What is PCI DSS?

DSS is built around six core principles and twelve main requirements. This document discusses how LogMeIn Central relates to each of these principles and requirements, based on PCI DSS version 3.0.

“The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.”

Source: https://www.pcisecuritystandards.org/security_standards/

- Network security
  - Installation and maintenance of a firewall configuration to protect cardholder data
  - Not using vendor-supplied defaults for system passwords and other security parameters
- Protecting cardholder data
  - Protection of stored cardholder data
  - Encrypted transmission of cardholder data across open, public networks
- Maintenance of a vulnerability management program
  - Application and maintenance of anti-virus software
  - Development and maintenance of secure systems and applications
- Implementation of strong access control measures
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly monitoring and testing networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
- Maintenance of and information security policy
  - Maintain a policy that addresses information security

How LogMeIn Central Supports PCI Compliance

LogMeIn understands that organizations that store, process, or transmit cardholder data must meet strict requirements to be PCI compliant. This document indicates some of the ways in which we help organizations comply with PCI requirements.

PCI compliance specifically relates to the security and controls around the payment applications and cardholder data within the merchant’s IT environment. LogMeIn is not a payment solution and at no time does LogMeIn handle, process, or store credit card data; therefore, LogMeIn Central falls outside of the scope of PCI review. According to the PCI Security Standards Council, it is the merchant or service provider’s responsibility to ensure that they are using only products that support compliance.

The role of LogMeIn Central is to provide secure remote access and systems administration to PCI-compliant organizations without compromising compliance. There is currently no PCI evaluation or certification process for third party applications like LogMeIn. As a result, the question “Is LogMeIn Central PCI Compliant?” is not the right question. As noted, the valid question is “How does LogMeIn Central help organizations comply with PCI requirements?”
NETWORK SECURITY: BUILD AND MAINTAIN A SECURE NETWORK

• Requirement 1. Install and maintain a firewall to protect data.
  LogMeIn servers are hosted at a leading, carrier-grade data center with restricted, secured
  access, redundant power, dual HVAC, fire detection systems, and 24/7 network monitoring.

• Requirement 2. Do not use vendor-supplied defaults for system passwords and other security
  parameters.
  LogMeIn Central customers define their own passwords when creating an account. These
  passwords are not generated by LogMeIn.

PROTECTING CARDHOLDER DATA

• Requirement 3. Protect stored data.
  No data from remote computers is stored on LogMeIn servers (only session data is stored). All
  data in transit is protected by end-to-end 256-bit SSL encryption.

• Requirement 4. Encrypt transmission of cardholder data and sensitive information across
  public networks.
  All LogMeIn Central remote sessions are protected with end-to-end 256-bit SSL encryption, the
  de-facto standard for secure communications over the Internet. This encryption method has
  been endorsed by Visa, MasterCard and American Express—the same coalition that came
  together to create the PCI compliance standards. The SSL implementation used by LogMeIn
  Central is OpenSSL.

VULNERABILITY MANAGEMENT

• Requirement 5. Protect against malware; use and regularly update antivirus software.
  LogMeIn cannot be responsible for the antivirus practices of its user base, but does actively
  protect and secure its own systems and servers. Moreover, Central provides tools that help
  users monitor antivirus software on host computers.

• Requirement 6. Develop and maintain secure systems and applications.
  LogMeIn deploys systems with hardened operating systems and maintains current security
  patch levels on exposed systems.

ACCESS CONTROLS

• Requirement 7. Restrict access to data by business need-to-know.
  LogMeIn Central has a number of features in place that restrict access to data, including:
  ○ The ability to limit access to computers to specific users in your Central organization.
  ○ The ability to only allow remote access when a user is present at the host computer to
    accept and authorize the session (known as “Request consent from host side user”).
  ○ Administrators can set granular permissions for users in their Central organization,
    authorizing individuals or groups to use only specified features and functions.

• Requirement 8. Assign a unique ID to each person with computer access.
  Each administrator and user has a unique password for logging in to LogMeIn Central, and
  specific permissions are attached to that user.
  ○ Users must log onto their PCs on your domain and then log into LogMeIn Central using
    a password only they know.
LogMeIn requires a unique user name and password for each account holder and user. Additionally, users can leverage advanced security features to make their account more secure:

- Two-step verification
- Emailed security code
- Printed security code
- QR Code login

Administrators can revoke access for any terminated users

Administrator can set up authentication attack blockers to block out users after multiple unsuccessful login attempts.

- **Requirement 9. Restrict physical access to cardholder data.**
  Administrators can create IP Filter Profiles to allow or deny connections to host computers from specific IP addresses.
  - Remember: No cardholder data is held in our datacenters.

**REGULARLY MONITOR AND TEST NETWORKS**

- **Requirement 10. Track and monitor all access to network resources and cardholder data.**
  Any remote support solution must place strong emphasis on accountability. LogMeIn Central offers extensive reports, including the following: Account activity and usage, Hardware and software inventory, User and computer access rights.

- **Requirement 11. Regularly test security systems and processes.**
  Anyone using Central can leverage its remote access features to support their efforts to comply with this requirement. LogMeIn itself is committed to ongoing security, and continually reviews its own software, policies and data centers for security.

**MAINTAIN AN INFORMATION SECURITY POLICY**

- **Requirement 12. Maintain a policy that addresses information security.**
  - LogMeIn enables automatic disconnect of remote sessions. The default is set to 30 minutes.
  - Regarding requirement 12.3.9 (Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use): It is each Central subscriber’s responsibility to implement a remote access usage policy based in line with their PCI initiative. LogMeIn does not negatively impact the ability to meet this requirement.

**Additional Resources**

- Securing your LogMeIn Remote Control Environment: [PDF](#) or [HTML](#)
- LogMeIn Security: An In-Depth Look: [PDF](#)
- PCI Security Standards Council [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)