ZeroDayCPA

KRAYON

MPC Wallet Solution

SOC 2

Report on System and Organization Controls Relevant to Security

As of July 1, 2023

Table of Contents

Section 1 - Independent Service Auditor’s Report

To: Krayon Digital

Scope

We have examined Krayon Digital’s accompanying description of its MPC Wallet Solution titled "Krayon Digital’s Description of Services as of July 1, 2023”, (description) based on the criteria for a description of a service organization’s system in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design of controls stated in the description as of July 1, 2023, to provide reasonable assurance that Krayon Digital’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Krayon Digital uses Amazon Web Services (AWS) to provide data services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Krayon Digital, to achieve Krayon Digital’s service commitments and system requirements based on the applicable trust services criteria. The description presents Krayon Digital’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Krayon Digital’s controls The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Krayon Digital, to achieve Krayon Digital’s service commitments and system requirements based on the applicable trust services criteria. The description presents Krayon Digital’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Krayon Digital’s controls. Our examination did not include such

complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Krayon Digital is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Krayon Digital's service commitments and system requirements were achieved. Krayon Digital has provided the accompanying assertion titled "Management's Assertion" (assertion) about the description and the suitability of design of controls stated therein. Krayon Digital is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed

- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria

- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

a. the description presents Krayon Digital's MPC Wallet Solution that was designed and implemented as of July 1, 2023, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of July 1, 2023, to provide reasonable assurance that Krayon Digital's service commitments and

system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of July 1, 2023 and if the subservice organization and user entities applied the complementary controls assumed in the design of Krayon Digital's controls.

Restricted Use

This report, is intended solely for the information and use of Krayon Digital, user entities of Krayon Digital's MPC Wallet Solution as of July 1, 2023, business partners of Krayon Digital subject to risks arising from interactions with the MPC Wallet Solution, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Lance Samona

Lance Samona
CPA
Zero Day CPA, PC

07/20/2023

Date

Section 2 - Management's Assertion

We have prepared the accompanying description of Krayon Digital's system titled , "Krayon Digital's Description of its MPC Wallet Solution" as of July 1, 2023" (description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the MPC Wallet Solution that may be useful when assessing the risks arising from interactions with Krayon Digital's system, particularly information about system controls that Krayon Digital has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Krayon Digital uses Amazon Web Services (AWS) (or 'subservice organization') to provide data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Krayon Digital, to achieve Krayon Digital's service commitments and system requirements based on the applicable trust services criteria. The description presents Krayon Digital's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Krayon Digital's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Krayon Digital, to achieve Krayon Digital's service commitments and system requirements based on the applicable trust services criteria. The description presents Krayon Digital's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Krayon Digital's controls.

We confirm, to the best of our knowledge and belief, that:

a. the description presents Krayon Digital's MPC Wallet Solution that was designed and implemented as of July 1, 2023, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of July 1, 2023, to provide reasonable assurance that Krayon Digital's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of July 1, 2023, and if the subservice organization and user entities applied the complementary controls assumed in the design of Krayon Digital's controls as of July 1, 2023.

07/20/2023

Chris Chan
Chief Operating Officer
Krayon Digital

Date

Section 3 - Krayon's Description of Services as of July 1, 2023

Company Background & System Overview

Krayon Digital was founded in 2022 in Singapore and Israel and has employees mostly remote and in an office in Israel. They make it easier for holders of digital assets to manage their private keys through a process called key sharding. They provide the solution via a software service that clients can pay for via a monthly fee and thereby make it easier for companies to manage their security around private keys.

Krayon was founded by several Fintech and Cyber security veterans from Cye, Israeli government office, Platform One, JPMorgan and Forge Global and has investors such as GSR, Aquanow, Saison capital, Sparkle VC, Blockchain founders fund and others.

Services Provided

The Krayon digital application enables any holder of digital assets to use their solution to manage their keys via a Front end web application which users can log into via a username and password. Users can create as many wallets as they like, and send and receive digital assets.

Krayon is also available as an API and soon to be SDK which offer clients the opportunity to embed the Krayon solution onto their own platform and offer wallets and key management services to their customers without building it themselves.

Principal Service Commitments and System Requirements

Krayon Digital designs its processes and procedures to meet its objectives for key management software services.

Those objectives are based on the service commitments that Krayon makes to its clients, while always respecting the laws and regulations that govern the provision of digital asset services, and the financial, operational, and compliance requirements that Krayon has established for the services.

The key management software services of Krayon are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which Krayon operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- Security principles within the fundamental designs of the Krayon platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

Krayon establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Krayon's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

Components of the System

Infrastructure

Primary infrastructure used to provide Krayon's Services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Amazon Web Services	Cloud Hosting Services	Scalable infrastructure services such as storage options, computing power, and database services

Software

Primary software used to provide Krayon's Services system includes the following:

Primary Software	
Software	**Purpose**
Datadog	Monitoring and analytics platform for cloud applications
GitHub	Version control and collaborative software development
Google Workspace	Business suite, email collaboration, access management
Jira	Issue and project tracking
Slack	Communication and workplace collaboration tool
Google Cloud Identity	A cloud-based identity and access management service

People

Krayon has a staff of 5 full time staff and another 5 contractors organized into the following functions:

Management: Individuals who are responsible for maintaining compliance, strategy and sales, and operations.

Product and Engineering: Product developers and engineers who design and maintain the Krayon key management software product including the back end infrastructure, and web interface and all debugging. This team also implements and tests new features, plans the roadmap and also remediates bugs and other fixes.

Operations: Monitoring and maintenance of the Krayon product, which involves proactively deploying monitoring software and tools and remediating them either directly or via feedback to the product and engineering team. The operations team responds to alerts generated by their system, identifies technology issues created by Krayon's customers, and determines the best path to resolution. Operations members also ensure that Krayon is using the correct compliance, legal and tech cloud infrastructure to maintain a solid operating environment. Finally, operations are responsible for responding to any potential security issues and notifying affected customers if applicable.

Sales and Marketing

- These are mostly commercial roles in marketing and sales of Krayon software. They are usually the primary point of contact for Krayons customers. They help identify which parts of the Krayon system are most useful to prospective customers, and what new product development needs to be engineered to meet customer needs.In the marketing role, they manage social media accounts and provide key product information to Krayon customers and prospective customers via email, blog posts, white papers, and other channels. Finally, the customer success team ensures that Krayon customers can use the product effectively and without errors, by assisting Krayon customers with onboarding into the product and ongoing use issues.

Data

All data produced by or for Krayon, regardless of format, will be categorized according to four levels of sensitivity: Highly Confidential, Confidential, Internal, and Public.

- Highly Confidential - Personal data of users
- Confidential - Client and employee contracts, financial documents
- Internal - Business Metrics, Standard Operating Procedures
- Public - Company Structure, Privacy Policies

Every existing type of information will have a designated owner who will be accountable for choosing the appropriate level of information classification in alignment with the needs of Krayon's business operations.

In cases where a range of sensitivity classifications are merged, the final information set should be classified under the strictest level applicable from the originating sources.

All employees of Krayon must adhere to this established information classification protocol.

Processes and Procedures

Krayon's policies and procedures ensure its Security. All personnel are expected to adhere to Krayon's policies and procedures that define how services should be delivered, including:

1. Acceptable Use Policy
2. Access Control and Termination Policy
3. Business Continuity and Disaster Recovery Plan
4. Change Management Policy
5. Code of Conduct
6. Configuration and Asset Management Policy
7. Data Classification Policy
8. Data Retention and Disposal Policy
9. Encryption and Key Management Policy
10. Information Security Policy
11. Internal Control Policy
12. MFA Reset Policy
13. Network Security Policy
14. Performance Review Policy
15. Physical Security Policy
16. Risk Assessment and Treatment Policy
17. Secure Development Policy
18. Security Incident Response Plan
19. Vendor Management Policy
20. Vulnerability and Patch Management Policy

Physical Security

All data is hosted by Amazon Web Services. Amazon Web Services data centers do not allow Krayon physical access.

Logical Access

Krayon employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users.

Access to systems should be allocated via a deny-all methodology - users should only gain access to a system upon receiving formal independent approval.

Krayon infrastructure runs on cloud and SaaS-based systems, and as such the resources used by employees to perform their roles are accounts and permissions within those systems.

Krayon employees and contractors use their account to sign-in to SaaS and cloud tools when supported. When available, multi-factor authentication should be used. Multi-factor authentication must be used for access to company email, version control tools and cloud infrastructure.

Computer Operations - Backups

Customer data is backed up in Amazon Web Services automatically on a daily basis. Backup infrastructure is maintained in Amazon Web Services, with physical access restricted according to applicable Amazon Web Services policies.

Computer Operations - Availability

Krayon maintains a Security Incident Management Policy that gives any Krayon employee a systematic incident response to a potential security risk that affects any of Krayon's information technology systems, network, or data, including Krayon data held or services provided by third-party vendors or other service providers. From time to time, Krayon may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations.

Krayon will allocate resources and implement procedures to promptly evaluate automated detection outcomes, review internal and external reports, and detect genuine information security incidents, with a requirement to document each identified incident.

This plan applies to all Krayon assets utilized by personnel acting on behalf of Krayon or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all Krayon policies and plans.

Change Control

Krayon maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Krayon uses version control software to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Krayon effectively manages and secures its networks, systems, applications, and data to combat both internal and external threats. They employ network firewalls, web application firewalls, and equivalent mechanisms to safeguard internet connections, internal network zones,

and applications. Appropriate firewall alerts and alarms are configured for timely response and investigation, extending to wireless networks. Network segregation is implemented based on information services, users, and systems, using firewall configurations to control connections between untrusted and trusted networks.

The company follows a layered security approach, ensuring minimal interactions between different layers and eliminating dependencies that could compromise security. They utilize a defense-in-depth (DiD) architecture to safeguard the confidentiality, integrity, and availability of their information systems and data. This includes placing information systems containing sensitive data in an internal network zone, effectively segregating them from the DMZ and other untrusted networks.

Boundaries of the System

The scope of this report includes the MPC Wallet Solution provided by Krayon.

This report does not include the data center hosting services provided by Amazon Web Services

The applicable trust services criteria and the related controls	
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives. Security refers to the protection of: ● Information during its collection or creation, use, processing, transmission, and storage. ● Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Internal Control Framework

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Krayon's control environment, affecting the design, administration, and monitoring of other

components. Integrity and ethical behavior are the product of Krayon's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Krayon's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.

Management's Philosophy and Operating Style

The Krayon management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows their customers entrust to them.

The management team meets frequently to be briefed on technology changes that impact the way Krayon can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Krayon to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with their core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Krayon's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. It has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting. It has an established organization structure with defined roles and responsibilities. Krayon currently operates under a hierarchical organizational structure, whereby team members report to their respective Department Leads.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Krayon's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Krayon's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

The HR policies and processes of Krayon are designed to:

1. Identify and hire competent personnel
2. Provide employees with the training and information they need to perform their jobs
3. Evaluate the performance of employees to verify their ability to perform job assignments
4. Through performance evaluation, identify opportunities for growth and job performance improvement

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for employee policies and a confidentiality agreement following new hire orientation
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment

The Risk Assessment Policy at Krayon provides guidance for conducting risk assessments, considering threats, vulnerabilities, likelihood, and impact on assets, team members, customers, vendors, suppliers, and partners. These assessments take into account the specific services offered by Krayon and address the security, availability, integrity, and confidentiality requirements.

Risk assessment process coordination involves the following responsibilities:

1. Scoping Assets:
    a. Review critical system asset inventory (hardware, software, facilities, etc.).
    b. Identify data owners (electronic and non-electronic data).
    c. Map data flow and conduct inventory of storage.
2. Identifying Threats and Vulnerabilities:
    a. Utilize vulnerability scanning, penetration tests, and security control monitoring.
    b. Analyze patterns, weaknesses, and refer to audits and external vulnerability databases.
3. Analyzing Risks:
    a. Identify risk owners responsible for each risk.
    b. Assess consequences for combinations of threats and vulnerabilities.
4. Risk Treatment:
    a. Develop action plans to mitigate critical or high risks.
    b. Implement control activities and patch vulnerable systems.
5. Calculating Residual Risks:
    a. Determine residual risks considering risk treatment decisions and implemented controls.
    b. Reassess likelihoods and impacts of initial risks.
6. Reporting:
    a. Create a risk assessment and treatment report for senior management.
    b. Include risk responses, accepted risks, and communicate findings across the organization.

Krayon conducts annual reviews of security policies and plans to align with objectives and meet regulatory requirements. Results are shared internally, findings are tracked, and changes are effectively communicated.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Krayon's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Krayon addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Krayon's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Control Activities

Control measures have been put in place to help ensure that processes are properly followed in order to protect service data security.

Authentication

The Access Control and Termination Policy at Krayon outlines requirements for managing access to data, systems, facilities, and networks. It emphasizes the principle of least privilege, where users are granted minimum access based on job function and the need-to-know principle. Administrative access to production servers and databases follows this principle as well. Unique user accounts with secure log-on processes and unique passwords are required, while multi-factor authentication is encouraged for enhanced security. Onboarding and offboarding procedures ensure proper handling of personnel transitions, including inventorying devices, documenting access needs, and revoking access when necessary. The policy also includes regular access reviews, exceptions for specific situations, and consequences for policy violations.

Krayon reviews and updates its security policies and plans annually to align with organizational objectives and meet regulatory requirements. The results are shared internally, and any necessary changes are communicated across the organization. The policy demonstrates Krayon's commitment to maintaining strong access control measures, minimizing privileges, and protecting data, systems, and facilities from unauthorized access or use.

User Provisioning and Deprovisioning

To protect and secure Krayon's production environment, role-based security has been implemented to control and restrict access. Access to the production systems is granted based on the employee's role, responsibilities, and the principle of least privilege, after obtaining approval from the system owner. To gain access to the systems, formal independent approval is required. When an employee or contractor leaves the company, their access is immediately revoked within 24 hours of their separation date, and all company devices are collected and accounted for.

Access Reviews

To ensure that internal user access is properly restricted, team managers conduct quarterly reviews of high-risk and critical vendor user accounts and their associated privileges. Any necessary changes to access are tracked and remediated.

System Inventory

The Krayon operations team maintains an inventory of the assets used to operate the platform, keeps track of these assets, and reviews and updates the inventory at least annually.

Network Security

In order to protect Krayon's production environment, firewall configurations ensure available networking ports and protocols are restricted. Additionally, administrative access to production servers and databases is restricted to executives and engineers and is reviewed when significant changes occur.

Encryption

Krayon maintains its Cryptographic Key Requirements which calls for the use of industry-approved strong algorithms for encryption processes for both data-in-transit and data-at-rest. In addition, Krayon uses cryptography and security protocols to safeguard sensitive data during transmission over open, public networks (TSLS 1.2+ or equivalent). Krayon prohibits the transmission of unprotected sensitive data using insecure end-user messaging technologies. Lastly, databases housing service data are encrypted at rest.

Vulnerability Management

The security team conducts periodic vulnerability scans. If any critical or high-rated vulnerabilities are identified, they are analyzed, reported to the relevant parties, and tracked until they are resolved. In addition to internal vulnerability scans, the Krayon team may engage a third party to perform an annual penetration test on both the network and application layers of the platform. Any critical or high-rated vulnerabilities discovered during this test will be analyzed, reported, and tracked until they are resolved.

User Endpoints

To ensure the security of user endpoints, regular monitoring of anti-malware is conducted. Configuration of robust password policies, anti-virus software, and hard drive encryption are required. Krayon implements measures to prevent, detect, and respond to the introduction of unauthorized or malicious software, aligning with its security objectives.

System Monitoring

Krayon uses logging and monitoring software to collect data from servers and endpoints, identify potential security threats or unusual system activity, monitor system performance, and track resource usage. System tools monitor load balancers and logs are made available to relevant team members. These logs are securely stored and kept for at least one year. Krayon has also implemented intrusion prevention and detection tools to monitor network traffic in the

production environment. Relevant team members receive alerts and take appropriate action in response.

Incident Management

Management has developed an incident response plan that outlines the steps for remedying security incidents that affect any of Krayon's information technology systems, networks, or data, including Krayon data held by or services provided by third-party vendors or other service providers.

Change Management

The Change Management Policy at Krayon governs the planning and implementation of changes to applications, systems, services, and infrastructure. Its goal is to increase awareness and understanding of proposed changes while minimizing negative impacts. The policy is periodically updated to align with security requirements, risk considerations, and applicable laws. All change requests, including code changes and critical infrastructure/network-related changes, must be documented using Krayon's change management tools. The process includes the following steps:

1. Product Roadmap
2. Planning & Evaluation
3. Build, Test, and Document
4. Code Review
5. Approval & Implementation
6. Communication
7. Post Change Review

By following this well-defined process, Krayon ensures that changes are carefully planned, reviewed, and communicated to minimize disruptions and maintain the quality of services provided.

Configuration Management

Krayon has a Configuration and Asset Management Policy that outlines the configuration settings for Krayon devices. These settings include encryption, security updates, malware protection, screensaver/lock screen settings, logging settings, password policy, firewall settings, and remote wipe settings. Krayon also uses a configuration management tool to ensure that the images of its production infrastructure are standardized and use the latest configurations. Any changes to the configuration are tested, reviewed, and approved by management before being deployed into the production environment.

Krayon maintains a comprehensive inventory of all assets involved in processing, storing,

transmitting, or affecting the confidentiality, integrity, or availability of sensitive information. This inventory encompasses systems connected to the network as well as network devices. It includes items such as servers, datastores, network devices, applications, and workstations. By diligently tracking these assets, Krayon ensures a complete and accurate record of the components that contribute to their information security ecosystem.

Backups and Disaster Recovery

Database backups are performed daily, encrypted, and tested periodically to validate the integrity of the backups. Backups are retained for a minimum of 30 days.

Business continuity is divided into three stages, Disaster, Response, and Recovery. A disaster is declared by senior management and all appropriate personnel are notified. An impact assessment is performed to determine those affected, possible relocation to alternate facilities, verification of backed up data, and restoration of essential services. Lastly, recovery begins with the restoration of Krayon services and facilities.

Data Management

Krayon follows its Data Retention and Disposal Policy when it comes to storing customer data. Customer data is retained while the account is active or in accordance with the agreement between Krayon and the customer. Upon request from former customers or as agreed upon with the customer, Krayon must dispose of the customer data within 30 days. Only a select group of personnel have the authority to delete customer data.

Information and Communications Systems

Krayon's internal control system relies on effective communication and the exchange of information. This includes identifying the necessary information, capturing it, and exchanging it in a timely manner to facilitate the management and control of the company's operations.

Krayon employs various channels for communication and information sharing internally, including chat systems and email. These channels are used to share information with management, employees, contractors, and customers. The company also holds weekly calls to discuss operational efficiencies within specific functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Krayon’s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is

accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Krayon's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Krayon's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Krayon's personnel.

Krayon collects and monitors audit logs and generates alerts for important events related to production systems, applications, databases, servers, message queues, load balancers, critical services, and IAM user and admin activities. To accomplish this, Krayon uses logging solutions and/or SIEM tools to collect event information from these systems and activities. Filters, parameters, and alarms are used to trigger alerts when there are deviations from established system and activity baselines. The logs are securely stored and archived in case they are needed for forensic purposes.

Reporting Deficiencies

Krayon's internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Risk meetings are held for management to review reported deficiencies and corrective actions.

Subservice Organizations

Krayon's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Krayon's services to be solely achieved by Krayon control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Krayon.

The subservice organization has been carved out for the purposes of this report.

The following subservice organization controls should be implemented by Amazon Web Services to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – Amazon Web Services		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Access to data centers is approved by authorized personnel. Physical access is revoked within 24 hours of the employee or vendor record being deactivated. Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. Access to server locations is managed by electronic access control devices.

Krayon management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Krayon performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing reports over services provided by vendors and subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

Krayon's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Krayon's services to be solely achieved by Krayon control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Krayon.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Krayon.
2. User entities are responsible for notifying Krayon of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.

4. User entities are responsible for ensuring the supervision, management, and control of the use of Krayon services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Krayon services.
6. User entities are responsible for providing Krayon with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Krayon of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Section 4 - Trust Services Criteria and Related Controls

TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) defines the criteria used within this report. The following pages contain the mapping of Krayon Digital's controls to relevant criteria; these controls have been specified by and are the responsibility of Krayon Digital. The Trust Services Criteria are classified into categories; the following categories, and their respective criteria, are included within the scope of this report:

- **Security -** The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

  Security refers to the protection of:

  1. information during its collection or creation, use, processing, transmission, and storage; and
  2. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of Krayon Digital's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information

The trust services categories and related controls specified by Krayon Digital are presented in Section 4 of this report.

Trust Services Criteria for Security		
TSC #	**Criteria**	**Platform Control Description**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	A code of conduct that outlines ethical expectations, behavior standards, and consequences of noncompliance or violations is established. New hires are required to acknowledge and adhere to this code upon hiring.
		Internal personnel are evaluated at least annually through a formal performance review.

		Employees who violate information security policies may face disciplinary action, up to and including termination of employment, which is clearly documented in one or more policies.
		An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed 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.	Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.
		Management maintains a formal organizational chart to clearly show positions of authority and lines of communication, and makes this chart available to internal personnel.
		Roles and responsibilities related to security and other criteria for all employees and executive roles are outlined in job descriptions and policies, as applicable.
		Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A code of conduct that outlines ethical expectations, behavior standards, and consequences of noncompliance or violations is established. New hires are required to acknowledge and adhere to this code upon hiring.
		Internal personnel are evaluated at least annually through a formal performance review.

		Background checks are completed for new employees and contractors as defined by the policy and as permitted by local laws.
		Hiring managers evaluate the qualifications, experience, and competency of new hires to ensure they are capable of fulfilling their responsibilities. Confidentiality agreements are signed upon hire.
		Internal personnel complete training programs on information security upon hire and on an annual basis, as specified in the policy. This training helps employees understand their obligations and responsibilities related to security.
		An Information Security Policy is in place to set security requirements for protecting relevant applications, systems, infrastructure and data. This policy is available to all relevant employees and contractors, and is reviewed annually.
		An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A Performance Review Policy is in place to provide employees with context and transparency into their performance and career development process. This policy is accessible to all relevant employees, and is reviewed annually.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.
		Internal personnel are evaluated at least annually through a formal performance review.
		A continuous monitoring solution is used to monitor internal controls related to service commitments and system requirements. This tool identifies instances of non-compliance for management to address.
		Management maintains a formal organizational chart to clearly show positions of authority and lines of communication, and makes this chart available to internal personnel.

		Employees who violate information security policies may face disciplinary action, up to and including termination of employment, which is clearly documented in one or more policies.
		An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A Performance Review Policy is in place to provide employees with context and transparency into their performance and career development process. This policy is accessible to all relevant employees, and is reviewed annually.
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A continuous monitoring solution is used to monitor internal controls related to service commitments and system requirements. This tool identifies instances of non-compliance for management to address.
		An Information Security Policy is in place to set security requirements for protecting relevant applications, systems, infrastructure and data. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
		Vulnerability scanning is conducted on relevant infrastructure systems and repositories, and identified deficiencies are addressed and remediated according to the 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.	Descriptions of the company's services, systems, security and other commitments are available to both internal personnel and external users. These are published on the organization's website.
		A confidential reporting channel is available to internal personnel and external users to report security and other concerns. Management monitors communications from the channel and responds in accordance with the Security Incident Response Plan.
		A Security Incident Response Plan is in place to outline the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution. This plan is available to all relevant employees and contractors, and is reviewed annually.

		A Network Security Policy is in place to establish requirements for protecting information and systems within and across networks. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.
		Internal personnel complete training programs on information security upon hire and on an annual basis, as specified in the policy. This training helps employees understand their obligations and responsibilities related to security.
		Roles and responsibilities related to security and other criteria for all employees and executive roles are outlined in job descriptions and policies, as applicable.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Descriptions of the company's services, systems, security and other commitments are available to both internal personnel and external users. These are published on the organization's website.
		The company's commitments with respect to security and other criteria are documented within the company's agreements, which are acknowledged by the customer. Terms of Service, Master Service Agreements, or equivalent documents that define confidentiality requirements are agreed to by the customer.
		The Change Management Policy and Security Incident Response Plan detail the requirements for communicating with external parties following a system change, an incident, or unauthorized disclosure of sensitive information.
		A reporting channel is available to internal personnel and external users to report security and other concerns. Management monitors communications from the channel and responds in accordance with the Security Incident Response Plan.
		A Privacy Policy that governs privacy commitments is accessible to external users and all relevant employees and contractors and is reviewed annually. The policy is published on the organization’s website.

		Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.
		Agreements, which include security requirements, are executed with vendors in accordance with the 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.	Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.
		A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
		A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
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.	A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
		A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
		A risk register is maintained to document risk mitigation strategies for unmitigated risks, and to track the development or modification of controls consistent with these strategies.

		A Vendor Management Policy is in place to establish a framework for managing vendor relationships. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.
		Vulnerability scanning is conducted on relevant infrastructure systems and repositories, and identified deficiencies are addressed and remediated according to the policy.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
		Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.
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.	A continuous monitoring solution is used to monitor internal controls related to service commitments and system requirements. This tool identifies instances of non-compliance for management to address.
		An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Vulnerability scanning is conducted on relevant infrastructure systems and repositories, and identified deficiencies are addressed and remediated according to the 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.	Senior management and the board of directors meet at least annually to review business goals, company initiatives, resource needs, risk management activities, and other matters. The information security team meets at least annually to review security risks, roles & responsibilities, controls, changes, audit results and other matters.

		A continuous monitoring solution is used to monitor internal controls related to service commitments and system requirements. This tool identifies instances of non-compliance for management to address.
		Vulnerability scanning is conducted on relevant infrastructure systems and repositories, and identified deficiencies are addressed and remediated according to the policy.
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.	An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
		A risk register is maintained to document risk mitigation strategies for unmitigated risks, and to track the development or modification of controls consistent with these strategies.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	A Secure Development Policy is in place to define basic rules for secure software and system development and maintenance. This policy is available to relevant employees and contractors, and is reviewed annually.
		A continuous monitoring solution is used to monitor internal controls related to service commitments and system requirements. This tool identifies instances of non-compliance for management to address.
		An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Roles and responsibilities related to security and other criteria for all employees and executive roles are outlined in job descriptions and policies, as applicable.
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.	An Access Control and Termination Policy is in place to regulate authentication and access to relevant data, systems, facilities, and networks. This policy is

		available to all relevant employees and contractors, and is reviewed annually.
		An Encryption and Key Management Policy is in place to support the secure encryption and decryption of app secrets and to regulate the use of cryptographic controls. This policy is accessible to all relevant employees and contractors and is reviewed on an annual basis.
		A Business Continuity and Disaster Recovery Policy is in place to outline the processes for restoring the service or supporting infrastructure in the event of a disaster or disruption. This policy is accessible to all relevant employees and contractors and is reviewed annually.
		A Data Classification Policy has been implemented to detail the security and handling protocols for sensitive data. This policy is available to all employees and contractors who need it, and it is reviewed annually.
		A Data Retention and Disposal Policy is in place that outlines how customer data is to be retained and disposed of based on compliance requirements and contractual obligations. This policy is accessible to all relevant employees and contractors and is reviewed on an annual basis.
		A Configuration and Asset Management Policy is in place to govern configurations for new sensitive systems. This policy is available to relevant employees and contractors, and is reviewed annually.
		A Change Management Policy is in place to govern the documentation, tracking, testing, and approval of system, network, security, and infrastructure changes for applications, resources, and tools. This policy is available to relevant employees and contractors, and is reviewed annually.
		A Secure Development Policy is in place to define basic rules for secure software and system development and maintenance. This policy is available to relevant employees and contractors, and is reviewed annually.
		A Privacy Policy that governs privacy commitments is accessible to external users and all relevant employees and contractors and is reviewed annually. The policy is published on the organization's website.
		A Security Incident Response Plan is in place to outline the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution. This plan is available

		to all relevant employees and contractors, and is reviewed annually.
		A Network Security Policy is in place to establish requirements for protecting information and systems within and across networks. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A continuous monitoring solution is used to monitor internal controls related to service commitments and system requirements. This tool identifies instances of non-compliance for management to address.
		An Acceptable Use Policy is in place to establish standards for appropriate and secure use of company hardware and electronic systems. New hires and contractors must acknowledge this policy upon hire, and it is available to all employees and contractors. The policy is reviewed annually.
		Employees who violate information security policies may face disciplinary action, up to and including termination of employment, which is clearly documented in one or more policies.
		An Information Security Policy is in place to set security requirements for protecting relevant applications, systems, infrastructure and data. This policy is available to all relevant employees and contractors, and is reviewed annually.
		An Internal Control Policy is in place to safeguard assets, promote operational efficiency, and ensure compliance with managerial policies. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A Performance Review Policy is in place to provide employees with context and transparency into their performance and career development process. This policy is accessible to all relevant employees, and is reviewed annually.
		Roles and responsibilities related to security and other criteria for all employees and executive roles are outlined in job descriptions and policies, as applicable.
		A Physical Security Policy that details the physical security requirements for physically protecting assets and the company facility is accessible to all relevant employees and contractors, and is reviewed annually.

		A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
		A Vendor Management Policy is in place to establish a framework for managing vendor relationships. This policy is available to all relevant employees and contractors, and is reviewed annually.
		A Vulnerability Management and Patch Management Policy is in place to properly identify and efficiently address vulnerabilities. This policy is available to all relevant employees and contractors, and is reviewed annually.
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.	Personnel are required to use strong, complex passwords and a second form of authentication, as specified in the policy, to access sensitive systems, networks, and information.
		An Access Control and Termination Policy is in place to regulate authentication and access to relevant data, systems, facilities, and networks. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Data stores housing sensitive customer data are encrypted at rest.
		An Encryption and Key Management Policy is in place to support the secure encryption and decryption of app secrets and to regulate the use of cryptographic controls. This policy is accessible to all relevant employees and contractors and is reviewed on an annual basis.
		A Configuration and Asset Management Policy is in place to govern configurations for new sensitive systems. This policy is available to relevant employees and contractors, and is reviewed annually.
		Company endpoints (workstations) used by employees and contractors are managed and configured with a strong password policy, anti-virus software, and hard drive encryption.

		A review of key configurations related to networking ports, protocols, services, and firewalls is conducted according to the policy to help ensure that the environment is adequately restricted from outside traffic. Any configurations identified during the review as needing changes are tracked until they are resolved.
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.	An Access Control and Termination Policy is in place to regulate authentication and access to relevant data, systems, facilities, and networks. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Users are granted access to systems based on established role-based access controls (RBAC) or a documented business need, along with an analysis of segregation of duties and approval from the system owner based on the principle of least privilege.
		Upon employee or contractor termination, or change in job function or role, access to inscope applications, resources, and tools is removed, and assets are returned, according to the policy.
		In accordance with policy documentation, system owners regularly review user access to inscope applications, resources, and tools to ensure that each user's access remains appropriate for their job responsibilities. If any unnecessary access is identified as no longer required, it will be promptly revoked.
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.	An Access Control and Termination Policy is in place to regulate authentication and access to relevant data, systems, facilities, and networks. This policy is available to all relevant employees and contractors, and is reviewed annually.

		Users are granted access to systems based on established role-based access controls (RBAC) or a documented business need, along with an analysis of segregation of duties and approval from the system owner based on the principle of least privilege.
		Upon employee or contractor termination, or change in job function or role, access to inscope applications, resources, and tools is removed, and assets are returned, according to the policy.
		In accordance with policy documentation, system owners regularly review user access to inscope applications, resources, and tools to ensure that each user's access remains appropriate for their job responsibilities. If any unnecessary access is identified as no longer required, it will be promptly revoked.
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.	A Physical Security Policy that details the physical security requirements for physically protecting assets and the company facility is accessible to all relevant employees and contractors, and is reviewed annually.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Personnel are required to use strong, complex passwords and a second form of authentication, as specified in the policy, to access sensitive systems, networks, and information.
		Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
		An Encryption and Key Management Policy is in place to support the secure encryption and decryption of app secrets and to regulate the use of cryptographic controls. This policy is accessible to all relevant employees and contractors and is reviewed on an annual basis.
		Security tools that monitor network traffic to the production environment and alert the company of potential security events are implemented.

		A review of key configurations related to networking ports, protocols, services, and firewalls is conducted according to the policy to help ensure that the environment is adequately restricted from outside traffic. Any configurations identified during the review as needing changes are tracked until they are resolved.
		A Network Security Policy is in place to establish requirements for protecting information and systems within and across networks. This policy is available to all relevant employees and contractors, and is reviewed annually.
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.	Data stores housing sensitive customer data are encrypted at rest.
		Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
		Company endpoints (workstations) used by employees and contractors are managed and configured with a strong password policy, anti-virus software, and hard drive encryption.
		An Acceptable Use Policy is in place to establish standards for appropriate and secure use of company hardware and electronic systems. New hires and contractors must acknowledge this policy upon hire, and it is available to all employees and contractors. The policy is reviewed annually.
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.	A code repository has been established to manage changes to the codebases for applications and ensure their secure deployment to the production environment.
		A code repository has been established to manage changes to the codebases for applications and ensure their secure deployment to the production environment.
		Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed through a deployment tool and are reviewed annually.

		Code changes are tested prior to being merged to the production branch.
		System changes are approved by at least one independent person prior to being merged to the production branch. Access to modify the deployment tool configurations is restricted to appropriate personnel.
		A Configuration and Asset Management Policy is in place to govern configurations for new sensitive systems. This policy is available to relevant employees and contractors, and is reviewed annually.
		A Change Management Policy is in place to govern the documentation, tracking, testing, and approval of system, network, security, and infrastructure changes for applications, resources, and tools. This policy is available to relevant employees and contractors, and is reviewed annually.
		Company endpoints (workstations) used by employees and contractors are managed and configured with a strong password policy, anti-virus software, and hard drive encryption.
		An Acceptable Use Policy is in place to establish standards for appropriate and secure use of company hardware and electronic systems. New hires and contractors must acknowledge this policy upon hire, and it is available to all employees and contractors. The policy is reviewed annually.
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.	A code repository has been established to manage changes to the codebases for applications and ensure their secure deployment to the production environment.
		Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed through a deployment tool and are reviewed annually.

		A Configuration and Asset Management Policy is in place to govern configurations for new sensitive systems. This policy is available to relevant employees and contractors, and is reviewed annually.
		Security tools that monitor network traffic to the production environment and alert the company of potential security events are implemented.
		Logging is enabled and monitoring is configured to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.
		Alerting software is used to notify impacted teams of potential security events and identified events are tracked to resolution.
		A Vulnerability Management and Patch Management Policy is in place to properly identify and efficiently address vulnerabilities. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Vulnerability scanning is conducted on relevant infrastructure systems and repositories, and identified deficiencies are addressed and remediated according to the policy.
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.	Security tools that monitor network traffic to the production environment and alert the company of potential security events are implemented.
		Logging is enabled and monitoring is configured to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.

		Logging is enabled and monitoring is configured to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.
		A Network Security Policy is in place to establish requirements for protecting information and systems within and across networks. This policy is available to all relevant employees and contractors, and is reviewed annually.
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.	A Security Incident Response Plan is in place to outline the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution. This plan is available to all relevant employees and contractors, and is reviewed annually.
		Identified incidents are documented, tracked, and responded to according to the Security Incident Response Plan.
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.	A Business Continuity and Disaster Recovery Policy is in place to outline the processes for restoring the service or supporting infrastructure in the event of a disaster or disruption. This policy is accessible to all relevant employees and contractors and is reviewed annually.
		The Change Management Policy and Security Incident Response Plan detail the requirements for communicating with external parties following a system change, an incident, or unauthorized disclosure of sensitive information.
		A Security Incident Response Plan is in place to outline the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution. This plan is available to all relevant employees and contractors, and is reviewed annually.

		Identified incidents are documented, tracked, and responded to according to the Security Incident Response Plan.
		A lessons learned document is created and shared with relevant internal personnel to make any required changes following an incident in order to continually improve security and operations.
		The Security Incident Response Plan is periodically tested to evaluate its effectiveness, and management makes changes to the plan based on the test results.
		Employees who violate information security policies may face disciplinary action, up to and including termination of employment, which is clearly documented in one or more policies.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The integrity of backups is verified by restoring backed-up data to a non-production environment at least annually.
		The Business Continuity and Disaster Recovery Plan is periodically tested through tabletop exercises or similar methods. If necessary, Management will make changes to the plan based on the results of these tests.
		The Change Management Policy and Security Incident Response Plan detail the requirements for communicating with external parties following a system change, an incident, or unauthorized disclosure of sensitive information.
		A Security Incident Response Plan is in place to outline the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution. This plan is available to all relevant employees and contractors, and is reviewed annually.
		Identified incidents are documented, tracked, and responded to according to the Security Incident Response Plan.
		A lessons learned document is created and shared with relevant internal personnel to make any required changes following an incident in order to continually improve security and operations.

		The Security Incident Response Plan is periodically tested to evaluate its effectiveness, and management makes changes to the plan based on the test results.
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.	A code repository has been established to manage changes to the codebases for applications and ensure their secure deployment to the production environment.
		A code repository has been established to manage changes to the codebases for applications and ensure their secure deployment to the production environment.
		Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed through a deployment tool and are reviewed annually.
		Code changes are tested prior to being merged to the production branch.
		System changes are approved by at least one independent person prior to being merged to the production branch. Access to modify the deployment tool configurations is restricted to appropriate personnel.
		The change management cycle uses non-production environments for developing, testing, and staging changes before they are deployed into production.
		Production data is not used in the development and testing environments, unless required for debugging customer issues.
		A Configuration and Asset Management Policy is in place to govern configurations for new sensitive systems. This policy is available to relevant employees and contractors, and is reviewed annually.

		A Change Management Policy is in place to govern the documentation, tracking, testing, and approval of system, network, security, and infrastructure changes for applications, resources, and tools. This policy is available to relevant employees and contractors, and is reviewed annually.
		A Secure Development Policy is in place to define basic rules for secure software and system development and maintenance. This policy is available to relevant employees and contractors, and is reviewed annually.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A Business Continuity and Disaster Recovery Policy is in place to outline the processes for restoring the service or supporting infrastructure in the event of a disaster or disruption. This policy is accessible to all relevant employees and contractors and is reviewed annually.
		A Security Incident Response Plan is in place to outline the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution. This plan is available to all relevant employees and contractors, and is reviewed annually.
		A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
		A formal risk assessment is conducted at least once annually to identify, update, and assess internal and external threats, related to security, availability and confidentiality, including the potential for fraud.
		A risk register is maintained to document risk mitigation strategies for unmitigated risks, and to track the development or modification of controls consistent with these strategies.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A Vendor Management Policy is in place to establish a framework for managing vendor relationships. This policy is available to all relevant employees and contractors, and is reviewed annually.
		Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.