



Shopify Inc.

System and Organization Controls (SOC) 3 Report

Shopify's Ecommerce Platform for the Period December 1, 2018 to September 30, 2019



Shopify's Ecommerce Platform System

Contents

SECTION I – Shopify's Management Assertion.....	3
SECTION II – Report of Independent Accountants	6
ATTACHMENT A – Description of Shopify's Ecommerce Platform System	9
ATTACHMENT B – Description of Criteria, Controls, Tests, and Results of Tests	21

SECTION I – Shopify’s Management Assertion

Shopify's Management Assertion

We, as management of, Shopify are responsible for:

- Identifying the Shopify Ecommerce Platform (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

The Shopify Ecommerce Platform uses the following independent subservice organizations (collectively "Sub-service Organizations");

Infrastructure as a Service (IaaS) providers

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

Data Center Hosting providers (*until June 2019*)

- RagingWire
- ServerCentral

Content Delivery Network (CDN) provider (*from June 2019*)

- Cloudflare

The Description (Attachment A) includes only the controls of Shopify and excludes controls of the Sub-service Organizations, however it does present the types of controls Shopify assumes have been implemented, suitably designed, and operating effectively at the Sub-service Organizations. The Description also indicates that certain trust services criteria specified therein can be met only if the Sub-service Organizations' controls assumed in the design of Shopify's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the Sub-service Organizations.

Shopify performs annual due diligence procedures of the Subservice Organizations and based on the procedures performed, nothing has been identified that prevents us from achieving its specified service commitments.

In designing the controls over the System we determined that certain requirements of the Criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period December 1, 2018 to September 30, 2019.



150 ELGIN ST., 8th Floor
OTTAWA, ONTARIO K2P 1L4

T 1.613.241.2828

F 1.877.350.0829

WWW.SHOPIFY.COM

We assert that the controls over the System were effective throughout the period December 1, 2018 to September 30, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.



SECTION II – Report of Independent Accountants

Report of Independent Accountants

To the Management of Shopify, Inc.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Shopify Ecommerce Platform Based on the Trust Services Criteria for Security and Availability" (Assertion), that Shopify's controls over the Shopify Ecommerce Platform (System) were effective throughout the period December 1, 2018 to September 30, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security and availability (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management's Responsibilities

Shopify's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Shopify's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Shopify's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Shopify uses Amazon Web Services (AWS) and Google Cloud Platform to provide Infrastructure as a Service (IaaS) services. Through 30 June 2019, Shopify used RagingWire and ServerCentral to provide data center hosting services. From 30 June 2019, Shopify used Cloudflare for content delivery

networking services. The organizations providing infrastructure, data center hosting and content delivery networking services to Shopify are collectively referred to as “Sub-service Organizations”. The Description of the boundaries of the System (Attachment A) indicates that Shopify’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if the Sub-service Organizations’ controls, assumed in the design of Shopify’s controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents Shopify’s system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at the Sub-service organizations. Our examination did not extend to the services provided by the sub-service Organizations and we have not evaluated whether the controls management assumes have been implemented at the Sub-service Organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period December 1, 2018 to September 30, 2019.

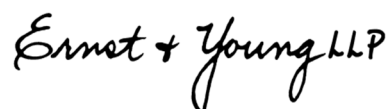
The description of the boundaries of the System also indicates that that Shopify’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Shopify’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Shopify’s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Shopify’s controls over the system were effective throughout the period December 1, 2018 to September 30, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, and if the Sub-service Organizations and user entities applied the controls assumed in the design of Shopify’s controls throughout the period December 1, 2018 to September 30, 2019.



July 10, 2020
San Francisco, CA

ATTACHMENT A – Description of Shopify's Ecommerce Platform System



Shopify overview

Shopify is a leading global commerce company, providing trusted tools to start, grow, market, and manage a retail business of any size. Shopify makes commerce better for everyone with a platform and services that are engineered for reliability, while delivering a better shopping experience for consumers everywhere.

Shopify's core Software as a Service (SaaS) offering is a cloud-hosted online storefront, a cloud-hosted checkout process, and a back-end administration portal for merchants to manage customers, products, orders, and other standard business operations, as well as Application Programming Interfaces (APIs) to support these processes.

Scope

Scope inclusions

The scope of this report *includes* systems required to provide the following functionality:

For all merchants:

Store: Create an online store that can display web pages to customers and potential customers.

Admin access: Connect to the store admin using secure transmission.

Accounts: Manage store staff accounts and permissions.

Products: Configure product descriptions, prices, discounts, taxes, shipping rates, and inventory.

Orders: View or modify details of completed orders, including fulfillment status, and related financial transactions.

Customers: View, modify, or delete customer records.

Shopify Payments: View financial transactions with Shopify Payments.

Gift cards: Configure gift cards (if on an appropriate plan).

Support: Contact 24/7 customer support for assistance.

For Shopify Plus merchants (opt-in applications):

Script Editor: Create personalized checkout experiences and promotions using Shopify Scripts.

Bulk Account Inviter: Onboard existing customers into a new Shopify Plus store.

Launchpad: Monitor events like sales campaigns, product releases, and content changes.

Wholesale: Sell products to wholesale customers.

Plus Merchant Onboarding: Onboard to a new Shopify Plus store with a purpose-built app.

Flow: Automate tasks and business processes.



Transporter: Bulk import information from another platform into a Shopify Plus store.

Avalara AvaTax App: Connect a Shopify Plus store to an Avalara AvaTax account.

Note: For the Shopify Plus merchant features listed above, controls were only tested from June 2019 to the end of the reporting period.

For customers:

Customer access: Connect to the online store using secure transmission.

Shopping cart: Add one or more products to a shopping cart.

Shipping: Select a shipping method.

Checkout: Complete checkout using Shopify Payments.

Scope exclusions

The scope of this report *excludes* systems required to provide the following functionality:

Store management mobile applications: Shopify store management iOS and Android applications.

Point-of-sale: Shopify POS iOS and Android applications.

Fraud analysis: Shopify's customer fraud detection tool.

Analytics: Analytics visible in Shopify Admin.

Shopify data warehouse: Tool to run Structured Query Language (SQL) queries on customer data.

Third-party payment gateways: Payment gateways other than Shopify Payments.

Domains: Purchase and management of domain records.

Shipping: Buying and printing shipping labels.

Opt-in applications: Platform applications from <https://apps.shopify.com> other than those listed in the **Scope inclusions** section under **Shopify Plus (opt-in applications)**.

Credit-card processing: Shopify's credit card processing environment (covered by PCI DSS Attestation of Compliance).

System components

Infrastructure

Shopify data processing and storage takes place in North America, in facilities operated by trusted third parties which are subject to annual review by Shopify.



Prior to June 2019, Shopify used a combination of colocation facilities for edge routing and public cloud service providers for store hosting and other services.

As of June 2019, Shopify uses a Network as a Service provider for edge routing and continues to use public cloud service providers as before.

By default, the infrastructure supporting stores is located in the United States. Shopify also has specialized Canadian infrastructure with strict Canadian localization requirements which is available on request for qualified merchants. In this environment, personally identifiable information (PII) is stored in Canada.

Routing

Default

Prior to June 2019, traffic entered Shopify's colocation data centers directly, where edge routing and load balancing took place before the requests were directed to the appropriate region in Shopify's infrastructure.

As of June 2019, an incoming web request for an online store hosted on Shopify travels over an encrypted Transmission Control Protocol (TCP) connection to the Network as a Service provider. Message bodies are decrypted when they reach the provider, re-encrypted before being forwarded, and decrypted again when they reach the appropriate region in Shopify's infrastructure.

Information is encrypted in transit using Transport Layer Security (TLS) wherever it passes over the Internet.

Canada

Infrastructure is slightly different for Shopify's Canadian geo-restricted service. Rather than going through routing in the Network as a Service provider, requests are routed directly to Shopify's Canadian-hosted infrastructure.

Software

The Shopify platform is a multi-tenant, cloud-based system that is engineered for high scalability, reliability, and performance. Shopify's software consists of a core application backed by databases that serves a storefront to customers and potential customers.

The core application makes APIs and dashboards available to store owners and staff which allows them to manage the configuration and business operations of their store in accordance with the features listed in the **Scope** section.



Data

To provide its services, Shopify collects data, primarily from Shopify merchants and merchants' customers. Merchant and customer data is encrypted at rest and sensitive information is further encrypted at the application layer.

Additional information on data collection and usage is noted in Shopify's privacy policy (<https://www.shopify.com/legal/privacy>).

Control environment

Organizational structure

Shopify maintains an organizational structure and clear lines of responsibility. Shopify's executive team sets the strategic direction for the company and works closely with the senior leadership team to establish objectives that will allow Shopify to achieve its mission to *Make commerce better for everyone*.

The Shopify Trust team is led by the VP of Security Engineering and IT. This individual is responsible for setting the security direction for the company. The Shopify Trust team's mission is to protect the trust that merchants have placed in Shopify.

In addition to security roles in Trust, other key security and operational roles at Shopify are in the following teams:

- Technology Experience (TX)
- Production Engineering
- Talent
- Legal

Hiring

Role descriptions are published in job postings on the Shopify external careers page (<https://www.shopify.com/careers>). Potential candidates are evaluated on their ability to meet the position requirements. The interview process includes members of the hiring team and relevant teams based on the position.

Shopify further screens candidates by conducting reference checks before hiring. Contractors who work for an outsourced vendor are screened in accordance with the contract Shopify holds with the vendor. For employees hired as part of an acquisition, Shopify performs due diligence on the company in preparation for the acquisition and no additional reference checks are conducted.



Board of Directors

The responsibilities of the Board of Directors are outlined in charters that are regularly reviewed by Board members and published on Shopify's website. The Board meets with Shopify's leadership regularly.

Risk assessment

Shopify has defined a risk management process drawn from a mix of standards and industry best practices. The results of the process are formally communicated to the VP of Security Engineering regularly. The VP of Security Engineering and IT is also continuously made aware of security findings, risk decisions, and actions taken. This information is communicated to senior management as deemed necessary by the VP of Security Engineering and IT.

Security assessment

Shopify security assessments generate findings that feed into the risk management process. Examples of these assessments are:

Third-party penetration test

Bug bounty program (<https://hackerone.com/shopify>)

Vulnerability assessments

Third-party security reviews

Safeguard assessments

Trust team assessment of the SOC 2 program

Other operational activities may also generate relevant security findings. These findings, along with output from the security assessment, are evaluated for risk using the risk management process.

Fraud risk assessment

Shopify conducts a regular fraud risk assessment that identifies and evaluates fraud threats to the organization.

Leadership assessment

Shopify leadership regularly assess adherence to policies, operational irregularities such as availability or security incidents, and regulatory and litigation matters.



Control activities

Policies and procedures

Shopify maintains a security policy that is reviewed regularly and approved by the VP of Security Engineering and IT. Upon hire, Shopify employees are required to review and acknowledge Shopify policies. During employment, Shopify employees are required to review and acknowledge relevant policies regularly. Employees also review and agree to the Code of Conduct regularly.

Shopify maintains security and availability response plans, IT Access Provisioning and Deprovisioning procedures, and procedures for reviewing the security of third-party software and services.

Incident management

Shopify believes that security should be a partnership between the company and merchants, which helps the company find security and availability flaws faster and shorten incident response time. Merchants' customers would report issues to the merchant, who would report them to Shopify.

Shopify's public website instructs merchants on how to report security or availability incidents (<https://www.shopify.com/security-response>), how to ask security or availability questions, and how to submit potential security or availability issues. If needed, the Shopify Support team is also available 24/7 to assist merchants with security or availability questions or issues.

If a serious security or availability issue is found, then the incident response process is activated. Incidents are tracked through resolution. When the situation warrants it, Shopify updates the public status page (<https://status.shopify.com>).

Service monitoring

Shopify maintains the security and availability of systems through automated logging, monitoring, and alerting.

Shopify forwards application and infrastructure logs to a centralized logging service for aggregation, correlation, and alerting. Logs are retained according to a defined retention schedule. Shopify also monitors production infrastructure metrics.

The logging and monitoring services are configured to generate security alerts. The alerts page an on call team member who evaluates if the alert could represent a security or availability incident. Relevant team members are on call 24/7.



Logical access control

Merchant access

When a merchant creates their Shopify store online, their store owner account is also created. Store owners can provision staff accounts, which they may set up to have only limited access to their store's data.

For Shopify Plus merchants, a Shopify Plus team member sends a sign-up link to the merchant through the Plus Merchant Onboarding app. The merchant then visits the link to complete the sign-up process in the Plus Merchant Onboarding app, which creates both their store and staff owner account.

There are two main flows for a merchant to authenticate to their account: visiting their store address directly or from <https://www.shopify.com>. In both workflows, credentials are sent over HyperText Transfer Protocol Secure (HTTPS). The Shopify application hashes the password and checks it against the stored hash. To further secure their accounts, store owners and staff should set up their accounts to use two-factor authentication (2FA).

The store owner's account and all staff accounts are terminated when a merchant closes their store. Merchants may also terminate staff accounts individually through the Shopify admin.

Shopify employee access

Default access

During onboarding, employees are provisioned with an email account and a Single Sign-On (SSO) account. Employees must authenticate with SSO to access email. 2FA is enforced on SSO accounts.

Employees access the code base using individual version control system accounts with unique usernames and passwords. Those accounts are invited to the Shopify version control system organization, which associates the version control system account with the user's email. 2FA is required on the version control system account for the invitation to be sent.

Remote access over the Internet is the primary means of default employee access, and authentication takes place using one of the following:

- SSO with 2FA
- Individual accounts with 2FA

Authorization for default access for Shopify employees occurs through identity management in Shopify's security systems. Employees belong to groups that define application-level permissions. Groups that are assigned to all employees define a set of default applications and capabilities.

Shopify removes employee access promptly following termination and according to a Shopify deprovisioning procedure.



Elevated access

Shopify restricts employee access to the production environment, and internal applications that manage production access, according to the principle of least privilege.

Shopify conducts semiannual reviews of employee access to the production environment and internal applications that manage production access.

Access to production, or applications that manage production access, is granted through one of the following mechanisms:

- Addition to an access control group
- Configuration management
- Invitation by a security system administrator

Access takes place over the Internet and authentication takes place using one of the following:

- SSO with 2FA
- Individual accounts with 2FA
- Certificate-based authentication

Authorization takes place using, one of:

- Access groups
- Cloud provider identity management
- Operating-system-based account permissions

Account termination for production environments follows the same process as default access.

In case of emergency, employees can access the network edge configuration using a dedicated emergency account. Activity on this account is monitored.

Network access

Depending on the environment, network access controls are defined per network:

- Directly in routing devices
- Security groups
- Firewall rules
- Infrastructure ingress resources

Cross environment resource access takes place over TLS.

Internal network controls are governed by:

- Use of private Internet Protocol (IP) addresses



- Application-level access permissions
- Vendor firewall rules and network policies

Application and infrastructure change management

Shopify's application and infrastructure change management process follows the principles of test-driven development, using a remote version control system.

Shopify's Development Handbook defines procedures for reviewing, deploying, and backing out changes. It also includes best practices for coding and security.

Shopify's deploy tooling provides functionality for a developer to initiate an automatic rollback to a previous deploy.

Availability

Shopify manages resources on an ongoing basis.

Shopify maintains a documented project to prepare for high load and component failure scenarios. Systems and procedures relevant to the project are tested and documentation is updated regularly.

Prior to June 2019, full images of Shopify production databases were backed up. As of June 2019, the entire disk of each database server is backed up. Backups were and are tested regularly.

Shopify's business continuity and disaster recovery planning combines capacity planning with backup recovery verification.

Information and communication

Internal communication

Shopify conducts security training for new employees. The training reinforces the commitments outlined in the security policy.

Shopify's commitments to the security and availability of the system are posted on an internal site. Shopify communicates timely updates to Shopify employees on security and availability topics, as required.

External communication

Shopify uses established communication channels to provide updates to merchants about changes that may impact the security and availability of the service.



Merchants are responsible for reviewing email communications as well as proactively reviewing Shopify's Terms of Service, Acceptable Use Policy, Privacy Policy, and website.

If merchants require additional assistance, Shopify maintains a 24/7 customer support operation (<https://help.shopify.com/questions>).

Shopify's anonymous whistleblower program is available internally and externally, and communicated through the Shopify Code of Conduct, and the Shopify Investor Relations website. Any communications to the whistleblower program are automatically sent to the Chair of the Audit Committee and to the Chief Legal Officer.

Monitoring activities

Shopify routinely monitors the performance of internal controls to verify they are appropriate for the current environment. Members of the Trust team regularly review and update control documentation, and ensure automated processes are monitoring the effectiveness of controls.

Incidents are handled by the appropriate individuals, depending on the severity, or potential severity, of the incident. Material incidents are disclosed to the executive team and the Board of Directors.

Subservice organizations

Shopify's subservice organizations include:

- **Amazon Web Services (AWS):** Infrastructure as a Service
- **Cloudflare:** Network as a service (as of June 2019)
- **Google Cloud Platform (GCP):** Infrastructure as a Service
- **RagingWire:** Colocation data center (prior to June 2019)
- **ServerCentral:** Colocation data center (prior to June 2019)

Shopify's controls were designed with the assumption that certain controls are implemented by these subservice organizations. Certain Trust services criteria can be met only if the complementary subservice organization controls, which are assumed in the design of Shopify's controls, are suitably designed and operating effectively, along with related controls at these subservice organizations.

While they were subcontracted, Shopify employees had physical access to RagingWire and ServerCentral. Access was removed when no longer needed, and regular reviews were performed to determine if physical access was appropriate.

To manage the quality of services provided by these third parties, Shopify's Trust team conducts security reviews of the subservice organizations regularly. Reviewers evaluate attestation reports or inquire about relevant security controls with the third party.



Complementary user entity controls

Shopify's Ecommerce Platform System controls were designed with the assumption that certain controls would be implemented by user entities (or "merchants"). This section describes additional controls that merchants should have in operation to complement the controls of Shopify's Ecommerce Platform System. The list of merchant control considerations presented below, and those presented with certain specified categories and criteria, do not represent a comprehensive set of all the controls that should be employed by merchants. Merchants may be required to implement additional technical or administrative controls to meet their business and legal needs.

Description	Criteria
Merchants are responsible for periodically reviewing the Terms of Service and Acceptable Use Policy web pages to evaluate if there are new or revised security or availability obligations.	CC 2.2, CC 2.3
Merchants are responsible for periodically reviewing the Shopify website to evaluate if there are new or revised security or availability commitments.	CC 2.2, CC 2.3, CC 5.3
Merchants are responsible for reviewing communications from Shopify regarding product changes and if necessary, taking steps to mitigate the effects of any changes.	CC 2.2, CC 2.3, CC 3.4
Merchants are responsible for ensuring that administration access to their stores is restricted to appropriate users and is provisioned in line with corporate policies and requirements.	CC 6.2, CC 6.3
Merchants are responsible for notifying Shopify of any unauthorized use of, and other known or suspected breach of, security related to the system.	CC 6.2, CC 6.3, CC 6.6
Merchants are responsible for ensuring that the contact information associated with their accounts is accurate and kept up to date.	CC 2.1, CC 2.3
Merchants are responsible for ensuring that their passwords are kept confidential.	CC6.1, CC 6.6
Merchants are responsible for ensuring owner and staff accounts have two-factor authentication enabled.	CC 6.6

Impact of Covid-19 (Corona Virus)

In response to the global Covid-19 pandemic and at the direction of local, state and governmental authorities in the jurisdictions in which we operate, Shopify implemented a work from home policy as of March 2020 for all non-essential employees and vendors. The architecture of our Ecommerce Platform has been designed in a manner which enables us to continue business as usual operations irrespective of the physical location of our employees.

ATTACHMENT B – Principal Service Commitments and System Requirements



Principal Service Commitments and System Requirements

Shopify designs its processes and procedures to meet its objectives for the Shopify Ecommerce Platform. Those objectives are based on the service commitments that Shopify makes to user entities (or merchants), the laws and regulations that govern the provision of the platform, and the financial, operational and compliance requirements that Shopify has established.

The platform is subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Shopify operates.

Security and Availability commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided on the Shopify website. Security and Availability commitments are standardized and include, but are not limited to, the following:

- Security principles inherent to the fundamental design of the Platform are intended to permit users to access the information and resources they need based on their role in the system while restricting them from accessing information not needed for their role.
- Availability principles inherent to the fundamental design of the Platform are designed to provide fault tolerance and sufficient resources to ensure the availability of the Platform.

Shopify establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Shopify's policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

The Platform is designed based on a shared responsibility model where both Shopify and the user entities are responsible for aspects of security, availability and confidentiality. Details of the responsibilities of user entities can be found on the Shopify website and in the customer contract.