Sana Agents security whitepaper

Last updated: July 4, 2025

Sana™

Table of contents

Sana Agents security whitepaper

Last updated: July 4, 2025

Introduction

Sana is dedicated to building a cutting-edge versatile AI Agent platform tailored to each organization's needs. Our core focus as a company is on information security, legal compliance, and privacy, which are integrated into every aspect of the design, development, and deployment of all Sana Agents services.

The purpose of this paper is to outline our efforts and the attributes of Sana Agents that address security, compliance, and privacy-so that end users can benefit from our services with peace of mind.

About Sana Agents

Sana Agents is a web- and mobile-based, enterprise-grade platform for creating expert AI agents grounded in your company's knowledge.

Sana Agents integrate information from many popular and widely-used enterprise sources such as Sharepoint, Google Drive, Confluence, Salesforce and many others.
They only access data that users and administrators have allowed them to query. This approach ensures strong data security and follows a modern approach to AI safety and information security.

Compliant with globally-leading standards and regulations

Sana Agents maintains compliance with the world-leading security and privacy standards and regulations - SOC 2 Type II, GDPR, and ISO/IEC 27001:2022.

Sana compliance team proactively monitors and implements updates to global security and privacy requirements to stay on top of emerging standards and requirements, and deliver the best-in-class security.

The most up-to-date reports, controls status and updates can be found on a dedicated Trust Portal: https://trust.sanalabs.com/

Security of AI systems and models

Sana upholds strict security policies for the use of AI in all its products. All models are carefully selected and vetted based on the model scorecard, performance, security and safety ratings. In addition, prompting, input and output validation techniques are used to prevent threats like prompt injection, data exfiltration, unsafe outputs.

Strict Zero-Data Retention policy and full prohibition of training models on customer data are enforced.

Sana is aligned with the latest stage of EU AI Act implementation, conducts AI impact and risk assessment, and integrates proactive security and safety measures as part of product development and operations.

How we uphold information security in product and infrastructure

Our ISMS is ISO/IEC 27001:2022 certified, and all security measures, controls, procedures are mapped to the standard.

Sana has implemented a Secure Development Lifecycle that integrates security into all aspects of product development - from design to operations. All engineers are annually trained on OWASP best practices and privacy-by-design approach. AI-assisted code review is static code analysis and is tasked with identifying vulnerabilities and shortcomings of code, and effectively mitigating it.

Regular third-party penetration testing by independent highly-skilled independent professionals, continuous vulnerability management, and secure computing for all operations ensure the security baseline.

How we control access to our systems and processes

Strong identity and access management for human- and service accounts is at core of Sana's approach:

- Role-based, least-privilege permissions.
- Strong multi-factor authentication (FIDO2/WebAuthn/biometric passkeys/passwordless solutions) for privileged access.
- Highly automated lifecycle management for onboarding/offboarding.
- System and data access is logged, centrally monitored, and reviewed through a next-generation SIEM.
- Physical access to data centers operated by cloud infrastructure providers is controlled with biometric security, 24/7 surveillance.
- Strict logical separation of all customer environments is enhanced with robust row-level security policies.

- Data is always protected in transit (TLS 1.2+) and at rest (AES-256).
- Regular vulnerability scanning, automated anomaly detection, and adaptive firewalls further reinforce access boundaries.

How we manage risk

Risk management is integral to all security, privacy, and compliance work at Sana. It defines improvement directions, helps prioritize and drive them forward.

Sana relies on scheduled risk assessments, continual compliance audits, an executive-reviewed and led risk register, and red-team/incident simulations.

Automated alerting and up-to-date assessment, mapping, and analysis of risks inform evolving controls and ensure a rapid response.

How we secure operations

Operations are safeguarded using:

- Advanced anti-malware/anti-virus systems
- Automated security updates and patching
- Annual phishing simulations and continuous security training
- Centralized logging and real-time threat detection
- Automated response and root cause analysis for exceptions/anomalies

How we uphold security with our staff

All team members undergo thorough security and privacy onboarding, annual training updates, and must adhere to strict codes regarding confidentiality and business ethics. Confidentiality agreements are a requirement for employment and engagement, with regular acknowledgements of privacy policy compliance.

How we partner with sub-processors and subcontractors

We diligently vet suppliers during the procurement process and only use suppliers for specific and necessary purposes to enhance Sana for our end-users. We require the same quality of technical and security measures from our suppliers as we uphold for ourselves. For our most critical sub-processors, we require ISO 27001 certification and SOC 2 Type II report, and GDPR compliance.

All contracts with chosen suppliers address our demands on the supplier's IT environment and information security measures. Each supplier is obligated to account for their technology, routines, and processes as well as their IT and information security policies.

Non-disclosure agreements, DPAs, and other relevant regulatory agreements are signed by our suppliers before the service is taken into use, and we conduct regular controls of suppliers' security, compliance and other aspects of each agreement with Sana.

How we ensure business continuity

Robust data backups are one of the three pillars of our continuity plan. Intelligent automation and trained personnel manage and follow up on backup execution to ensure the integrity, confidentiality, and accuracy of the backup data. Backups are stored for 30 calendar days.

The second pillar of our continuity plan is the Incident response processes and routines that are carried out when a serious problem occurs. We continually work on keeping processes and routines updated. The continuity plan is tested at intervals based on regular risk assessments.

Our third pillar is to have a high degree of digitization, and all the services and tools are digitally accessible using Google Accounts' SAML-based Federated SSO. Our IT and product infrastructure is highly distributed with multiple failover regions and locations, vehicle maintaining strict compliance with local processing requirements. This allows Sana to efficiently and quickly recover from severe disruptions caused by unpredictable events such as earthquakes, fires, epidemies. Following the same approach, most employees are equipped to and can continue to work from other locations even if our offices are closed or not accessible due to an extreme event.

Frequently Asked Questions

How do Sana algorithms incorporate privacy and security requirements?
Sana Agents internal algorithms are optimized for the efficient and safe data retrieval, transformation and handling of AI responses. The algorithms are developed and trained solely on pseudonymized and pre-processed datasets. Customer content remains private and is never used in third-party model training.

Will our data be used by third-parties to train their AI models?
No, Sana enforces strict policy about never allowing third-party models to be trained on customer data. In addition, Sana enforces Zero-Data retention with these model providers, meaning that the data is deleted immediately after processing by a model.

How does Sana Agents platform ensure the security of our data?
Sana isolates all customer data using a single tenant architecture and strict row-level security policies that ensure robust logical and programmatic separation between customers. Data at rest is encrypted with AES 256 and data in transit is encrypted with TLS 1.2+.

Will Sana Agents index our data?
Data integrated into the platform is securely stored and indexed within logically segregated cloud environments in an AI-digestible format, with encryption in transit (TLS 1.2+) and at rest (AES-256). Some integrations are only available through real-time API connectors. For those integrations, data is not indexed and is only accessed at run-time.

What documents can a user see in the company workspace?
Granular access controls as set by administrators and integration type-whether via direct upload, private, or shared connections-determine document visibility. For private integrations, the access rights of a user are replicated - this means that Sana allows a user to only access the documents that are available based on user's permissions in an integrated system. Admins can create a company-wide integration that would let everyone on the platform access a set of documents, as defined by the administrator.

Flexible Role-based access control (RBAC) and collection permissions set access boundaries to and in the Sana Agents workspace.

Can I, as an admin, enable integrations on behalf of my organization?
Admins have full control over organizational integrations and which data feeds are accessible to platform intelligence. Sana platform also provides a visibility into integration status, the documents accessible via it, the last sync time, and informs an administrator in case of any issues.

Will employees at Sana be able to see our content data and search queries?
Sana employees do not have access to your workspace by default, and will only be able to access it if you grant them access by extending an invite. Invited Sana employees cannot view any files without specific permission, and do not have access to search queries. Sana employees involved in solution engineering, may have access to downvoted queries in Free and Team tiers, in order to improve the experience and troubleshoot the issues, with all user information being anonymized. Developers may receive access to underlying databases on the need-to-know and least-privilege basis with detailed audit trails.