A White Paper on Privacy and Security at Kognitos, Inc.

©Kognitos Inc. 2023. All rights reserved.

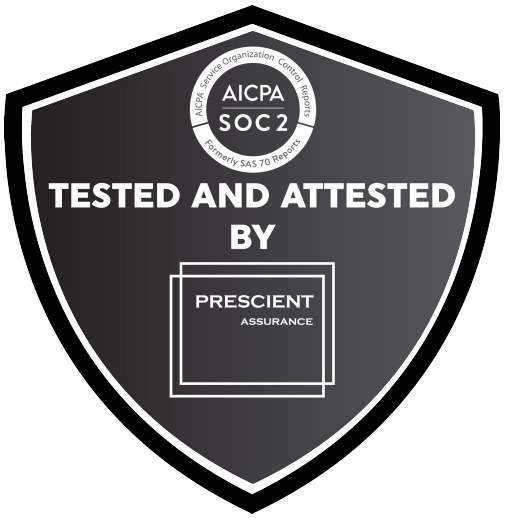
Data Protection and Storage

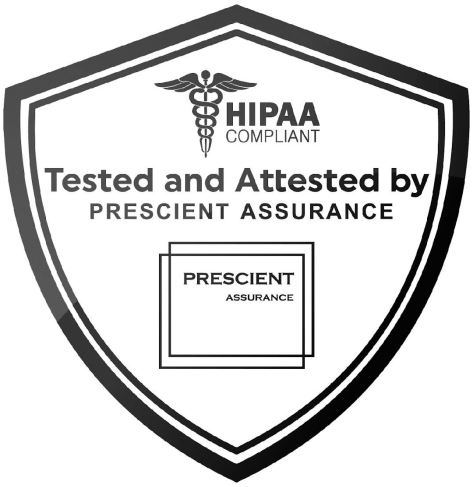
This Document captures the Security, Architecture and Governance details of the Kognitos Platform.

The information contained within the document captures, at a high level, the security details, the data flow through the system, the architecture of the SaaS platform and the Governance hierarchy implemented within the platform.

Data Protection

Kognitos adheres to HIPAA standards and controls, and is audited annually by a third party. We adhere to SOCII controls and have achieved SOCII-Type 2 Certification.





Data Storage

Kognitos stores data from process runs within the procedure and is bifurcated by departments. There are separate instances of execution engine per customer, which ensures privacy and security for the respective client.

Kognitos is hosted in AWS with multi-site redundancy.

The Platform can accommodate specific customer needs including geo-specific data residency upon request.

Data and Information Security

Data Retention

Data is securely persisted with encryption enabled in S3, DynamoDB and AuroraDB. Based on the use-case, Kognitos, Inc. provides the ability to purge customer data either on demand, or based on a retention schedule.

Signing in

Kognitos, Inc. employs Password-Less Authentication. We do not keep any user passwords for Kognitos accounts in our system, substantially reducing the attack vectors possible. All Kognitos users use their email to authenticate their identity.

Information Security

Kognitos is deployed on AWS across multiple availability zones and regions.

All data at rest is encrypted by using security-hardened services like AWS DynamoDB, S3, and AuroraDB with the highest security configuration.

Hierarchy of Governance

Kognitos is arranged in following structure:

Organizations > Departments > Processes

Organization: A customer is listed as an 'Organization' within Kognitos. Customer data sits within this organization and can be further segmented down to the department or process level. Administrators and those with the highest levels of privileges within the customer are able to see organization-wide views, manage permissions for other users, and create/delete departments as needed. Credentials that are required organization-wide are stored and managed at the organization level.

Department: A Kognitos department is a subunit of the organization housing the various processes needed by that department. A common example of a department is Accounts Receivable. At the department level, organizations can manage and view processes and users within that department, manage exceptions and apply learnings.

Process: A process is the basic unit within Kognitos, where automations are built and run in English. The Process page details the current process flow. The process page details the current process flow, facts that are found and used in previous process runs, and any runs that currently require human intervention/exception handling.

Permissions are governed at the organization and department level.

Architecture

Kognitos' Software is provided as a service (SaaS). Users interact with the service via our secure web portal at app.kognitos.com. Anyone that uses Kognitos would need to be able to access the site via a web browser. Additionally, those users must be able to receive emails from app.kognitos.com.

Our integrations use API calls to perform the steps in an automation. To do this, we need API access to an account of the requested application. Configuration varies by application.