Maple Security & Privacy Overview

Last update: February 2021

Table of Contents

Organizational Security

Information Security Program
Maple has established and implemented a comprehensive set of information security policies, processes and standards. Our information security program is aligned with the ISO 27001:2013 standard, NIST Special Publication (SP) 800 series, and AICPA Trust Service Principles.

Security Governance
Security is represented at the highest level of the company. The VP, Data & Security reports to the Chief Operating Officer (COO) and is a member of the Senior Leadership Team. Our policies and standards are approved by management, available to all Maple employees, and reviewed annually.

Platform Infrastructure

Data Center Security
Maple outsources the hosting of its infrastructure to the world’s leading cloud infrastructure provider, Amazon Web Services (AWS). AWS regularly achieves third-party validation for thousands of global compliance requirements, including PCI-DSS, HIPAA, HITECH, ISO 27001, SOC framework.

AWS infrastructure services include back-up power, HVAC systems, and fire suppression equipment to protect servers and data. On-site security features include security guards, fencing, security feeds, intrusion detection technology, and other security measures.

Maple uses AWS resources located in the Canada (Central) Region. Maple does not host any production software systems within its corporate offices.

For more information about AWS, visit these websites:

- AWS Cloud Security - https://aws.amazon.com/security/
- AWS Cloud Compliance - https://aws.amazon.com/compliance/
- AWS Data Centers - https://aws.amazon.com/compliance/data-center/

Network Security
Maple divides its systems into separate environments to better protect sensitive data. Maple's production environment is segregated from the development environment and Maple's office network. Access to the Maple office network does not grant a user with elevated access to any system environments.

AWS security groups restrict all inbound traffic in every environment to the essential protocols and ports. AWS activity monitors the network perimeter and provides mitigations against distributed denial of service (DDoS) attacks.

Configuration Management

All infrastructure resources in the production environment are provisioned and configured using an "infrastructure-as-code" approach. All server instances use a standard image that is hardened to remove unnecessary packages, disable password authentication, etc. Additionally, host-based intrusion detection software is installed and centrally monitored.

Infrastructure Access

Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. Administrative access to the production environment is restricted to authorized employees and requires SSH.

Application Security

Account Security

Passwords are salted and hashed using bcrypt before being stored. For additional protection, users can enable two-factor authentication (2FA) on their account.

Antivirus

All files uploaded by customers and providers are automatically scanned for viruses before being allowed into the database. Virus signatures are automatically updated.

Change Management

Maple has a formal change management process. All changes are tracked and approved. A change is reviewed before being deployed into a staging environment for further testing. Once further testing is complete, the change is deployed to the production environment.

Customer Data Protection

Encryption

External and internal network traffic is encrypted using TLS. External network traffic is encrypted with TLS 1.2. Our servers enforce HTTP Strict Transport Security (HSTS).

Data at rest is encrypted with AES-256. This includes all file volumes, databases, snapshots, backups, and logs.

Payment Card Information Protection

Maple does not store, process or collect credit card information submitted to us by customers. Instead, we use Stripe, a certified PCI Level 1 Service Provider that has been audited by an independent PCI Qualified Security Assessor (QSA). This is the most stringent level of certification available in the payments industry.

Maple Employee Access

Maple adheres to the principle of least privilege for all systems. Employees and contractors receive access to resources based on their role. Where possible, the accounts will be provisioned automatically by Maple's access management tools. Authorized employees must use two-factor authentication and a unique and complex password to access Maple's administrative console. User access to the production environment is reviewed quarterly. Access is revoked immediately upon employee termination.

Workstation Security

All Maple issued laptops are hardened according to a documented configuration standard. The standard disables unnecessary functionality and enables features, including but not limited to: full disk encryption, screen locking, firewall, endpoint protection, and automatic security updates.

Privacy

Maintaining the privacy of our customers' information is a key objective of Maple's security program. We have implemented physical, technological, and organizational safeguards to restrict access to personally identifiable information (PII) and personal health information (PHI). For more details, review the Privacy Policy at https://www.getmaple.ca/privacy/.

System Operations

System Monitoring

Maple actively monitors the production environment with a variety of tools. System logs are automatically shipped and ingested into a security information and event management (SIEM) tool. An infrastructure and application performance monitoring (APM) tool collects system metrics. Application errors are captured in real-time using an error monitoring and reporting tool. All of these tools have rules configured to issue alerts based on defined criteria.

Vulnerability Management

Maple's source code and third-party libraries are automatically scanned for known vulnerabilities when changes are made. Every week, a third-party service provider scans Maple's production environment for vulnerabilities.

Penetration Testing

Twice a year, Maple engages a third-party to perform a network vulnerability assessment and web application penetration testing.

Incident Management

Maple has established a security incident response plan and team (SIRT). The SIRT investigates and responds to security events reported by internal and external sources. Customers can report events to Maple using the real-time chat on the mobile app or website or by email to support@getmaple.ca.

Business Continuity & Disaster Recovery

Recovery Planning
Maple maintains a formal business continuity plan that is regularly reviewed and updated. We test our plan annually.

Customer Data Backups
Maple uses AWS S3 and RDS services to durably store customer data. RDS performs automatic, continuous backups of customer data to S3. All objects in S3 are encrypted at rest and stored redundantly across multiple availability zones.

Vendor Management

Vetting Process
All prospective third-party critical vendors undergo a security and privacy risk assessment before contracting with Maple. We do not proceed with vendors who do not meet our requirements.

Ongoing Monitoring
Annually, Maple reviews vendors for security, privacy, business continuity, and contractual performance concerns.

Offboarding
Maple ensures that data is returned or deleted at the end of a vendor relationship.

Third-Party Audits, Certifications, and Assessments

SOC 2
Maple has obtained a SOC 2 Type 1 audit report for the Trust Services Principles of Security. The independent audit was conducted by Richter LLP, one of Canada's largest independent accounting, business advisory, and consulting firms.

Top Tier Infrastructure Provider
The Maple platform is hosted with Amazon Web Services (AWS) in the Canada (Central) region. AWS regularly achieves third-party validation for thousands of global compliance requirements, including PCI-DSS, HIPAA, HITECH, ISO 27001, SOC framework.

Certified PCI Level 1 Service Provider
Maple relies on Stripe to store credit card information and process payments. Stripe is a certified PCI Level 1 Service Provider that has been audited by an independent PCI Qualified Security Assessor (QSA). This is the most stringent level of certification available in the payments industry.

Privacy Assessment
Since the beginning, Maple has undergone rigorous privacy reviews and consultations. This has included an assessment from leading health privacy lawyer, Bonnie Freedman of Borden Ladner Gervais LLP, as well as consultation with Ann Cavoukian, the former Ontario Information and Privacy Commissioner.

Compliance

Maple complies with applicable regulatory and legal requirements. Maple staff are obligated to protect information by adhering to our policies, practices and applicable laws. All patient health data, personal information and data collected during patient/provider interactions are kept and stored within Canada to comply with privacy legislation.