

SOC2 System Description

Overview of operations

Company Background

Founded in [YEAR], [Company Name] is a customer's trusted partner in data security. [Company Name] is committed to protecting customers' data and ensuring privacy. [Company Name]'s security posture is built upon robust technology, industry-leading practices, and adherence to globally recognized security and privacy frameworks.

[Company Name] proactively identifies and mitigates risks, continuously enhancing security measures. This approach safeguards customers' data and helps them meet regulatory obligations effectively.

This Security Posture document provides a detailed overview of [Company Name]'s data security and privacy measures, including our commitment to risk management, best practices, and continuous improvement.

Description of Services Provided

[Company Name] has developed a cloud-hosted, information security software application ("[Product Name]") designed to help customers implement secure InfoSec practices and improve their security posture. [Company Name]'s mission is to enhance security management for Software as a Service (SaaS) companies, achieve and maintain global standards of information security compliance, and help them build trust with their customers.

Principal service commitments and system requirements

[Company Name] makes service commitments to its user organizations and has established system requirements as part of its services. Some of these commitments are principal to service performance and related to applicable trust service criteria. [Company Name] is responsible for its service commitments and system requirements and for designing and implementing controls within the system. Service commitments are documented and communicated in the Master Service Agreement and any other agreements as agreed by [Company Name] and user organizations.

[Company Name] makes the following security, availability, confidentiality, and privacy commitments to its customers:

- ✦ Production cloud infrastructure hosted within multiple geographically diverse availability zones/regions
- ✦ Encryption of data in transmission using transport layer security (TLS) or other technologies over public networks

- ◆ Maintenance of commercially reasonable administrative, technical, organizational, and physical measures to protect customer data
- ◆ Encryption of confidential data using Advanced Encryption Standard (AES)
- ◆ Data retention according to customer-defined policies
- ◆ Disaster recovery (DR) plans are tested at least annually
- ◆ PII data processing driven by contract or consent to fulfill service obligations

Components of the system used to provide the service

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The system description delineates the boundaries of the system, including the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

The infrastructure for the [Product Name] is hosted on [Cloud Provider] in [regions]. The infrastructure is designed to generate security-related audit events, which are regularly reviewed for unusual or suspicious activity.

Primary Infrastructure

Production System	Business Function Description	Platform
Containers	Serverless compute engine	[Service]
Containers	Container image management	[Service]
Storage	Object Storage	[Service]
Database	Managed SQL database service	[Service]

Database	In-memory caching service	[Service]
Networking	Isolated cloud resources	[Service]
Networking	Load balancing	[Service]
Security	Threat detection	[Service]
Security	Vulnerability management	[Service]
Security	Secrets management	[Service]
Security	Security monitoring	[Service]
Management	Activity tracking	[Service]
Management	Resource monitoring	[Service]
Cryptography	Encryption key management	[Service]
Business Applications	Email services	[Service]

Software Tools

Purpose	Software
Source code management	[Tool]
Office communication	[Tool]
Compliance monitoring	[Tool]

Customer support	[Tool]
Project management	[Tool]
Collaboration platform	[Tool]
Messaging	[Tool]
Customer Relationship Management	[Tool]

People

[Company Name]'s staff are organized into various functions, including Sales, Customer Experience, Support, Engineering, Product Management, etc. Key roles include:

Senior Management

Senior Management carries ultimate responsibility for organizational objectives. They ensure necessary resources are applied to develop capabilities for accomplishing the mission, assess risk assessment results for decision-making, and understand their role in effective risk management.

Information Security Officer

The Information Security Officer (ISO) oversees the information security program, identifying risks, threats, and vulnerabilities, and implementing controls to mitigate them. They report residual risks to Senior Management.

Privacy Officer

The Privacy Officer (PO) ensures compliance with data protection laws, oversees data protection impact assessments, employee training, and collaborates with supervisory authorities.

Compliance Program Manager

The Compliance Program Manager (CPM) ensures the smooth operation of the Information Security Program and oversees the execution of tasks for maintaining information security controls across all departments.

System Users

Staff members using IT systems are expected to adhere to policies, guidelines, and rules of behavior to reduce risk and safeguard IT resources. All staff with access to IT resources receive annual security awareness training.

Procedures

Formal policies and procedures have been established, covering:

- ✦ Acceptable Usage
- ✦ Asset Management
- ✦ Business Continuity
- ✦ Cloud Security
- ✦ Code of Business Conduct
- ✦ Network Security
- ✦ Compliance
- ✦ Data Classification
- ✦ Data Protection
- ✦ Data Retention
- ✦ Disaster Recovery
- ✦ Encryption
- ✦ Endpoint Security
- ✦ HR Security
- ✦ Incident Management
- ✦ Information Security
- ✦ Media Disposal
- ✦ Operations Security
- ✦ Physical & Environmental Security
- ✦ Privacy by Design
- ✦ Risk Management
- ✦ System Acquisition and Development Lifecycle
- ✦ Vendor Management

All policies are available to staff through internal systems, providing clear guidance on roles and responsibilities. Staff members acknowledge understanding of these policies upon hiring and annually thereafter.

The company provides information to clients and staff members on reporting failures, incidents, concerns, or complaints related to services or systems.

HR and Training

Job descriptions define necessary skills and responsibilities. Candidates are interviewed to assess qualifications and undergo background checks. Employees sign acknowledgments of the Code of Conduct and information security policies. Access requests are submitted through designated channels and reviewed based on employee roles. Security awareness training is required for new hires and annually thereafter.

Access Management

The platform employs role-based security architecture requiring user identification and authentication. Access to critical systems follows least privilege principles and is revoked within three business days after employment termination. The Information Security Officer conducts annual access reviews.

Change Management

A documented Operations Security policy guides application and infrastructure changes. Changes are initiated by authorized staff, managed through version control systems, and require peer review. Production infrastructure changes are restricted to authorized personnel and logged.

Data Backup and Disaster Recovery

The Operations Security Policy governs backup procedures. Automated database backups occur daily and are retained for seven days. Backups are tested annually. Business Continuity & Disaster Recovery Policies establish procedures for continuing operations during disruptions or security incidents.

Endpoint Security

Endpoints are managed using centralized Mobile Media Management (MDM) with secure configurations, application control, inventory and patch management, full disk encryption, and host-based antivirus.

Incident Response

Staff and clients can report incidents through established channels. Staff acknowledge incident management policies and their responsibilities. Senior management reviews high-severity security incidents annually.

Privacy

The company maintains a privacy program for managing external privacy requests in compliance with applicable requirements. The privacy policy covers information collection, usage, legal basis, international transfer, data security, retention, data subject rights, and more.

System Monitoring

The company leverages managed services for threat detection, logging, and alert generation. Infrastructure logs are centrally collected for analysis and correlation.

Vendor Management

The company assesses vendor risks through due diligence during onboarding and annual reviews for critical vendors. Security compliance is verified through assessment reports or periodic meetings.

Data

The following table describes information used and supported by the system:

Data Description	Data Reporting	Classification
Customer Data	Available to customers via a web application	Customer Confidential
Application and error logs	User activity and error details for investigation	Company Confidential and Personal Data
User profile data	Individual account information and access rights	Company Confidential and Personal Data

All data is classified according to the Data Classification Policy into the following categories:

- Customer confidential
- Company Confidential
- Company Internal
- Private
- Public

All customer data is treated as confidential with access limited by job function. Storage and transmission use industry-standard encryption, and data is regularly backed up.

Significant Changes During the Review Period

[Describe any significant changes that affected the system during the review period, or state that there were none.]

Subservice Organizations

The Company utilizes services from [Cloud Provider(s)] for infrastructure and database hosting. These providers are responsible for operating, managing, and controlling components from the host operating system and virtualization layer down to physical security and environmental controls. They are examined annually through review of their SOC 2 reports.

This report includes only the controls of [Company Name] and not those implemented at subservice organizations. The subservice organizations are expected to implement the following controls:

Control Activity	Applicable Trust Services Criteria
Managing logical access to underlying network, virtualization, and storage	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8
Restricting physical access to data centers and systems	CC6.4
Managing incidents impacting underlying systems	CC7.1, CC7.2, CC7.3, CC7.4, CC7.5

Managing changes to underlying systems	CC8.1
Implementing environmental security safeguards	A1.2

Control environment

Integrity and Ethical Values

The company has implemented controls to incorporate ethical values:

- ✦ Documented Code of Business Conduct communicating values and standards
- ✦ Required acknowledgment of policies and procedures
- ✦ Background checks for new employees

Board of Directors Oversight

Controls are significantly influenced by senior executive management. The management team meets periodically to oversee operations and discuss issues.

Organizational Structure

The CEO reviews the Organizational Chart annually. The structure defines authorities, facilitates information flow, and establishes responsibilities for achieving objectives.

Commitment to Competence

The company defines competence as knowledge and skills necessary to accomplish tasks. Controls include:

- ✦ Defined roles and responsibilities are reviewed annually
- ✦ Annual Security Awareness Training
- ✦ Performance reviews
- ✦ Competence evaluation during hiring

Accountability

Management philosophy encompasses risk monitoring, information processing, accounting functions, and personnel management.

Risk assessment

The risk assessment process identifies and manages risks affecting service reliability. Management identifies risks in products and services, with each risk receiving a score based on likelihood and potential impact. Risks and mitigation decisions are mapped to controls.

The Risk Assessment and Management Policy outlines processes for identifying, assessing, and mitigating risks. Principles include:

- ◆ Senior management commitment
- ◆ Staff involvement and cooperation
- ◆ Systematic risk identification
- ◆ Thorough risk analysis
- ◆ Strategic treatment of risks
- ◆ Communication of risks to management
- ◆ Encouraging staff to report risks

The program applies to all systems and data, evaluating infrastructure, business/IT practices, procedures, and physical spaces as needed.

Trust services criteria and related control activities

Integration with Risk Assessment

The company identifies specific risks to service commitments and designs controls to address them. Management performs annual Risk Assessment Exercises to identify and evaluate risks, impacts, likelihood, severity, and mitigating actions.

Information and communication systems

Internal Communications

The company establishes behavioral standards through its Code of Business Conduct. Information security policy provides guidance on reporting incidents, which are managed through a monitored email box.

External Communications

Information about the company and its services is available on its website.

Monitoring

Ongoing Monitoring

The Engineering Department continuously monitors system health and is alerted to problems. On-call staff respond to security, confidentiality, or availability issues. Incidents are documented and discussed to improve response. Third-party penetration tests regularly test application security.

Separate Evaluations

The company has implemented a compliance program to evaluate control activities over time. Assessment methodology includes structured inquiry, observation, inspection, and sample testing. Results are documented and communicated to management and business owners.

Subservice Organization Monitoring

The company annually reviews subservice organization assessment reports or security questionnaires to evaluate relevant controls.

System Incident Disclosures

[Document any system incidents that occurred during the review period, or state that none occurred]

Evaluating and Communicating Deficiencies

Protocols ensure control deficiencies are reported to responsible individuals. Management evaluates deficiencies and decides on corrective actions based on specific circumstances.

Complementary controls at user entities

The company's services assume certain controls will be implemented by user entities. User entities should implement internal controls to complement the company's procedures. Recommended complementary user entity controls include:

Control Responsibilities	Related Trust Services Criteria
Managing platform accounts and security configurations	CC5.1, CC5.2, CC5.3, CC6.1
Appointing administrators for account access	CC6.2, CC6.3
Securing endpoints and preventing data exfiltration	CC6.7
Communicating security issues and incidents	CC7.2, CC7.3, CC7.4
Managing user and organization data	CC8.1
Meeting data controller requirements for PII	P1.1, P2.1, P3.2

User entities' auditors should exercise judgment in selecting and reviewing these complementary controls as they represent only part of the control considerations at user entities' locations.

About Sprinto

Thousands of ambitious tech companies trust Sprinto to streamline their GRC program, automate management, and maintain security best practices. Sprinto supports over 20 security standards, including SOC 2, ISO 27001, GDPR, HIPAA, and PCI-DSS, as well as custom frameworks. Featuring a smart, adaptive and scalable architecture, Sprinto ensures security best practices without getting in the way of your growth ambitions.

For more information visit sprinto.com

[View Sprinto Trust Center](#) ↗



Get in touch

 sales@sprinto.com  support@sprinto.com

© Sprinto 2025 All Rights Reserved. THIS DOCUMENT HAS BEEN PREPARED FOR GENERAL INFORMATIONAL PURPOSES ONLY. IT IS PROVIDED IN GOOD FAITH, HOWEVER, WE MAKE NO REPRESENTATION OR WARRANTY INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, COMPLETENESS, OR ACCURACY. THE INFORMATION PROVIDED IN THIS DOCUMENT IS ONLY ILLUSTRATIVE AND DOES NOT DIRECTLY OR INDIRECTLY CREATE ANY CONTRACTUAL OBLIGATIONS. THIS DOCUMENT SHALL NOT BE DISCLOSED TO ANY THIRD PARTY IN ANY FORM OR BY ANY MEANS, ORALLY OR IN WRITING, FOR ANY PURPOSE, WITHOUT OUR PRIOR WRITTEN CONSENT. WE RESERVE THE RIGHT TO CHANGE THE CONTENTS OF THIS DOCUMENT, WITHOUT NOTICE. UNDER NO CIRCUMSTANCE SHALL WE BE LIABLE FOR ANY LOSS OR DAMAGE INCURRED BY ANY PARTY IN CONNECTION WITH THE USE OR RELIANCE OF INFORMATION PROVIDED IN THIS DOCUMENT.