CYBERGUARD COMPLIANCE

Cronofy

System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Cronofy's Temporal Infrastructure System Based on the Trust Services Criteria for security, availability, and confidentiality

For the Period April 1, 2025 to March 31, 2026

TABLE OF CONTENTS

SECTION 1: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Cronofy

Scope

We have examined Cronofy ("Cronofy") accompanying assertion titled "Assertion of Cronofy Management" (assertion) that the controls within Cronofy's Temporal Infrastructure System (system) were effective throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that Cronofy's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.*

Cronofy uses subservice organizations to provide cloud hosting services. The description of the boundaries of the system presented in Attachment A 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 the types of complementary subservice organization controls assumed in the design of Cronofy's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization 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 also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cronofy is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was

conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Cronofy's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Cronofy's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations
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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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, management's assertion that the controls within Cronofy's Temporal Infrastructure System were effective throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that Cronofy's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

July 6, 2026
Las Vegas, Nevada

SECTION 2: MANAGEMENT'S ASSERTION

July 6, 2026

Scope

We are responsible for designing, implementing, operating, and maintaining effective controls within Cronofy's (Cronofy) Temporal Infrastructure System (system) throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that Cronofy's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.* Our description of the boundaries of the system is presented in Attachment A (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that Cronofy's service commitments and system requirements were achieved based on the applicable trust services criteria. Cronofy's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

Cronofy uses subservice organizations to supplement its services. The description of the boundaries of the system 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 of the boundaries of the system does not disclose the actual controls at the subservice organizations.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that Cronofy's service commitments and system requirements were achieved based on the applicable trust services criteria.

Cronofy

SECTION 3:
ATTACHMENT A: CRONOFY'S DESCRIPTION OF THE BOUNDARIES OF ITS TEMPORAL INFRASTRUCTURE SYSTEM

Company Background

Cronofy was founded in 2014 to address the needs of people wanting to streamline their scheduling within the business applications they use. The core service is delivered as a software as a service (SaaS) platform with both browser-based end-user tooling and an application programming interface (API) designed to allow individuals and software developers to interact with people's schedules and drive scheduling workflows with it.

A highly technical founding team continues to grow and lead the Company. Cronofy's headquarters are in Nottingham, United Kingdom (UK), with additional offices in London, UK and Amsterdam, NL. 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 businesses and software vendors providing solutions to a wide variety of industries, including human resources, finance, healthcare, labor marketplaces, education and customer relationship management (CRM).

System Overview

The System is comprised of the following components:

- ***Infrastructure*** **-** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** **-** The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** **-** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** **-** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures*** **-** The automated and manual procedures involved in the operation of a system

Infrastructure

Hardware	Type	Purpose
Virtual Network	Amazon Web Services (AWS) Virtual Private Cloud (VPC)	Manage the traffic to and between the components of the service.
Servers	Elastic Computer Cloud (EC2) instances	Hosts and runs the components of the Cronofy service.
Relational database (RDS)	AWS Aurora Postgres	The storage and retrieval of data required for the Cronofy service.
Key-value store	AWS Elastic Cache Redis	The storage and retrieval of ephemeral data required for the Cronofy service.
Kubernetes cluster	AWS Elastic Kubernetes Service (EKS)	Orchestration of the components of the system running on the servers.
Persistent queue	AWS Simple Queue Service (SQS)	Distribution of tasks to the asynchronous processing tasks.
Load balancers	AWS Application Load Balancer (ALB)	Routing of traffic to multiple instances of the Cronofy service.

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.

Software	Operating System	Purpose
JIRA Service Desk	SaaS	Internal ticketing system.
Zendesk	SaaS	Customer-facing ticketing system.
Honeycomb	SaaS	Monitoring of the Cronofy platform
GitHub	Saas	Change control for the Cronofy service
1Password	SaaS	Password manager for all staff application passwords
Google Workspace	SaaS	Email service provider for all staff email accounts
Personio	SaaS	HR system for managing staff contracts
OneTrust	SaaS	ISMS platform

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
- Virtual meeting recordings and transcripts
- Availability rules and exceptions
- Application and infrastructure logs
- Output reports
- System files

Inbound integrations to the Cronofy System are configured with third parties via Cronofy Company-developed APIs. Additionally, Commercial Partners and Publishers transfer contact data to Cronofy via secure file transfer and manual upload within the front-end application.

Cronofy validates, stores, and processes contact data within the Cronofy System. Data is stored on database servers running PostgreSQL within the production VPC. All data is encrypted at rest, and SSL encrypts data in transit between the container and databases. Processed contact data is provided to customers in various ways:

- Data is inserted into end user calendars via the Cronofy API.
- Customers can access the processed contact data via the Cronofy web portal.
- Outbound integrations via APIs send processed contact data to third-party marketing automating platforms, CRMs, and Custom Data Platforms.

Under a managed services agreement, Cronofy manages the product on behalf of the customer. As part of these services, customers can view usage reports in the Cronofy web portal.

People

Cronofy has a staff of approximately 43 employees organized in the following functional areas:

- *Board of Directors* oversees Cronofy's strategic direction, governance, and high-level decisions. Responsible for legal duties, appointing senior executives, and monitoring performance without managing daily operations. The Board of Directors includes internal officers and external, independent directors.
- *Executive Management* establishes business and strategic objectives to meet the interests of stakeholders, and provides independent oversight of financial and operational performance. The Board of Directors, including the executive management team meet on a quarterly basis, or more frequently as needed. Management presents operational and third-party assessment results to the Board of Directors upon completion. Board attendance is tracked, and discussion points and decisions are documented in board minutes. The Board operates under bylaws that define responsibilities, including the oversight of management's system of internal control. The Board consists of sufficient members who are independent from management and are objective in making decisions.
- *Leadership Team* – Executives and senior operations staff. These individuals use Cronofy's meeting and scheduling infrastructure 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.
- *Engineering* – 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 Operations.
- *Company Administrative Support Staff* – Compliance, facilities management, accounting, and finance. They provide support for the day-to-day operational services, such as invoicing, people management and compliance reporting.
- *Support* – Staff that administers the support and administration of user of Cronofy's meeting and scheduling infrastructure. They provide the direct day-to-day services, such as calendar connectivity assistance, software integration support, and reporting
- *Sales* – Staff that are responsible for generating new business and revenue.
- *Marketing* – Employees who are responsible for driving traffic to Cronofy, and generating leads for the sales team, as well as design and branding.
- *Product* – People who are responsible for the direction and trajectory of Cronofy's product offering.

Cronofy is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. Cronofy endorses a work environment free from discrimination, harassment, and sexual harassment.

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 within the Company's GRC platform and can be accessed by any Cronofy team member.

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 a bi-annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of Cronofy's controls are suitably designed and operating effectively at the subservice organizations, along with related controls at Cronofy.

Subservice organizations are used to deliver products and services that Cronofy relies on to serve its customers and clients. AWS provides cloud hosting services, which includes implementing physical security controls to restrict access to the facility and hosted in-scope systems.

Cronofy has carved out AWS from the scope of the system. The controls and processes operated by this provider are not included in Cronofy's description of its system or in the independent service auditor's tests of operating effectiveness.

Amazon Web Services (AWS)

Cronofy uses AWS as the cloud hosting provider for the Temporal Infrastructure System. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at AWS, alone or in combination with controls at Cronofy, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.1, 6.2, 6.3, 6.6	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.
6.4	AWS is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
6.5	AWS is responsible for discontinuing logical and physical protections over physical assets when they are no longer required.
7.2	AWS is responsible for monitoring, detecting, and automatically alerting appropriate personnel of security incidents.
A 1.2	AWS is responsible for maintaining and monitoring environmental protections and recovery infrastructure.
A 1.3	AWS is responsible for maintaining and implementing testing system recovery procedures.

GitHub

Cronofy uses GitHub for cloud services for the Temporal Infrastructure System. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at GitHub, alone or in combination with controls at Cronofy, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.1, 6.2, 6.3, 6.6	GitHub is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.4	GitHub is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
6.5	GitHub is responsible for discontinuing logical and physical protections over physical assets when they are no longer required.
A 1.2	GitHub is responsible for maintaining and monitoring environmental protections and recovery infrastructure.
A 1.3	GitHub are responsible for maintaining and implementing testing system recovery procedures.

Cronofy Management receives and reviews the AWS and GitHub SOC 2 Type 2 report on an annual basis. Any deficiencies identified in a subservice organization's SOC 2 report are analyzed for relevance to and effect on Cronofy's organization and its users. As part of the review:

- Management confirms that the CSOCs listed above are covered within the scope of AWS' and GitHub's SOC 2 Type 2 reports and are found to be operating effectively during the audit period.
- Management determines that the Complementary User Entity Controls (CUECs) identified in AWS' and GitHub's SOC 2 Type 2 reports are included in the scope of this SOC 2 report as controls that are tested by the service auditor.

In addition, through its daily operational activities, management monitors the services performed by AWS and GitHub to ensure that operations and controls expected to be implemented are functioning effectively.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Description of Services Provided

The core services that Cronofy's Temporal Infrastructure System provides are tools to enhance and augment scheduling workflows. This includes an API to enable software applications to interact with end-user calendar data, and a web application for managing scheduling workflows.

Typical operations, applications, and end-users will perform using Cronofy services are:

- 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
- Recording and transcribing virtual meetings

The Cronofy Platform consists of the following components:

- Cronofy API
- Cronofy web browser

An integrating application communicates with the Cronofy API through JavaScript object notation (JSON), and end-users interact with the Cronofy service via a web browser. Both exchange data over Hypertext Transfer Protocol (HTTP) secured by Transport Layer Security (TLS).

Google Chrome, Outlook, and various other integration add-ins are available.

Principal Service Commitments and System Requirements

Cronofy designs its processes and procedures related to Cronofy's Temporal Infrastructure System 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 scheduling platform, and the financial, operational, and compliance requirements that Cronofy has established for the services.

Cronofy's security, availability, and confidentiality 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. The principal security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of Cronofy's Temporal Infrastructure 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.
- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the Cronofy platform and the customer data in accordance with Cronofy's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
    - Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) examinations.
    - International Organization for Standardization (ISO) 27001:2022, 27018:2109, 27701:2019 certification reviews.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and bi-annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of Cronofy personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain an availability SLA for customers of 99.99% uptime for each calendar month.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

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 Cronofy's Temporal Infrastructure System.

Cronofy regularly reviews the security, availability, confidentiality, and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security, availability, confidentiality commitments within the agreement, Cronofy will notify the customer via the Cronofy website or directly via email.