BAIN & COMPANY

Coro | Security White Paper

Introduction

This section would need to be completed by the product team developing the application. This section describes the applications functions and what exactly it does.

Organizational Security

Coro was designed with security at the forefront of priorities leveraging the application development services of Follow Analytics, recommended by our partners at Salesforce.

The Coro application is hosted within Heroku, a platform also owned by Salesforce and hosted within AWS

Hosting Provider Certifications

The Coro application is hosted on Heroku's SOC 2 compliant platform owned by Salesforce. The platform resides within AWS infrastructure. For further information regarding the security practices in place please see the following links:

https://trust.salesforce.com/en/security/stay-current-security/
https://www.heroku.com/policy/security
https://aws.amazon.com/security

Encryption

Data at rest within the Coro application is encrypted using industry standards and best practices that meet the security requirements of the Client.

TLS encryption is leveraged to provide secure communication by protecting the confidentiality and integrity for all data in transit within the Coro application.

Network Security

In the interest of protecting data, Coro logically and physically separates its networks. The corporate network is utilized for all corporate functions. This is separate from the production network, which is used for customer instances. To prevent inadvertent

information flow between different networks, access controls are implemented and reviewed periodically.

Access Control

Authentication
Authentication to the Coro application is achieved by leveraging Single Sign On through the customers Salesforce instance.

Provisioning
Access is provisioned within the clients Salesforce instance. Salesforce has strong logical access controls for their production network which include:

- Manger approved production access, based on the principal of least privilege, to include necessary segregation of duties
- Timely access removal for terminated employees
- Multi-factor authentication to internal systems
- Bastion Host in place as secure perimeter between authentication and core servers
- Centralized log correlation in place to capture system activity

Clients are responsible for granting the appropriate access permissions to data within the Coro application.

Data Retention and Disposal

Clients define the data being stored within the Coro application and can set unique data retention and disposal requirements, as well as purge data at their discretion.

Data stored within the application is housed within an AWS data center, further information regarding their disposal practices can be found at https://aws.amazon.com/security

Disaster Recovery/Business Continuity Planning

The platform Coro is hosted on maintains redundancy to prevent single points of failure and ensure the availability of data stored within the application. In the event of an outage, the platform is deployed across multiple data centers designed for resiliency. Additionally, data within the application can also be restored from backups that have been configured to meet the requirements of the client.

Incident Management

The platform hosting the Coro application has a defined and implemented incident management policy in place. The response procedure identifies when events should be escalated and who should be notified. This allows for timely response and correct alignment of personnel to resolve potential incidents.

All incidents are logged into an automated workflow and online ticketing system that tracks the incident from initiation to resolution. Personnel tending to security incidents do not have access to data stored within the application unless there is explicit permission from the client.