GoToMyPC

White Paper: PCI

GoToMyPC Corporate and Payment Card Industry (PCI) Compliance

GoToMyPC Corporate provides industry-leading configurable security controls and centralized endpoint management that can be implemented to meet the PCI DSS requirements.

Scope and audience

This guide is for GoToMyPC Corporate customers and other stakeholders who need to understand how GoToMyPC can meet the requirements outlined in the Payment Card Industry Data Security Standard (PCI DSS). This document solely addresses the GoToMyPC Corporate product as it pertains to the PCI DSS standards. This document is only a guide and not an authority on validating the GoToMyPC Corporate product with the PCI DSS. It is ultimately up to the merchant, service provider or Qualified Security Assessor (QSA) whether the GoToMyPC Corporate product would address the PCI DSS requirements as implemented in the customer's unique environment.

Introduction

Protecting the integrity of your company network and the privacy of sensitive data like credit card information is of utmost concern to any enterprise, especially when extending remote access. Merchants who are involved with the processing, storing or transmitting of credit card information must also comply with the PCI DSS. This guide was created to assist those merchants who want to implement GoToMyPC Corporate into their environment that needs to comply with the PCI DSS.

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.

The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS does this by providing a baseline of technical and operational requirements designed to protect cardholder data. These regulations apply to all entities involved in payment card processing – including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmit cardholder data.

This document focuses on the information security features of GoToMyPC Corporate as it pertains to the PCI DSS. Before reading, you should already have a basic understanding of the product, its features and the PCI DSS. Additional materials on GoToMyPC Corporate may be found online at **www.gotomypc.com** or by contacting a representative. Additional information on the PCI DSS program can be found at **https://www.pcisecuritystandards.org**.

Payment Card Industry Data Security Standard compliance

The GoToMyPC Corporate product contains various security and administrative features that can be used to meet the PCI DSS requirements. The table below describes some of these features and which PCI DSS requirement they may meet in the customer's environment. This list is not intended to be exhaustive but rather a highlight of the key controls when looking at the PCI DSS program. Detailed information about the security controls in GoToMyPC Corporate can be found in the GoToMyPC Corporate **Security White Paper** and **Security FAQs**.

Key requirements guide

PCI DSS Requirement	GoToMyPC Corporate
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	• GoToMyPC generates only outbound HTTP/TCP traffic to ports 80,443 and/or 8080. • Traffic can be filtered to only the GoToMyPC broker address. • We will filter GoToMyPC connections to only company-authorized network address blocks.
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.	• GoToMyPC is completely compatible with application proxy firewalls, dynamic IP addresses and network/ port address (NAT/PAT) translation.
2.1 Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	• Unique accounts and passwords must be created at installation of product. No vendor defaults are used.
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	• All GoToMyPC Corporate connections are "end-to-end" encrypted using 128-bit AES (FIPS 197) encryption in Counter Mode (CTR). • Unique 128-bit AES secret encryption keys are generated for each session. • The Secure Remote Password (SRP) protocol is used for "end-to-end" encrypted authentication. • Numerous additional checks are made on the session data after it is received to ensure network transmission integrity. • All website connections are protected using SSL with a minimum of 128-bit symmetric encryption and a 1024-bit authenticated key agreement.
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	• We continuously tests and improves upon the GoToMyPC Corporate product. Updates are regularly released to customers. • Our servers run on hardened Linux servers with the latest security patches installed. Servers have penetration and vulnerability testing conducted on them.
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. 8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	• Account managers organize users into groups, defining access policy on a per-user or per-group basis. • Users and account managers are identified by using their unique email address as their log-in name. • GoToMyPC does not circumvent operating system-level access controls already in place.

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)	• Users are required to enter a username and password and then a secondary password at the host computer. • Users can generate optional one-time passwords (OTP). • GoToMyPC integrates with existing RSA SecureID infrastructure. • Local operating system access controls are never overridden.
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	• Passwords are always transmitted or stored encrypted. • Access code verifiers are stored encrypted on the user's computer and never transmitted.
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. 8.5.2 Verify user identity before performing password resets. 8.5.4 Immediately revoke access for any terminated users. 8.5.5 Remove/disable inactive user accounts at least every 90 days. 8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use. 8.5.8 Do not use group, shared, or generic accounts and passwords or other authentication methods. 8.5.9 Change user passwords at least every 90 days. 8.5.10 Require a minimum password length of at least seven characters. 8.5.11 Use passwords containing both numeric and alphabetic characters. 8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts. 8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	• Administrators can add, delete and modify users. • Users can either reset their password via a self-service function verified through email or by contacting a support representative who will verify their identity. • Administrators can revoke user access at any time. • The administration center can be used to check the activation status for individuals and groups. Controls are available to temporarily suspend or permanently cancel any user or group account. • A guest mode can be used and is restricted to a one-time use for the guest. Access can be monitored and terminated at any time. A view-only mode exists for more restricted access. • Unique accounts and passwords are used. • The password expiration period is configurable. If the account holder logs in and the password has expired, the account holder is forced to change his or her password. • Passwords are required to be at least 8 characters long. • Passwords are required to contain both numbers and letters. • Password reuse rules can be configured. • By default, after 3 authentication failures, access to the user's account and computer are temporarily deactivated for 5 minutes. Administrators can match existing security policies by customizing the lockout period and enabling hard lockout after a consecutive number of incorrect password entries. Hard lockouts require administrator intervention to unlock the user's account. Reports allow administrators to view GoToMyPC Corporate usage and account information. • Users are logged out of the GoToMyPC website after 15 minutes of inactivity. The viewer session is configurable to time out after a period of inactivity.

Requirement 10: Track and monitor all access to network resources and cardholder data	• The administrator can view connection history for any given day, including connections that are still active. Each connection record displays details such as the first and last name of the user, name of host, the IP address, connection start and stop times and connection duration. • The administrator can generate reports for specific dates and ranges that provide details on users, connection time and duration, enabled users, security features enabled for users/groups, hours of access, last log-in time and failed log-in attempts. • Event logs can be integrated into existing reporting infrastructure. • We maintain additional logs about the connection to aid in diagnosis. Logs are restricted to select personnel.

Frequently asked questions

Q: Is GoToMyPC Corporate compliant with the PCI DSS?

GoToMyPC Corporate is not directly subject to the PCI DSS because it is a remote access technology. If GoToMyPC Corporate is used as a remote access solution for a customer's environment that is subject to the PCI DSS, then certain PCI DSS requirements may need to be met depending on how the product is implemented and the network scope of the PCI environment. It is up to a PCI Qualified Security Assessor (QSA) and the customer to determine the scope for their PCI DSS assessment.

Q: I am using the GoToMyPC Pro product instead of GoToMyPC Corporate. Can that meet the intent of the PCI DSS requirements?

It is recommended that GoToMyPC Corporate be used in an environment needing to comply with the PCI DSS requirements due to the extra configurable security controls and centralized management found in the product.

Q: Are you compliant with the PCI DSS?

Yes, as a merchant we maintain compliance with the PCI DSS. An annual assessment, quarterly vulnerability scans and penetration testing are conducted to maintain compliance.