/ SECURITY WHITEPAPER

Stacksync

Stacksync: Comprehensive data protection, privacy, and compliance for modern automation and data sync across enterprise systems

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports
®

HIPAA

ISO

CCPA

DPF

Overview

At Stacksync, safeguarding our customers' data is fundamental to everything we build. It enables our customers to operate with confidence in highly regulated and security-conscious environments.

This white paper provides an in-depth overview of Stacksync's security architecture, data protection measures, and compliance posture. It addresses common questions from security, legal, and compliance teams, and references our technical documentation and security resources.

Security-First Platform Design

Stacksync is engineered with a security-first mindset, integrating robust encryption, granular access controls, and continuous monitoring into every layer of the platform. Every operation, whether data sync, workflow automation, or API integration, is governed by strict authentication and authorization policies.

- **Zero Data Retention:** Stacksync does not persistently store your data. Data is processed transiently during sync operations and purged immediately after successful delivery, except in rare cases of destination outages or schema change processing, where data is temporarily queued and always encrypted.
- **Isolated Processing:** Each customer's data is processed in isolated environments with strict access controls and least-privilege principles enforced by hardened IAM policies.
- **Granular Access Controls:** Stacksync uses Role-Based Access Control (RBAC) at the workspace level, supporting multiple roles (Owner, Editor, Viewer) and resource-specific sharing options.

Encryption & Secure Connectivity

- **Encryption in Transit:** All data transfers use TLS 1.2+ for secure, encrypted communication. Any attempt to connect over an unencrypted channel is automatically redirected to HTTPS.
- **Encryption at Rest:** Credentials and configuration metadata are encrypted with AES (military-grade protocol) and regularly rotated keys. Key rotation schedule is frequent, ever changing and autonomous.
- **Advanced Connection Security:** Stacksync integrates with external systems using industry-standard security protocols that align with the tools and practices customers already trust and manage in their daily operations. Stacksync supports SSL-encrypted connections, SSH tunneling, VPC links, OAuth 2, and advanced private networking options for secure integration with customer environments.

Regulatory Compliance & Data Privacy

Stacksync is built to support compliance with leading global data protection and privacy regulations:

- **SOC 2 Type II:** Regular, independent audits verify controls for security, availability, and confidentiality.
- **ISO 27001:** Certified information security management system.
- **GDPR & CCPA:** Full support for data subject rights, data minimization, and regional processing. Stacksync assists customers in responding to data subject requests and demonstrating compliance.
- **HIPAA:** Optional Business Associate Agreements (BAA) for healthcare customers.
- **Data Privacy Framework:** Adherence to cross-border data transfer regulations.

Data Handling & PII

- **PII Processing:** Stacksync may process PII as part of your sync workflows, but never stores it in plain text or outside the business relationship. All processing is limited to customer-defined purposes and applicable law.
- **Data Residency:** Customers can choose their preferred data processing region from over 20 global locations.
- **Data Lifecycle:** Data is processed for only a few seconds (rarely up to one hour) and purged immediately after delivery. Only reduced hashed fingerprints are stored for change detection, not reversible to original data.

Security Operations & Monitoring

- **Continuous Monitoring:** Real-time monitoring and automated threat detection protect against unauthorized access and anomalous behavior. Privileged actions are logged and reviewed regularly.
- **Alerting & Notifications:** Custom alerting rules and real-time notifications ensure rapid incident response and operational reliability.
- **System status monitoring:** All systems are continuously monitored, with real-time status updates available to users at status.stacksync.com.
- **Audit Trails:** Every action, from data syncs to API calls, is logged for compliance and transparency.
- **Vulnerability Management:** Regular penetration testing, vulnerability scans, and continuous improvement of security controls.

FAQs

Q1. Does Stacksync store any of my data?

A: Stacksync does not persistently store your business data. Data is processed transiently during sync operations and purged immediately after successful delivery. In rare cases of destination outages or schema changes processing, data may be temporarily queued and is always encrypted using military-grade AES encryption.

Q2: Is my data encrypted at every stage?

A: Yes. All data is encrypted both in transit (using TLS 1.2+) and at rest (using AES with regularly rotated keys). Credentials and configuration metadata are stored in encrypted form, and any temporarily queued data is also encrypted.

Q3. How does Stacksync handle Personally Identifiable Information (PII)?

A: Stacksync may process PII, PHI or PCI as part of your sync workflows, but never stores any data in plain text or outside the scope of the business relationship. All processing is strictly limited to customer-defined purposes and legal requirements. Stacksync is designed with privacy by design principles and supports compliance with regulations such as SOC 2 type II, ISO 27001, GDPR, CCPA, and HIPAA compliance.

Q4. What compliance certifications does Stacksync hold?

A: Stacksync is certified for SOC 2 Type II and ISO 27001, GDPR, HIPAA, CCPA, and the Data Privacy Framework (DPF-US/EU/UK/CH). Regular independent audits verify our controls for security, availability, and confidentiality, and we provide documentation to support your own compliance needs.

Q5. Can I control who accesses my data and workflows?

A: Yes. Stacksync provides granular, Role-Based Access Controls (RBAC) at the workspace level and resource level. You can assign permissions for users, teams, and integrations, supporting multiple roles such as Owner, Editor, and Viewer.

Contact information

For security, privacy, or data protection inquiries, reach us at security@stacksync.com, privacy@stacksync.com, dpo@stacksync.com or via our contact form at www.stacksync.com/contact

For urgent or critical matters, please contact critical@stacksync.com immediately.

/ START SYNCING TODAY

Stacksync is the leader in real-time and two-way sync for enterprise data and workflow automation.

Read more about Stacksync's security on our security page and security documentation.

Start syncing your enterprise systems today in less than 20 minutes at

www.stacksync.com

Stacksync