Security White Paper

How Cronofy approaches security and how it relates to your customers' calendar data and synchronization.

CRONOFY

Contents

1 | Introduction

Cronofy enables businesses to access and interact with end-user and organizational calendar data to deliver rich interactions and embedded workflows that enable new ways of working. Whether via the Cronofy Scheduler, or the Cronofy APIs, your data is secure at all times.

Customers of the businesses that use Cronofy services, should have confidence that Cronofy takes their security seriously and employs best practices to ensure their privacy isn't compromised.

The nature of the data Cronofy handles on behalf of its clients requires that security is a core part of the approach to building, scaling and managing our service.

Security is represented at the highest level in the company, with the Chief Technology Officer taking the lead on all security initiatives. Information security policies and standards are approved by the executive management team and the company receive training on these policies on an annual basis.

This purpose of this document is to outline how Cronofy ensures your data remains safe and secure, at all times.

2 | People Security

Security is a key part of the culture at Cronofy. The people who are building, scaling and managing Cronofy, are fundamental to providing a secure service to our customers. We support our employees by having a set of policies, procedures and playbooks in place, so that expectation is consistently clear for all, and if uncertain, the correct information is easy to find.

Background checking

Before anybody joins the company, Cronofy conducts background checks. The depth of these background checks can vary dependent on the position that the individual is taking. Background checks generally include verifying an individual's education, previous employment and references, as well as a background check with a credit reference agency.

Employee Code of Conduct

The Cronofy Employee Code of Conduct outlines what is expected of everybody at Cronofy. All employees agree upon a set of principles that are adhered to and are asked to respectfully challenge each other when this may not be the case.

Employees agree to the Code of Conduct as part of their on-boarding, and are asked to re-read it every year, or whenever there's a change to it, whichever occurs first.

Security Awareness Training

All employees must complete security training as part of their orientation when joining Cronofy. Awareness training is rolled out continuously, either when updates are made to policies, or on an annual basis.

Security awareness training includes training on, but is not limited to, good security practices, such as password security and multifactor authentication, handling incidents and preserving evidence, and information security responsibilities.

Policies and processes

Cronofy maintains a robust suite of policies and process which underpin the everyday operation of the business.

Cronofy utilises Tugboat Logic for the day-to-day management of Information Security, including the writing and distribution of policies. Policies are available to review by any member of staff, at any member of time, within Tugboat Logic.

Copies of these policies are available to customers, upon request.

Access Control Policy

Access to operational applications, platforms and data is strictly limited according to an employee's role. Cronofy operates a general rule of least privilege, meaning that, employees only receive the access they need to perform their role, and nothing more.

Access Reviews

Cronofy conducts quarterly access reviews, ensuring that employees' access to critical systems has not changed, and is still appropriate for their role. Where this isn't the case, the event is recorded, investigated, and the access adjusted.

Authentication policies

Employee accounts

All employees are trained to use 1Password to generate a random, unique password for each service, using a password as long as the service will support (or 64 characters, the maximum supported by 1Password).

Cronofy employees are trained to not share credentials unless the service does not provide "team access" functionality. In this case, 1Password Team Vaults is used to store and share credentials.

Cronofy employees will always use two-factor authentication when available. Where a solution supports it, Cronofy will set policies for the service to ensure compliance when available (such as regular password resets and blocking recycled passwords).

Cronofy customer accounts

Passwords for Cronofy customer accounts must be at least 8 characters and not on a blacklist of 10,000 common passwords (2,086 of the blacklisted passwords are 8+ characters in length).

Cronofy also offers support for multi factor authentication, should Cronofy customers want to use it.

Incident Management Policy

Cronofy's Incident Management Policy defines how Cronofy responds to events that threaten the security or privacy of confidential information, ensuring that incidents are properly identified, contained, investigated, and remedied.

The policy is supported by an Incident Response Playbook, which assigns roles, responsibilities and general guidelines on how to handle an incident. This ensures consistent handling, no matter who is managing the incident at the time.

Information Security Responsibilities

The Information Security Responsibilities outline the roles and responsibilities of employees in relation to Information Security, based on their job role. This helps all Cronofy employees understand their role within Cronofy, in relation to Information Security.

Business Continuity

Cronofy has a Business Continuity Plan which ensures that the organization can quickly recover from unexpected events while continuing to support customers and other stakeholders.

The Business Continuity Plan is tested by Cronofy on at least a yearly basis, in line with the requirements outlined in ISO27001.

After each test of the Business Continuity Plan, improvements are documented, actioned and resolved, to better improve the Business Continuity Plan.

Disaster Recovery

Cronofy's Disaster Recovery plan exists to prevent and minimize any period of loss of service for Cronofy customers. Cronofy's varies dependent on the circumstances.

For example, if AWS were to completely fail, our RTO would be six hours, and our RPO would be 24 hours. This, however, is very much a worst-case scenario.

Asset Management

Cronofy closely manages IT systems and the data that they contain from purchase to disposal. All pertinent information concerning assets is recorded within an Asset Register.

All laptops have end-user compliance tooling installed, to ensure that assets are not misused.

Equipment disposal

To appropriately protect our constituent's data, all equipment being disposed of must be disposed of per the Equipment Disposal Policy. This ensures that data is appropriately destroyed, and equipment is disposed of, both securely and in an environmentally responsible manner.

Vendor Management

The Vendor Management policy helps to ensure that Cronofy, and Cronofy's customers, are protected and that the vendors used are assessed appropriately. All new vendors must complete a Vendor Risk Assessment before Cronofy will commence service with them.

All vendors are reviewed, and risk assessed annually, to ensure that they still meet the strict data protection requirements outlined by Cronofy.

Internal Audits

The organization conducts Internal Audits on its employees, policies and controls to ensure the best level of service to its customers. If or when gaps are identified, training takes place to ensure those gaps are filled.

Security Team

Cronofy employs security and privacy professionals, as part of our Engineering and Operations teams. This team is tasked with maintaining the company's security posture, whilst developing security processes, and staying abreast of new vulnerabilities.

Our Privacy and Compliance program is led by our Head of Operations, who is involved in ensuring Cronofy meet the expectations set out by our external accreditations, by government agencies, and by our customers.

Cronofy leverages Amazon's AWS suite of services to deliver robust, reliable and scalable infrastructure to ensure continuity of service.

3 | Product Security

The Cronofy product team considers security as a first-class concern when building and developing any aspect of the Cronofy service.

Encryption in Transit

Cronofy supports TLS 1.2 to encrypt network traffic between the customer application and Cronofy's services. TLS is enforced for all communication with Cronofy APIs. TLS to calendar services is used where available.

Encryption at Rest

All calendar and personal data is encrypted at rest. Current technologies we use for this include Amazon Aurora and Amazon S3.

For particularly sensitive data where the original values are not needed, such as our own passwords, we hash the data in application using the BCrypt algorithm.

Where the original values are needed, such as authentication details for accessing calendars, the values are encrypted, again in application, using the AES-256-GCM algorithm using a unique, randomly generated salt for each set of sensitive data.

Penetration Testing

Cronofy commissions third-party penetration tests every quarter. The outcome of these tests are recorded and actioned within an appropriate timescale.

For example, high priority issues are remediated within a shorter timescale than low priority issues

Calendar Data Permissions

Cronofy uses the permissions schemes provided by the calendar service providers to access the end-user calendar.

This normally provides Cronofy's sync engine with full access to all calendar data accessible by the end-user. In some cases, the permission schemes used also provide access to email and contacts data. This is NOT accessed by the Cronofy sync engine.

Cronofy provides a permission scheme to application providers that allows them to only request the level access required to deliver the functionality they need.

For example, an application can request only free-busy access to existing events but can write additional events to the end-user's calendar. This means that only the minimum data required transits to the application.

4 | Infrastructure and Network Security

Cronofy leverages Amazon's AWS suite of services to deliver robust, reliable and scalable infrastructure to ensure the highest service levels to our customers.

Data Centres

Cronofy currently hosts production environment instances in the USA (AWS US-East Region), Germany (AWS Frankfurt Region), Singapore (AWS Singapore Region), Australia (AWS Sydney Region) and UK (AWS London Region).

Cronofy utilize multiple availability zones in these regions to enable Cronofy to remain highly available.

Each production instance operates discreetly, and no customer or account data is transferred between instances to ensure Cronofy customers' use of these instances will comply with local data privacy regulations.

Physical Security

Cronofy leverages AWS data centres for all production systems, including the storage of customer data. AWS has robust physical safety measures in place, such as fire detection and suppression, multi-resilient power sources, and strict access control policies.

For more information on AWS Data Centre Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Monitoring and Alerting

The Cronofy platform, services and third parties involved in the delivery of Cronofy services are monitored 24/7/365 by our Engineering team. Cronofy has a robust and well-documented incident response plan in place. This is supported by Disaster Recovery and Business Continuity plans, to ensure consistent delivery of service.

Current and historic status reports are available at: https://status.cronofy.com

Distributed Denial-Of-Service (DDOS) Prevention

Appropriate technologies are in place at both network infrastructure and application level, to detect, mitigate and prevent DDoS attacks.

5 | Security Compliance

Cronofy is committed to mitigating risk and ensuring that Cronofy services meet regulatory and security compliance requirements:

Regulatory Environment

Cronofy complies with applicable legal, industry, and regulatory requirements as well as industry best practices. Geographically discrete production instances allow our customers to use our services and stay compliant with regional regulations.

Top Tier Infrastructure Provider

Cronofy's service is hosted at Amazon Web Services (AWS) data centres, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS.

Data Retention

Cronofy retains the minimum amount of information, required to deliver services to our customers and end-users. The longest amount of time that Cronofy retains any event data, is 90 days. More information on data retention and data retention periods can be found in the Cronofy Data Retention policy.

ISO 27001 Compliant

Cronofy's ISMS (Information security management system) has been independently audited and meets the standards set out by the International Standards Organization for the ISO 27001 standard. A copy of Cronofy's ISO 27001 report is available on request.

SOC2 Attested

The security, availability, processing integrity, confidentiality and/or privacy controls of Cronofy, were audited, based on their compliance with the AICPA's SOC2 Standard. Cronofy's controls were found to be designed effectively and are suitably operated. A copy of the Cronofy SOC2 Type 2 report is available on request.

EU General Data Protection Regulation

Cronofy is compliant with the EU General Data Protection Regulation (GDPR) and can provide a Data Processing Agreement (DPA) on request.

HIPAA Compliance

Cronofy is HIPAA-ready and can supply a Business Associate Agreement (BAA) on request.

California Consumer Privacy Act (CCPA)

Cronofy complies with the California Consumer Privacy Act (CCPA).

Further reading

More information about our Privacy and Security program can be found at:

https://www.cronofy.com/privacy

Alternatively, we are always happy to answer further questions in regard to Cronofy's security policies and controls. Please contact our Security Team via privacy@cronofy.com in the first instance.

ISO27001 CERTIFIED

GDPR COMPLIANT

SOC 2 ATTESTED

HIPAA COMPLIANT

CCPA COMPLIANT

CRONOFY

To find out more, visit **www.cronofy.com**