# SOC 2 Readiness report for AI Health Studio LLC

## Generated on 03 November 2026

## Report summary

This report provides a summary of AI Health Studio LLC's readiness posture for SOC 2 compliance as of 3rd November 2026. Sprinto continuously monitors the security and readiness posture of AI Health Studio LLC to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. Below is a list of controls implemented by the organization to meet the compliance requirements. Sprinto achieves this by connecting to the systems, tools and policies of the company, and running continuous checks to determine the health of the controls.

# A1

## Additional Criteria for Availability

### A1.2

The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

MONITORED via 5 checks

Backup should be enabled on production database
Versioning should be enabled for storage assets
Operation Security Policy
Business Continuity Plan
Operations Security Procedure

Control **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

DECLARED via 1 check

Data backup restoration

---

## A1.1

The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 6 checks

Health of production infrastructure should be monitored
Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

---

## A1.3

The entity tests recovery plan procedures supporting system recovery to meet its objectives.

### INTERNAL CONTROLS AND CHECKS

**Control** **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

**Control** **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

**Control** **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

DECLARED via 1 check

Data backup restoration

**Control** **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

DECLARED via 1 check

Disaster recovery

# CC1

# Control Environment

## CC1.1

COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

MONITORED via 1 check

Code of Business Conduct Policy

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

MONITORED via 1 check

Organization of Information Security Policy

## CC1.2

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

MONITORED via 2 checks

Senior management should be assigned

Compliance Policy

DECLARED via 1 check

Management Review of Internal Audit

Control **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

MONITORED via 3 checks

Organization chart should be reviewed by senior management

HR Security Procedure

HR Security Policy

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

MONITORED via 2 checks

Risk assessment should be reviewed by senior management
Risk Assessment & Management Policy

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

## CC1.3

COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

### INTERNAL CONTROLS AND CHECKS

Control SDC 2

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

MONITORED via 5 checks

Org chart should be maintained
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 3

Entity has established procedures to communicate with staff about their roles and responsibilities.

MONITORED via 3 checks

Organization roles and JDs should be validated
HR Security Procedure
HR Security Policy

Control SDC 22

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

MONITORED via 1 check

Information security officer should be assigned

Control **SDC 154**

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

MONITORED via 1 check

Infrastructure operations person should be assigned

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

MONITORED via 2 checks

People operations person should be assigned

HR Security Policy

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

MONITORED via 3 checks

Compliance program manager should be assigned

Compliance Procedure

Compliance Policy

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

MONITORED via 2 checks

Senior management should be assigned

Compliance Policy

DECLARED via 1 check

Management Review of Internal Audit

## CC1.4

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 4**

Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.

MONITORED via 2 checks

HR Security Procedure

HR Security Policy

Control **SDC 5**

Entity has established procedures to perform security risk screening of individuals before authorizing access.

MONITORED via 2 checks

HR Security Procedure

HR Security Policy

## CC1.5

COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

MONITORED via 2 checks

Security training provider should be configured
HR Security Policy

Control **SDC 9**

Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.

MONITORED via 2 checks

HR Security Procedure
HR Security Policy

DECLARED via 1 check

Staff Performance Evaluations

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

MONITORED via 3 checks

Infosec training should be completed by onboarded staff
HR Security Procedure
HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

MONITORED via 2 checks

Infosec training should be completed by onboarded staff
Staff should periodically complete security training

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

## CC2

## Communication and Information

### CC2.1

COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

MONITORED via 3 checks

Health of production infrastructure should be monitored

Asset Management Policy

Asset Management Procedure

Control **SDC 14**

Entity displays the most current information about its services on its website, which is accessible to its customers.

MONITORED via 1 check

Product marketing website should be available

Control **SDC 382**

Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.

MONITORED via 1 check

Data Classification Policy

Control SDC 71

Entity has a documented policy outlining guidelines for the disposal and retention of information.

MONITORED via 1 check

Data Retention Policy

## CC2.2

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

### INTERNAL CONTROLS AND CHECKS

Control SDC 6

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control SDC 387

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

MONITORED via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control SDC 388

Entity documents, monitors, and retains individual training activities and records.

MONITORED via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

MONITORED via 1 check

Code of Business Conduct Policy

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

MONITORED via 1 check

Information Security Policy

## CC2.3

COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 14**

Entity displays the most current information about its services on its website, which is accessible to its customers.

MONITORED via 1 check

Product marketing website should be available

Control SDC 16

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

MONITORED via 1 check

Customer support page (Contact Us) should be available

## CC3

## Risk Assessment

### CC3.2

COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#### INTERNAL CONTROLS AND CHECKS

Control SDC 18

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control SDC 6

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

## CC3.1

COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

## CC3.3

COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

MONITORED via 1 check

Risk assessment should be conducted periodically

## CC3.4

COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

## CC4

## Monitoring Activities

### CC4.1

COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#### INTERNAL CONTROLS AND CHECKS

Control SDC 154

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

MONITORED via 1 check

Infrastructure operations person should be assigned

Control SDC 389

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

MONITORED via 2 checks

Asset Management Policy

Asset Management Procedure

DECLARED via 1 check

Internal Audit

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

MONITORED via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

DECLARED via 1 check

Internal Audit

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

MONITORED via 2 checks

Senior management should be assigned

Compliance Policy

DECLARED via 1 check

Management Review of Internal Audit

Control **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

MONITORED via 3 checks

Organization chart should be reviewed by senior management
HR Security Procedure
HR Security Policy

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

MONITORED via 2 checks

Risk assessment should be reviewed by senior management
Risk Assessment & Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

## CC4.2

COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

INTERNAL CONTROLS AND CHECKS

Control SDC 15

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

MONITORED via 1 check

Information Security Policy

Control SDC 23

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

DECLARED via 1 check

Internal Audit

Control SDC 24

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

Control SDC 25

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

MONITORED via 2 checks

Senior management should be assigned

Compliance Policy

DECLARED via 1 check

Management Review of Internal Audit

# CC5

## Control Activities

### CC5.1

COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 105**

Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.

MONITORED via 1 check

Acceptable Usage Policy

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company's control environment.

MONITORED via 1 check

Org policy should be defined

Control **SDC 32**

Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.

MONITORED via 4 checks

Org chart should be maintained
Compliance Procedure
Compliance Policy
Information Security Policy

### CC5.2

COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#### INTERNAL CONTROLS AND CHECKS

**Control** **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

DECLARED via 1 check

Internal Audit

**Control** **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

**Control** **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

MONITORED via 2 checks

Senior management should be assigned

Compliance Policy

DECLARED via 1 check

Management Review of Internal Audit

**Control** **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

MONITORED via 3 checks

Organization chart should be reviewed by senior management

HR Security Procedure

HR Security Policy

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

MONITORED via 2 checks

Risk assessment should be reviewed by senior management
Risk Assessment & Management Policy

Control **SDC 28**

Entity's Infosec officer reviews and approves the list of people with access to production console annually

MONITORED via 1 check

Access to critical systems should be reviewed

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

## CC5.3

COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

## CC6

## Logical and Physical Access Controls

### CC6.1

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

MONITORED via 3 checks

Access to critical systems should be reviewed
Access Control Procedure
Access Control Policy

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

MONITORED via 3 checks

Access Control Procedure
Acceptable Usage Policy
Access Control Policy

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control SDC 381

Entity has documented policies and procedures to manage physical and environmental security.

MONITORED via 2 checks

Physical and Environmental Security Procedure
Physical & Environmental Security Policy

## CC6.2

Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

### INTERNAL CONTROLS AND CHECKS

Control SDC 33

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control SDC 34

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 35

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

## CC6.3

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

### INTERNAL CONTROLS AND CHECKS

Control SDC 34

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 35

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure

HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

## CC6.5

The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

## CC6.6

The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

MONITORED via 7 checks

Staff devices should have disk encryption enabled
Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Acceptable Usage Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

MONITORED via 3 checks

Endpoint Security Policy
Asset Management Policy
Asset Management Procedure

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

MONITORED via 3 checks

Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Procedure

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

MONITORED via 5 checks

Staff devices should have antivirus running
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 3 checks

Staff devices should have disk encryption enabled
Staff devices should have disk encryption enabled
Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

MONITORED via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

MONITORED via 3 checks

Staff devices health should be monitored regularly
Staff devices should have screen lock enabled
Endpoint Security Policy

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

MONITORED via 4 checks

Infrastructure provider should be configured
Asset Management Policy
Network Security Procedure
Asset Management Procedure

DECLARED via 1 check

Deny by default firewall ruleset should be set up on all production hosts

Control **SDC 119**

Entity has documented guidelines to manage communications protections and network security of critical systems.

MONITORED via 2 checks

Communications & Network Security Policy
Network Security Procedure

## CC6.7

The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

MONITORED via 3 checks

Critical Infrastructure assets should be identified
Asset Management Policy
Asset Management Procedure

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

MONITORED via 1 check

Encryption Policy

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

MONITORED via 7 checks

Staff devices should have disk encryption enabled
Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure
Acceptable Usage Policy

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 3 checks

Staff devices should have disk encryption enabled
Staff devices should have disk encryption enabled
Endpoint Security Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

MONITORED via 5 checks

Data at rest should be encrypted
Data at rest should be encrypted
Encryption Policy
Asset Management Policy
Asset Management Procedure

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

MONITORED via 1 check

Production systems should be secured with HTTPS

Control **SDC 52**

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

MONITORED via 1 check

Critical Infrastructure assets should be identified

## CC6.8

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

MONITORED via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

MONITORED via 4 checks

Infrastructure provider should be configured
Asset Management Policy
Network Security Procedure
Asset Management Procedure

DECLARED via 1 check

Deny by default firewall ruleset should be set up on all production hosts

## CC7

## System Operations

### CC7.1

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

MONITORED via 1 check

Threat detection system should be enabled

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 6 checks

Health of production infrastructure should be monitored
Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

MONITORED via 3 checks

Audit logs should exist
Operation Security Policy
Operations Security Procedure

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

MONITORED via 2 checks

Vulnerability should be closed in SLA
Vulnerability scanner should be enabled

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

MONITORED via 1 check

Vulnerability should be closed in SLA

### CC7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its

objectives; anomalies are analyzed to determine whether they represent security events.

#### INTERNAL CONTROLS AND CHECKS

**Control** **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

MONITORED via 1 check

Threat detection system should be enabled

**Control** **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 6 checks

Health of production infrastructure should be monitored
Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

**Control** **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

**Control** **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

MONITORED via 3 checks

Audit logs should exist
Operation Security Policy

Operations Security Procedure

Control SDC 55

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

MONITORED via 2 checks

Vulnerability should be closed in SLA

Vulnerability scanner should be enabled

Control SDC 56

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

MONITORED via 1 check

Vulnerability should be closed in SLA

## CC7.3

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

### INTERNAL CONTROLS AND CHECKS

Control SDC 61

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

MONITORED via 1 check

Threat detection system should be enabled

Control SDC 62

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 6 checks

Health of production infrastructure should be monitored
Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

Control **SDC 63**

Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.

MONITORED via 1 check

VAPT exercise should be conducted annually

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

MONITORED via 3 checks

Audit logs should exist
Operation Security Policy
Operations Security Procedure

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

DECLARED via 1 check

Internal Audit

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

MONITORED via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

MONITORED via 2 checks

Vulnerability should be closed in SLA
Vulnerability scanner should be enabled

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

MONITORED via 1 check

Vulnerability should be closed in SLA

Control SDC 112

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

## CC7.4

The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

### INTERNAL CONTROLS AND CHECKS

Control SDC 23

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

DECLARED via 1 check

Internal Audit

Control SDC 53

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 54

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

## CC7.5

The entity identifies, develops, and implements activities to recover from identified security incidents.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

# CC8

## Change Management

### CC8.1

The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

MONITORED via 4 checks

SDLC Procedure
Operation Security Policy
Operations Security Procedure
System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

MONITORED via 5 checks

Change management repos should be classified
Change management source should be configured
SDLC Procedure
Operation Security Policy
Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

MONITORED via 5 checks

Changes to production code should be reviewed by peers
Change requests should be reviewed by peers
SDLC Procedure
Operation Security Policy
Operations Security Procedure

Control SDC 52

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

MONITORED via 1 check

Critical Infrastructure assets should be identified

## CC9

## Risk Mitigation

### CC9.1

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#### INTERNAL CONTROLS AND CHECKS

Control SDC 67

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

MONITORED via 1 check

Risk Assessment & Management Policy

Control SDC 18

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control SDC 19

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

MONITORED via 1 check

Risk assessment should be conducted periodically

## CC9.2

The entity assesses and manages risks associated with vendors and business partners.

### INTERNAL CONTROLS AND CHECKS

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

MONITORED via 1 check

Risk Assessment & Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

# C1

## Additional Criteria for Confidentiality

### C1.1

The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#### INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 2 checks

Policies should be acknowledged by onboarded staff

Policies should be acknowledged by onboarded staff

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 3 checks

Staff devices should have disk encryption enabled

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

MONITORED via 5 checks

Data at rest should be encrypted
Data at rest should be encrypted
Encryption Policy
Asset Management Policy
Asset Management Procedure

Control SDC 69

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

MONITORED via 1 check

Information Security Policy

Control SDC 70

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

MONITORED via 1 check

Data Classification Policy

## C1.2

The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

#### INTERNAL CONTROLS AND CHECKS

Control SDC 48

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

MONITORED via 1 check

Data Retention Policy

## About Sprinto

Sprinto is a modern platform for continuous compliance monitoring. It automates the detection, remediation, and management of security risks, ensuring ongoing compliance with leading security and privacy standards.