Cronofy Limited
Type 1 SOC 2
2019

REPORT ON CRONOFY LIMITED'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

November 5, 2019

Table of Contents

SECTION 1 ASSERTION OF CRONOFY LIMITED MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 CRONOFY LIMITED'S DESCRIPTION OF ITS CRONOFY'S CALENDAR AND SCHEDULING SERVICES SYSTEM AS OF NOVEMBER 5, 2019 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 8
Components of the System 9
Boundaries of the System 12
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 12
Control Environment 12
Risk Assessment Process 14
Information and Communications Systems 14
Monitoring Controls 14
Changes to the System in the Last 12 Months 15
Incidents in the Last 12 Months 15
Subservice Organizations 15
COMPLEMENTARY USER ENTITY CONTROLS 16
TRUST SERVICES CATEGORIES 17
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 18
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 18

SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR 42

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 43

SECTION 1

ASSERTION OF CRONOFY LIMITED MANAGEMENT

ASSERTION OF CRONOFY LIMITED MANAGEMENT

November 11, 2019

We have prepared the accompanying description of Cronofy Limited's ('Cronofy' or 'the Company') Cronofy's Calendar and Scheduling services system titled "Cronofy Limited's Description of Its Cronofy's Calendar and Scheduling services system as of November 5, 2019" (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 Cronofy's Calendar and Scheduling services system that may be useful when assessing the risks arising from interactions with Cronofy's system, particularly information about system controls that Cronofy 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 (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*).

Cronofy uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cronofy, to achieve Cronofy's service commitments and system requirements based on the applicable trust services criteria. The description presents Cronofy's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cronofy'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 are necessary, along with controls at Cronofy, to achieve Cronofy's service commitments and system requirements based on the applicable trust services criteria. The description presents Cronofy's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Cronofy's controls.

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

a. the description presents Cronofy's Calendar and Scheduling services system that was designed and implemented as of November 5, 2019, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of November 5, 2019, to provide reasonable assurance that Cronofy's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Cronofy's controls as of that date.

Garry Shutler
Chief Technology Officer (CTO)
Cronofy Limited

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Cronofy Limited

Scope

We have examined Cronofy's accompanying description of its Cronofy's Calendar and Scheduling services system titled "Cronofy Limited's Description of Its Cronofy's Calendar and Scheduling services System as of November 5, 2019" (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 November 5, 2019, to provide reasonable assurance that Cronofy'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*).

Cronofy Limited uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cronofy, to achieve Cronofy's service commitments and system requirements based on the applicable trust services criteria. The description presents Cronofy's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cronofy'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 Cronofy, to achieve Cronofy's service commitments and system requirements based on the applicable trust services criteria. The description presents Cronofy's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Cronofy'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

Cronofy 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 Cronofy's service commitments and system requirements were achieved. Cronofy has provided the accompanying assertion titled "Assertion of Cronofy Limited Management" (assertion) about the description and the suitability of the design of controls stated therein. Cronofy 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 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 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 report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents Cronofy's Calendar and Scheduling services system that was designed and implemented as of November 5, 2019, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of November 5, 2019, to provide reasonable assurance that Cronofy's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Cronofy's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Cronofy, user entities of Cronofy's Calendar and Scheduling services system as of November 5, 2019, business partners of Cronofy subject to risks arising from interactions with the Cronofy's Calendar and Scheduling services system, 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.

A-LIGN ASSURANCE

_____

Tampa, Florida
November 11, 2019

SECTION 3

CRONOFY LIMITED'S DESCRIPTION OF ITS CRONOFY'S CALENDAR AND SCHEDULING SERVICES SYSTEM AS OF NOVEMBER 5, 2019

OVERVIEW OF OPERATIONS

Company Background

Cronofy was founded in 2014 to address the needs of people wanting to connect their calendars with the business applications they use. The core service is delivered as a software as a service (SaaS) application programming interface (API) designed to allow a software developer to interact with an end-user's calendar data and drive scheduling workflows with it.

A highly technical founding team continues to grow and lead the company. Cronofy's headquarters are in Nottingham, UK, with an additional office in London, UK. The company operates a hybrid distributed working model with team members working from one of the offices and/or remote as needed.

Cronofy's serves software vendors providing solutions to a wide variety of industries, including human resources, finance, healthcare, labor marketplaces, education and customer relationship management (CRM).

Description of Services Provided

The core service Cronofy provides is an API to enable software applications to interact with end-user calendar data. Typical operations and application will perform with the API include:

- Reading event data
- Creating calendar events
- Reading free busy information
- Finding available times for an event within one or more user or resource calendars
- Generating self-serve booking links
- Generating calendar invitations
- Managing rules for availability
- Hosting calendar data

An application interacts with this API through JavaScript object notation (JSON) exchange over HTTP secured by transport layer security (TLS).

Principal Service Commitments and System Requirements

Cronofy designs its processes and procedures related to Cronofy's Calendar and Scheduling services to meet its objectives. Those objectives are based on the service commitments that Cronofy makes to user entities, the laws and regulations that govern the provision of Cronofy's Calendar and Scheduling services, and the financial, operational, and compliance requirements that Cronofy has established for the services.

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 are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the Cronofy's Calendar and Scheduling services 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.

Cronofy establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Cronofy'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. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cronofy's Calendar and Scheduling services.

Components of the System

Infrastructure

Primary infrastructure used to provide Cronofy's Calendar and Scheduling services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Amazon Web Services (AWS) VPC	Virtual network	Manage the traffic to and between the components of the service.
Servers	EC2 instances	Hosts and runs the components of the Cronofy service.
Relational database	AWS Aurora Postgres	The storage and retrieval of data required for the Cronofy service.
Key-value store	AWS Elasticache Redis	The storage and retrieval of ephemeral data required for the Cronofy service.
Kubernetes cluster	AWK EKS	Orchestration of the components of the system running on the servers.
Persistent queue	AWS SQS	Distribution of tasks to the asynchronous processing tasks.
Load balancers	AWS ALB	Routing of traffic to multiple instances of the Cronofy service.

Software

Primary software used to provide Cronofy's Calendar and Scheduling services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Cronofy application	Linux	The proprietary software of the Cronofy service.
AWS CloudWatch	Linux	Monitoring of key metrics such as server utilization, mean response time, etc.
PagerDuty	SaaS	Distribution of alerts driven by metric-driven alarms being triggered and other alerts.
Notion	SaaS	Company knowledge base and ticketing system.

Primary Software		
Software	**Operating System**	**Purpose**
Zendesk	SaaS	Customer-facing ticketing system.

People

Cronofy has a staff of approximately 12 employees organized in the following functional areas:

- *Corporate*. Executives, senior operations staff, and company administrative support staff, such as compliance, accounting, and finance. These individuals use Cronofy's Calendar and Scheduling services primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Cronofy's user entities
- *Operations*. Staff that administers the support and administration of user of Cronofy's Calendar and Scheduling services. They provide the direct day-to-day services, such as calendar connectivity assistance, software integration support, and reporting
- *Engineering.* Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom

Data

Data, as defined by Cronofy, constitutes the following:

- Operational information, such as contact details
- Billing information and logs, such as company name and tax identification detail
- Calendar credentials, calendar listings, and calendar event data
- Availability rules and exceptions
- Application and infrastructure logs
- Output reports
- System files

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Cronofy policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Cronofy team member.

Physical Security

The physical data center is operated by AWS.

Logical Access

Cronofy uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Cronofy implements monitoring of one or more of the responsibilities.

Computer Operations - Backups

Customer data is backed up and monitored by AWS operations personnel for completion and exceptions as part of managed services such as AWS RDS Aurora.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

Cronofy monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Cronofy evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Change Control

Cronofy 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. Development and testing are performed in environments that are logically separated from the production environment. Changes are approved by an appropriate person prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized 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 made by developers.

Version control software is also utilized to maintain infrastructure definition versions of the infrastructure, with changes tested in an indicative staging environment before being applied to production environments. The version control software maintains a history of code changes to support rollback and tracks changes made by administrators.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third party vendor uses an accepted industry standard penetration testing methodology specified by Cronofy. The third party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third party vendor on a quarterly basis in accordance with Cronofy policy. The third party vendor uses industry standard scanning technologies and a formal methodology specified by Cronofy. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Cronofy system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading virtual private network (VPN) technology.

Boundaries of the System

The scope of this report includes the Cronofy's Calendar and Scheduling services system performed in the Nottingham, England facilities.

This report does not include the cloud hosting services provided by AWS at the multiple facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

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 Cronofy's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Cronofy'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 handbook and understand their responsibility for adhering to the policies and procedures contained within the handbook
- 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

Cronofy'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 particular 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 particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain and expand the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Cronofy's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

Cronofy's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Cronofy's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

Human Resources Policies and Practices

Cronofy'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. Cronofy's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the employee handbook following new hire orientation on their first day of employment, and a confidentiality agreement is included in their contract of employment
- 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 Process

Cronofy's risk assessment process identifies and manages risks that could potentially affect Cronofy's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Cronofy identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Cronofy, and management has implemented various measures designed to manage these risks. Risks identified in this process include the risk management requirements for the identification of appropriates risks information and communication systems assets at the company.

Cronofy has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Cronofy attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Cronofy's Calendar and Scheduling services system; as well as the nature of the components of the system result in risks that the criteria will not be met. Cronofy 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, Cronofy's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Cronofy's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Cronofy, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Specific information systems used to support Cronofy's Calendar and Scheduling services system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Cronofy'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

Cronofy'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 Cronofy'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 Cronofy's personnel.

Reporting Deficiencies

An internal 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. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the last 12 months.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the last 12 months.

Criteria Not Applicable to the System

All Common criteria was applicable to the Cronofy's Calendar and Scheduling services system.

Subservice Organizations

Subservice Description of Services

This report does not include the cloud hosting services provided by AWS at the multiple facilities.

Complementary Subservice Organization Controls

Cronofy'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 Cronofy's services to be solely achieved by Cronofy control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Cronofy.

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		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.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Cronofy 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, Cronofy performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

Cronofy'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 of the Trust Services Criteria related to Cronofy's services to be solely achieved by Cronofy control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Cronofy's.

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 Cronofy.
2. User entities are responsible for notifying Cronofy of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Cronofy 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 Cronofy services.
6. User entities are responsible for providing Cronofy with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Cronofy of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. 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.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook. An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Upon hire, personnel are required to complete a background check. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct. An anonymous email address is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually. Executive management defines and documents the skills and expertise needed among its members. Executive management evaluates the skills and expertise of its members annually. Executive management maintains independence from those that operate the key controls within the environment. Executive management meets annually to assess the effectiveness and performance of internal controls within the environment. Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet. Executive management reviews job descriptions annually and makes updates, if necessary. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Executive management has established proper segregations of duties for key job functions and roles within the organization.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct evaluations are performed for personnel on an annual basis. The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process. Employees are required to attend continued training annually that relates to their job role and responsibilities. Executive management has created a training program for its employees. The entity has implemented a mentor program to develop its personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Executive management tracks and monitors compliance with continued professional education training requirements. The entity assesses training needs on an annual basis. Upon hire, personnel are required to complete a background check. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct evaluations are performed for personnel on an annual basis. Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary. Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the company intranet. Data flow diagrams, process flowcharts, and policies are documented and maintained by management to identify the relevant internal and external information sources of the system. Data is only retained for as long as required to perform the required system functionality, service or use.
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.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet. The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the company intranet. Upon hire, employees are required to complete information security and awareness training. Current employees are required to complete information security and awareness training on an annual basis. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities. An anonymous email address is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner. Changes to job roles and responsibilities are communicated to personnel through the company change ticket portal, departmental meetings and slack or email.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and made available to employees through the company intranet. The entity's objectives, including changes made to the objectives, are communicated to its personnel through the company intranet. Management tracks and monitors compliance with information security and awareness training requirements. The entity's vendor agreement delineates the boundaries of the system and describes relevant system components. The entity's vendor agreement communicates the system commitments and requirements of third parties. The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system. The entity's vendor agreement outlines and communicates the terms, conditions and responsibilities of vendors. Customer commitments, requirements and responsibilities are outlined and communicated through the standard terms on Cronofy’s website. Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via notifications through the customer management platform, HubSpot. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties. Executive management meets annually with operational management to discuss the results of assessments performed by third parties. An anonymous email address is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound. Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis. Executive management reviews and addresses repeated control failures. Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities. The entity has defined the desired level of performance and operation in order to achieve the established entity objectives. Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. Executive management reviews operational and resourcing reports to evaluate performance and resourcing at least annually. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis.
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.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. The entity's risk assessment process includes identifying the relevant information security risks and mitigating the risks identified. Identified risks are rated using a risk evaluation process and ratings are approved by management. Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Be self-insured and accept the risk • Seek external insurance • Adjust control to reduce expected losses Management develops risk mitigation strategies to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities. The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations. Identified fraud risks are reviewed and addressed using one of the following strategies: • Be self-insured and accept the risk • Seek external insurance • Adjust control to reduce expected losses

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	As part of management's assessment of fraud risks, management considers key fraud factors such as opportunity for unauthorized access or use of data, and employee morale and attitude. As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT. Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats and unusual system activity. Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. External vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities. Evaluations of policies, controls, systems, tools, applications, and third parties for effectiveness and compliance is required at least annually. A third party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment. Performance and conduct evaluations are performed for personnel on an annual basis. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.
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 assesses the results of the compliance, control and risk assessments performed on the environment. Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed. Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives in acceptable levels.	Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations. Executive management meets annually to assess the effectiveness and performance of internal controls within the environment. Management has documented the relevant controls in place for each key business or operational process. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Business continuity and disaster recovery plans are developed and updated on an annual basis.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to its personnel through the company intranet. Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. The internal controls implemented around the entity's technology infrastructure include, at a minimum, the authentication of access and protecting the entity’s assets from external threats.
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.	Organizational and information security policies and procedures are documented and made available to its personnel through the company intranet. The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel. Management has implemented controls that are built into the organizational and information security policies and procedures. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company intranet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	An inventory of system assets and components is maintained to classify and manage the information assets. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Administrative access to the production server is restricted to the following users: • CTO • Consultant AWS environment is configured to enforce the following password requirements: • Minimum password length
	Operating System (Application and Database Servers)	
		Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • Consultant Operating systems are configured to enforce password requirements that include: • Password length
	Database	
		Database administrative access is restricted to user accounts accessible by the following personnel: • CTO • Consultant
	Application	
		Application administrative access is restricted to user accounts accessible by the following personnel: • Chief Executive Officer (CEO) • CTO The application is configured to enforce password requirements that include: • Password length Application account lockout settings are in place that include: • Account lockout threshold

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Application audit policy settings are in place that include: • Added to Role
	Remote Access	
		The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • CEO • CTO VPN users are authenticated prior to being granted remote access to the system. A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment. Critical data is stored in encrypted format using software supporting the AES encryption. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination 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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. An inventory of system assets and components is maintained to classify and manage the information assets. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
	Network	
		Administrative access to the production server is restricted to the following users: • CTO • Consultant AWS environment is configured to enforce the following password requirements: • Minimum password length
	Operating System (Application and Database Servers)	
		Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • Consultant Operating systems are configured to enforce password requirements that include: • Password length
	Database	
		Database administrative access is restricted to user accounts accessible by the following personnel: • CTO • Consultant
	Application	
		Application administrative access is restricted to user accounts accessible by the following personnel: • CEO • CTO The application is configured to enforce password requirements that include: • Password length Application account lockout settings are in place that include: • Account lockout threshold Application audit policy settings are in place that include: • Added to Role

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
	Remote Access	
		The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • CEO • CTO VPN users are authenticated prior to being granted remote access to the system. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
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.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section for controls managed by the subservice organization.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Data is only retained for as long as required to perform the required system functionality, service or use.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses. VPN, secure socket layer (SSL), and other encryption technologies are used for defined points of connectivity. VPN users are authenticated prior to being granted remote access to the system. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	An intrusion detection software (IDS) is utilized to analyze network events and report possible or actual network security breaches. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a daily basis. The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • CEO • CTO VPN users are authenticated prior to being granted remote access to the system. The entity secures its environment a using multi-layered defense approach that includes firewalls, an IDS, antivirus software and a DMZ. VPN, SSL, and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. NAT functionality is utilized to manage internal IP addresses. An IDS is utilized to analyze network events and report possible or actual network security breaches. Backup media is stored in an encrypted format.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	An IDS is utilized to analyze network events and report possible or actual network security breaches. A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment. External vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities. Documented change control policies and procedures are in place to guide personnel in the change management process. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a daily basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Management has defined configuration standards in the information security policies and procedures. Monitoring software is used to identify and evaluate ongoing system capacity, security threats, changing resource utilization needs and unusual system activity. The CTO get alerts when thresholds have been exceeded. An IDS is utilized to analyze network events and report possible or actual network security breaches. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. External vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities. A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment.
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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system capacity, security threats, changing resource utilization needs and unusual system activity. An IDS is utilized to analyze network events and report possible or actual network security breaches. A firewall is in place to filter unauthorized inbound network traffic from the internet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a daily basis.
	Operating System (Application and Database Servers)	
		Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • Consultant Operating systems are configured to enforce password requirements that include: • Password length
	Database	
		Database administrative access is restricted to user accounts accessible by the following personnel: • CTO • Consultant
	Application	
		Application administrative access is restricted to user accounts accessible by the following personnel: • CEO • CTO The application is configured to enforce password requirements that include: • Password length Application account lockout settings are in place that include: • Account lockout threshold

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented and communicated to the users within the corresponding ticket. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are classified, prioritized and resolved based on the system impact.
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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Resolution of incidents are documented and communicated to the users within the corresponding ticket. Remediation actions taken for security incidents are documented within the ticket and communicated to affected users. Identified incidents are classified, prioritized and resolved based on the system impact.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Resolution of incidents are documented and communicated to the users within the corresponding ticket.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users. Business continuity and disaster recovery plans are developed and updated on an annual basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented change control policies and procedures are in place to guide personnel in the change management process. The change management process has defined the following roles and assignments: • Changes are peer reviewed/approved • Changes are tested System changes are communicated to affected internal and external users via the entity's website or newsletters. Access to implement changes in the production environment is restricted to the: • CTO • Consultant Major system changes are peer reviewed prior to implementation. Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. Development and test environments are physically and logically separated from the production environment. System change requests are documented and tracked in a ticketing system. System changes are tested prior to implementation. Documented change control policies and procedures are in place to guide personnel in the change management process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops vendor risk mitigation strategies to address risks identified during the risk assessment. The entity's vendor agreement delineates the boundaries of the system and describes relevant system components. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by vendors.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Cronofy was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Cronofy and did not encompass all aspects of Cronofy's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.