

SOC 2 CONTROLS LIST

Criteria		Control
CONTROL ENVIRONMENT		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Entity establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet
		Entity requires that new employees review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Entity's Senior Management reviews and approves all company policies annually.
		Entity's Senior Management reviews and approves the state of the Information Security program annually
		Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities
		Entity ensures clarity in job responsibilities for client serving, IT and engineering positions (via OKRs, Job Descriptions etc.) to increase the operational effectiveness of the organisation
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Entity ensures that new hires have been duly evaluated for competence in their expected job responsibilities.
		Entity ensures that new hires go through a background check as part of their onboarding process
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Entity has established an Information Security Awareness training, and its contents are available for all staff on the company intranet.
		Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually

		Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their Job responsibilities
		Entity requires that all staff members review and acknowledge company policies annually

Criteria		Control
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.	The entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.
		Entity makes all policies and procedures available to all staff members via the company intranet
		Entity displays the most current information about its services on its website, which is accessible to its customers.
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.	Entity establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet
		Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually
		Entity requires that all staff members review and acknowledge company policies annually
		Entity makes all policies and procedures available to all staff members via the company intranet
		Entity has provided information to employees, via the Information Security Policy, 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.
		Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Entity displays the most current information about its services on its website, which is accessible to its customers.
		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.

Criteria		Control
RISK ASSESSMENT		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Entity has formally documented policies and procedures to govern risk management.
		Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements
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.	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements
		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.
		Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
		Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements
		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.
		Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements

Criteria		Control
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.	Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.
		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
		Entity's Senior Management reviews and approves all company policies annually.
		Entity's Senior Management reviews and approves the state of the Information Security program annually
		Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met
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.	Entity has provided information to employees, via the Information Security Policy, 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.
		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
		Entity's Senior Management reviews and approves all company policies annually.
		Entity's Senior Management reviews and approves the state of the Information Security program annually

Criteria		Control
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.	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
		Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	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
		Entity's Senior Management reviews and approves all company policies annually.
		Entity's Senior Management reviews and approves the state of the Information Security program annually
		Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		Entity's Infosec officer reviews and approves the list of people with access to production console annually
		Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met
		Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
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.	Entity makes all policies and procedures available to all staff members via the company intranet
		Entity requires that all staff members review and acknowledge company policies annually
		Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
		Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Criteria		Control
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.	Entity has developed an Access Control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.
		Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.
		Entity's Senior Management or the Information Security Officer periodically reviews and approves the list of people with access to the entity's system
		Entity's Senior Management or the Information Security Officer periodically reviews and approves the list of people with Administrative access to the entity's system
		Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access
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.	Entity has developed an Access Control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.
		Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.
		Staff access to Entity's systems are made inaccessible in a timely manner as a part of the offboarding process.
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.	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.
		Staff access to Entity's systems are made inaccessible in a timely manner as a part of the offboarding process.
		Entity ensures that access to the Infrastructure provider's environment (production console) is restricted to only those individuals who require such access to perform their job functions

		Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Entity relies on an infrastructure provider for hosting the systems supporting its production environment. As a result there is no physical access available to its staff members
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.	Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor-authentication
		Entity requires that all endpoints with access to production systems are protected by malware-protection software
		Entity requires that all company-owned endpoints be encrypted to protect them from unauthorised access
		Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.
		Entity requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity
		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.
		Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access
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.	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorised access
		All production database[s] that store customer data are encrypted at rest.
		User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.
		Entity maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.

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.	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.
		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.

Criteria		Control
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.	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		Entity tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.
		Entity's infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.
		Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.
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.	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		Entity tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.
		Entity's infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.
		Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.
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.	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
		Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.

		Entity maintains a record of information security incidents.
		Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		Entity tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.
		Entity's infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.
		Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.
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.	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
		Entity has established an Incident Management & Response Policy, which includes guidelines and procedures to be undertaken in response to information security incidents. This is available to all staff members via the company intranet.
		Entity maintains a record of information security incidents.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.
		Entity has a documented Data Backup Policy, and makes it available for all staff on the company intranet.

Criteria		Control
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.	Entity has a documented Change Management Policy, which is available to all Staff Members via the company intranet
	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Entity uses a change management system to track, review and log all changes to the application code.
		Entity maintains a list of infrastructure assets and segregates production assets from its staging/development assets.
		Entity's change management system is configured to enforce peer reviews for all planned changes. For all code changes, the reviewer must be different from the author.

Criteria		Control
RISK MITIGATION		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Entity has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.
		Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements
		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.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Entity has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.
		Entity has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.
		Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements

Criteria		Control
ADDITIONAL CRITERIA FOR AVAILABILITY		
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.	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.
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.	Entity has a documented Data Backup Policy, and makes it available for all staff on the company intranet.
		Entity backs-up their production databases periodically.

		Entity's data backups are restored and tested annually
		Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.
		Entity's data backups are restored and tested annually

Criteria		Control
ADDITIONAL CRITERIA FOR CONFIDENTIALITY		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Entity has a documented Confidentiality Policy, and makes it available for all staff on the company intranet.
		Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.
		Entity requires that all staff members review and acknowledge company policies annually
		Entity has a documented Data Classification Policy, and makes it available for all staff on the company intranet.
		All production database[s] that store customer data are encrypted at rest.
		Entity requires that all company-owned endpoints be encrypted to protect them from unauthorised access
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Entity has a documented Data Retention Policy, and makes it available for all staff on the company intranet.
		Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.