CRONOFY

Security White Paper

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

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. 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.

2

People Security

The people building, scaling and managing Cronofy's service are fundamental to providing a secure service to our customers. Some of our policies:

Role based access

Access to operational applications, platforms and data are strictly limited according to an employee's role.

AUTHENTICATION POLICIES

Employee accounts

- Use 1Password to generate a random, unique password for each service
- Use a password as long as the service will support (or 64 characters, the maximum supported by 1Password)
- Do not share credentials unless the service does not provide "team access" functionality, in which case use 1Password Team Vaults to share them
- Use two-factor authentication when available
- Set policies for the service to ensure compliance when available

Cronofy customer accounts

Passwords 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).

Training

Regular training and updates on security protocols are given to all employees, at least annually.

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. SSL is enforced for all communication with Cronofy APIs. SSL 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 need, 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 is commissions third-party penetration tests on a quarterly basis.

Calendar data permissions

Cronofy uses the permissions schemes provided by the calendar service providers in order to access 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 continuity of service.

Data centers

Cronofy currently hosts production environment instances in the USA (AWS US-East Region) and Germany (AWS Frankfurt Region). These environments utilize multiple availability zones in these regions to enable Cronofy to remain resilient to failure.

Each production instance operates discretely 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 centers for all production systems and customer data.

For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper.

Monitoring

The Cronofy service is continuously monitored for availability and utilization by internal and external tools. Current and historic status reports are available at https://status.cronofy.com.

Distributed Denial-of-Service (DDoS) prevention

Protections 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 hosted at Amazon Web Services (AWS) data centers, 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.

EU-US Privacy Shield

Whilst Cronofy does not pass data across the Atlantic, Cronofy is a member of the EU-US Privacy Shield and is compliant with data protection laws both in the US and in Europe. You can view Cronofy's EU-US Privacy Shield participant page here.

California Consumer Privacy Act (CCPA)

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

Further information

For further details and for further information about Cronofy's security policies and controls please contact our Security Team via security@cronofy.com

ISO27001
CERTIFIED

PRIVACY SHIELD
COMPLIANT

GDPR
COMPLIANT

SOC 2
ATTESTED

HIPAA
COMPLIANT

CRONOFY

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