll-free at 1-800-549-8541, direct dial +1-690-5729 or email gotoassist@citrixonline.com.

Citrix Online

About Citrix Online

Citrix Online provides secure, easy-to-use online solutions that enable people to work from anywhere with anyone. Whether using GoToMyPC® to access and work on a remote PC, GoToAssist® to support customers or GoToMeeting® to hold online meetings and Webinars, our customers – more than 35,000 businesses and hundreds of thousands of individuals – are increasing productivity, decreasing travel costs and improving sales, training and service on a global basis. A division of Citrix Systems, Inc. (Nasdaq: CTXS), Citrix Online is based in Santa Barbara, California. For more information, visit www.citrixonline.com or call 805-690-6400.

17399/8.27.08/PDF

CITRIX® | online