SECURITY PRACTICES OVERVIEW

2018 | Helcim Inc.

Our Security at a Glance

› PCI-DSS Level 1 compliant service provider with Visa, MC, Amex & Discover.

› Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) on all servers and firewalls.

› All company workstations and laptops require full-disk encryption.

› Strict user access controls, and enforcement of multi-factor authentication.

› Redundant hardware, data centers and daily off-site backups.

› AES256 encryption on all sensitive merchant and cardholder data.

› In-house development team trained on secure software development standards.

› Ongoing penetration testing and vulnerability scanning of environments and code.

› Trusted by thousands of merchants, including Fortune 500 enterprises.

About Helcim Inc.

Helcim is a payments+ company that lets businesses accept credit cards and run their entire merchant operations from a cloud-based, all-in-one merchant platform. From retail to service to e-commerce, Helcim merchants have access to an amazing set of tools to build their business.

Website https://www.helcim.com/

Email help@helcim.com

Telephone +1 (877) 643-5246

Calgary Head Office

5720 4th Street SE
Suite 320
Calgary, AB, Canada
T2H 1K7

Seattle Office

701 5th Avenue
Suite 4200
Seattle, WA, USA
98104

Summary

Helcim is committed to helping our merchants stay secure and compliant. We undergo rigorous audits, testing, and inspections to maintain the highest level of compliance in the industry. Our talented team of in-house developers, systems engineers and security administrators work to maintain strict security standards at all times.

This document outlines the steps Helcim takes to secure all merchant and customer data, software and applications, and physical hardware that we utilize to operate our business and secure yours.

Network Setup

Helcim's systems and security team takes a proactive approach to protect all data that is housed on and moves through our servers. Our firewalls and servers have both Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS) to evaluate incoming traffic and protect against harmful actions.

Our systems and security team perform regular updates to all company systems and can respond quickly to any major vulnerability by applying patches. The company's servers are also hardened using recommended guidelines to increase system security.

Server Hardening

Following industry guidelines, including National Institute of Standards and Technology (NIST), Helcim develops server and appliance hardening processes for each type of server, appliance, firewall and services deployed in our environment.

By implementing hardening best practices, hardware and software is more secure than when left to default standards. Hardening includes limiting access and eliminating known security holes.

Firewalls and IDS / IPS

Helcim's security system includes firewalls with both an Intrusion Detection System and an Intrusion Prevention System to protect against both active and passive threats. The systems monitor network traffic and look for any unusual behavior, abnormal traffic, or malicious coding and prevent exploitation of any potential vulnerabilities.

In addition to inclusion on Helcim's firewalls, all servers in our environment are also required to have IDS and IPS installed locally to detect and warn system administrators of unusual activity and to inspect attack data if it occurs. If suspicious activity is identified, the IPS will take the corresponding action required to protect the servers. Alerts are also sent to Helcim's security team for ongoing monitoring and review.

System Updates

The server and network appliances are regularly updated to ensure all software is up to date. If a major vulnerability is discovered, patches are applied immediately by Helcim's system and security team. Per our compliance, all updates are logged as part of our change-control policies.

Data Management

By trusting Helcim with sensitive data storage, our merchants are able to shift large portions of their data security and compliance scopes away from their business. This is accomplished using a variety of available tools, including our Card Vault, Helcim.js, hosted payment pages and developer API functionality.

Thousands of merchants trust Helcim to secure the payment and personal information of their customers, removing their own systems from scope. Helcim protects this data by keeping it separate from web servers.

Daily Backups

Databases are automatically backed up daily to protect merchants against lost, corrupted, stolen or destroyed data. Backups are performed between data centers, as well as offsite. This is part of our commitment to ensuring ongoing business continuity.

Data Storage

Transaction, cardholder and merchant data is stored on segregated pools of self-replicating database clusters. Our database server architecture ensures uptime and load balancing of database servers. Sensitive cardholder data is stored for up to 24 months of inactivity. Data between merchants is logically separated and inaccessible. All merchant data access by authorized Helcim staff is logged.

Data from customers and merchants is stored separately from the Helcim web servers. Keeping the databases separate from the web servers provides an additional layer of security and is a practice is required as part of our PCI-DSS compliance requirements.

Hard Drive Disposal

Our company follows best practices when destroying hard drives. Retired hard drives are wiped to render all data unreadable. As an added security step, the hard drives are also physically destroyed using secure practices.

Authentication & Access Controls

To protect Helcim's data and systems, our company implements strong access controls.

This includes the requirement for VPN to all internal systems, controlled definitions of user roles, and the requirement of multi-factor authentication. Local and centralized logging ensures that an audit trail of all network access and activity is available.

Internal office networks are kept separate from Helcim platform environments, and do not feature any wireless accessibility. Internal systems are also only accessible by employees who are locally and physically connected to the network. Virtual Private Networks (VPNs) provide secure remote access to a limited number of systems, while protecting company data and servers.

Multi-Factor Authentication

Helcim requires all staff to use multi-factor authentication when accessing Helcim systems. Multi-factor authentication is also available to our merchants based on their compliance and internal requirements.

Physical Data Access

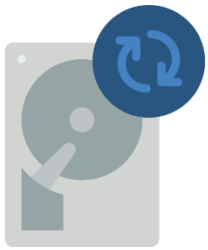
Data centers have 24/7 onsite security. Physical access to environments are limited to key personnel, with multi-factor authentication, including biometrics.

Deny-All Policies

Firewalls deployed to our server environments have deny-all policies enabled by default. All connections for inbound and outbound traffic must be approved and added as new firewall rules.

Password Protection

Strict password standards are in place to ensure security at Helcim. Passwords for all users are required to be complex in nature and changed regularly. Software settings applied by Helcim ensure that these requirements are enforced at all times. Passwords are also hashed and salted and are software-enforced to be changed frequently. Logs of previous hashed passwords are stored, preventing users from re-using their 13 previous passwords.



Encryption

Helcim encrypts all sensitive merchant data and cardholder data using the Advanced Encryption Standard (AES) with 256-bit keys. To meet PCI compliance requirements, all sensitive cardholder fields, including name, card numbers, expiry dates and cardholder addresses (for AVS) are encrypted when stored. Helcim does not store card-verification-values (CVV), PIN, EMV, nor mag data.

Key Management

Cryptographic keys are split and stored on FIPS compliant hardware. When in production, keys are never stored on physical drives, but instead reside in secured memory to prevent unwanted physical and logical access. Keys are never stored as part of software source code.

Dedicated Hardware

Encryptions and decryptions are not handled directly by web servers. Instead, encrypt and decrypt functions are performed by segregated hardware in separate network zones from web servers.

Information in Transit

To protect data in transit, Helcim requires TLS version 1.2 connections to its servers, using a limited set of strong cyphers. This ensures that data is encrypted in transit and maintains its integrity. Outdated standards including SSLv3, TLSv1.0, TLSv1.1 are no longer active on our systems.

Workstation Encryption

Helcim goes above and beyond compliance requirements and requires all staff workstations, including laptops, to enable full-disk encryption. This ensures that in the event of lost or stolen hardware, hard drives will remain unreadable.

Compliance

Helcim is a Level 1 PCI-DSS compliant service provider, which means we undergo rigorous on-site audits, vulnerability scanning, penetration testing, and inspections to maintain the highest level of compliance with the Payment Card Industry Data Security Standard (PCI-DSS). Security practices from the National Institute of Standards and Technology (NIST) are also followed to maintain the highest level of data security compliance.

Documentation & Business Continuity

Helcim maintains an information security management system (ISMS) and extensive documentation outlining all processes and procedures. These documents are reviewed yearly by our Qualified Security Assessor (QSA) to ensure that all documentation and procedures meet compliance requirements.

Helcim also maintains business continuity and emergency response plans to deal with incidents and disaster events. These plans are kept up-to-date and appropriate staff members are trained on their implementations. Helcim also holds cyber, intrusion and E&O insurance policies to ensure that adequate financial resources are available in such events.

PCI-DSS Requirements

As per our compliance requirements, our company:

- Protects our networks with firewalls.
- Hardens systems and requires strong passwords and multi-factor access.
- Encrypts and protects stored cardholder data.
- Encrypts the transmission of cardholder data across open, public networks.
- Uses anti-virus software across all servers and workstations.
- Regularly updates and patches systems.
- Restricts access to cardholder data by business need-to-know.
- Assigns a unique ID to all employees who have computer access and maintains strict user access controls.
- Restricts access to Helcim's physical workplace offices and data centers.
- Implements centralized logging and log management across all devices and networks.
- Conducts vulnerability scans and penetration tests with certified vendors.
- Maintains documentation, change controls and performs risks assessments throughout our organization and processes.

Service Uptime

Helcim devotes significant resources to ensure the most uptime possible for our networks and merchants. These safeguards include redundant data centers with 6 upstream fiber internet providers as well as backup power generation and dual-path power distribution systems. Data centers are in unmarked, low-risk geographic locations.

Our dedication to maximizing uptime lead to an 99.948% uptime in 2016 and 99.992% uptime in 2017.

Multiple Data Centers

Helcim has both a primary and a backup data center to protect merchant data. The backup data center is configured for hot-data replication of the primary data center, replicating data in real-time. In the event of an incident impacting our primary data center, Helcim can move all services and data processing operations to the backup environment with minimal downtime and data impact.

DDOS Protection

Helcim also employs DDOS mitigation techniques to reduce potential downtime from distributed denial of service attacks. This includes DDOS mitigation services from upstream providers.

Mirrored Environment

Our network environment features mirrored hardware, with at least one pair of servers, firewalls, and network appliances for each required task. Configured for high-availability, this setup ensures that the failure of any single-device cannot cause a service interruption. Hardware zones typically feature numerous servers arranged in clusters to ensure work load distribution and uptime.

Back Up Hardware

Helcim stocks additional units of all network devices, appliances and servers employed in our environments. This allows our systems team to quickly replace failed hardware without having to wait for manufacturer replacement.

SaaS Development

Helcim employs a talented team of in-house programmers who develop all our systems and applications. Building applications in-house ensures that they are built to Helcim's strict security standards and allows our team to work closely with QAs and security staff to identify and correct any potential issues before they become a problem.

Secure Coding Practices

All applications are developed in-house, and Helcim developers are trained and regularly updated on the latest secure coding guidelines, including those set by the Open Web Application Security Project (OWASP). Internal development allows our company to maintain tight controls over coding standards, source codes and deployment cycles.

Penetration Testing

Helcim completes regular penetration testing to attempt to identify potential network, system and application vulnerabilities and determine whether unauthorized access or other malicious activity is possible. Penetration testing is performed both internally by Helcim security team, and by 3rd party professionals. Vulnerabilities are addressed immediately by both our systems staff and our development teams.

Vulnerability Scanning

Regular vulnerability scanning of Helcim's networks and applications identifies potential security concerns. Per compliance requirements, Helcim performs both internal and external network scans, with external scans performed by Approved Scanning Vendors (ASV).