SugarCloud Information Security FAQs

Updated August, 2025

This document provides an overview of SugarCRM's Cloud Platform security practices, controls, and compliance measures to help customers understand how their data is protected within the SugarCloud Platform and associated products. The SugarCloud Platform suite includes Sell, Serve, Market, Identity, Mobile, Sales-i.

1. Data Ownership and Usage

What types of data can be stored?

Customers may store any business-related data, including Personally Identifiable Information (PII), within the Platform. However, the Platform is not designed or intended for storing or processing Payment Card Industry (PCI) data, such as credit card information. Customers are responsible for ensuring that their data handling practices comply with all applicable laws, regulations, and SugarCRM's Terms of Service available here: https://sugarcrmstg.wpengine.com/legal/agreements/customers/terms-of-service/.

Who owns the data?

Customers retain full ownership of their data throughout the service contract. Upon termination, data remains accessible for up to 120 days (30 days for Sales-i), after which it is permanently deleted unless requested sooner.

Will SugarCRM use my data for other purposes?

No. Customer data is used exclusively for the purpose of delivering the services as described in the applicable service terms. SugarCRM does not sell or share customer data with external parties for other purposes.

What data is stored during DocMerge operations?

Only template metadata (e.g., field names, relationships) is stored temporarily. Customer data is not retained post-merge. All data is encrypted in transit and at rest.

2. Hosting and Infrastructure

SugarCRM is hosted on Amazon Web Services (AWS), with data center regions in:

- United States
- United Kingdom
- Germany
- Australia

Sales-i, a SugarCRM offering, is hosted on Microsoft Azure, with data center regions in the United States, United Kingdom, Germany, and Australia.

Does data remain in the selected region?

Customer data, including backups and snapshots, is stored within the selected region. However, in some cases, limited access by authorized support personnel outside the region may occur to resolve technical issues.

Such access is strictly controlled, logged, and protected through VPN-connected bastion hosts. When data is accessed from outside the EU/EEA, it is governed by Standard Contractual Clauses (SCCs) and aligned with GDPR requirements, including technical and organizational safeguards.

How is access to customer data controlled?

Customers manage access to their environments using configurable role-based access controls (RBAC). This allows fine-grained assignment of permissions based on user roles and responsibilities.

SugarCRM support staff access is limited to authorized personnel and is permitted only when necessary, such as in response to a customer support request. Access is:

- Individually authenticated (no shared accounts)
- Approved through a ticketed process
- Logged, monitored, and subject to audit

All access follows the principles of least privilege and purpose limitation and is regularly reviewed as part of our SOC 2 and ISO 27001 compliance programs.

Is the hosting environment multi-tenant?

Yes. SugarCloud uses logical separation at the database and file system levels, with unique encryption keys per customer. Dedicated hosting options are available upon request.

3. Integrations

Is SugarCloud a standalone service?

Yes. SugarCloud operates as a standalone cloud service. However, customers can integrate on-premises and other cloud systems using SugarCRM's RESTful APIs.

Who is responsible for securing integrations between on-prem and cloud services?

Customers are responsible for securing any external systems they connect to the SugarCloud Platform. Sugar's APIs use industry-standard encryption (TLS 1.2 and 1.3) to protect data in transit.

4. Internet Accessibility

Is the Platform accessible from the internet?

Yes. SugarCloud is a web-based application accessible via supported browsers. See the Supported Platforms page for details here:
https://support.sugarcrm.com/Resources/Supported_Platforms//.

Can internet access be restricted?

Yes. Customers can configure IP allow/block lists to restrict access. Note: This feature is not currently available for the Sales-i product.

5. Identity and Access Management

What identity providers are supported?

SugarCloud supports SAML and OpenID for third-party identity integration.

Are password policies configurable?

Yes. Customers can define password length, complexity, and expiration policies. Multifactor Authentication (MFA) is supported across the Platform.
Note: MFA support for Sales-i is coming soon.

Does SugarCRM monitor login activity?

Yes. The Platform is monitored 24/7/365 for suspicious login behavior, including brute force attempts and anomalous access patterns.

Can inactive accounts be disabled automatically?

Yes. Customers can configure automatic account deactivation based on inactivity.
Note: This feature is not currently available for the Sales-i product.

6. Data Protection

What security controls are in place?

SugarCRM applies a comprehensive defense in depth strategy to safeguard customer data and system integrity. This layered approach includes:

- **Endpoint Detection & Response (EDR):** Monitors and responds to threats across devices and environments.
- **Security Information and Event Management (SIEM):** Aggregates, correlates, and analyzes logs and security events across the environment to detect anomalies and support incident response.
- **Web Application and Network Firewalls:** Protect against unauthorized access and malicious traffic.
- **Secure Software Development Practices:** Includes static, dynamic, and interactive code analysis throughout the SDLC.
- **Vulnerability Management:** Regular scanning and expert 3rd party penetration testing to identify and remediate risks.
- **Data Loss Prevention (DLP):** Prevents unauthorized data exfiltration or exposure.
- **Bug Bounty Program:** Engages external researchers to identify vulnerabilities.
- **Employee Security Awareness:** Mandatory training, phishing simulations, and ongoing education.
- **Third-Party Risk Management:** Evaluates and monitors vendors for security and compliance.
- **Distributed Denial-of-Service (DDoS) Protection:** Mitigates service disruption from large-scale attacks.
- **External Certifications:** SugarCRM is SOC 2 Type II audited and ISO 27001 certified.
  Note: Sales-i inclusion is in progress.

How is data protected in transit and at rest?

- **In transit:** TLS 1.2 and 1.3 encryption
- **At rest:** AES-256 encryption
  Note: Encryption outside the Platform is the customer's responsibility.

How are backups secured?

Backups are encrypted, access-controlled, and integrity-verified. Customers can retrieve backups via SFTP over TLS, manually or on a schedule.

Is AI used in SugarCRM products?

Yes. The Intelligence add-on includes predictive analytics, sentiment analysis, and generative AI. For more information see:

- Intelligence Add-on Overview: https://sugarclub.sugarcrm.com/engage/b/sugar-news/posts/new-intelligence-add-on
- Product Terms: https://www.sugarcrm.com/legal/agreements/customers/product-terms/

7. Application Security & Patching

Does SugarCRM follow secure development practices?

Yes. Security is embedded throughout SugarCRM's Software Development Lifecycle (SDLC). Developers receive secure coding best practices training upon hire and annually thereafter.

How are applications and APIs secured?

SugarCRM uses multiple code analysis tools and follows secure coding practices aligned with the OWASP Top 10. All pull requests are scanned for vulnerabilities, and hotfixes are issued for supported versions when needed.

Is penetration testing performed?

Yes. SugarCRM engages expert, certified third-party penetration testers not less than annually to assess production systems, APIs, and cloud infrastructure, using industry standards like OWASP. Internal vulnerability scans are performed regularly. Findings are risk-ranked, remediated, and validated through follow-up testing. Executive summaries are available upon request, and results inform our broader risk management efforts.

What is the vulnerability patching policy?

- Critical: within 14 days
- High: within 30 days
- Medium: within 90 days
- Low: within 180 days
  Code vulnerabilities are patched via release cycles or hotfixes.

8. Incident Response & Breach Notification

Is there a formal incident response plan?

Yes. SugarCRM maintains a documented incident response plan that is reviewed at least annually to ensure effectiveness and alignment with evolving threats. This process is independently validated through our SOC 2 and ISO 27001 audits. In addition, we conduct post-incident reviews to capture lessons learned and continuously strengthen our response capabilities.

Is malware protection in place?

Yes. SugarCRM uses industry-leading Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) solutions across all environments. Monitoring is performed 24/7/365 by internal and external security teams.

How quickly will customers be notified of a breach?

Customers are notified of suspected data breaches without undue delay.

Does SugarCRM carry cyber insurance?

Yes. SugarCRM maintains Cyber Liability coverage.

9. Compliance

Is SugarCRM GDPR compliant?

Yes. SugarCRM acts as a data processor and adheres to the requirements of the General Data Protection Regulation (GDPR). Customers, as data controllers, are responsible for ensuring their own compliance with GDPR obligations. To support this, SugarCRM offers a Data Processing Addendum (DPA) for customers in the EU, which includes the European Commission's approved Standard Contractual Clauses (SCCs) to ensure lawful international data transfers.

Additionally, SugarCRM is certified under the Data Privacy Framework, enabling customers in the EU, Switzerland, and the UK to transfer personal data to SugarCRM in the United States without the need for Standard Contractual Clauses. More information is available via the Data Privacy Framework participant search here: https://www.dataprivacyframework.gov/s/participant-search. For questions, please contact: dataprivacy@sugarcrm.com.

Is SugarCRM ISO 27001 certified?

Yes. SugarCRM is ISO 27001 certified.
Note: Sales-i is a newly acquired product and is being integrated into the certification scope.

Does SugarCRM comply with other security and privacy frameworks?

Yes. In addition to completing an annual SOC 2 Type II audit and maintaining ISO 27001 certification, SugarCRM aligns with recognized industry standards and practices to support a robust security and privacy program:

- **Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM):** SugarCRM is listed in the CSA STAR Registry (Level 1 – Self-Assessment).
- **Privacy Regulations:** Supports customer compliance with GDPR, CCPA, and other global privacy laws.
- **Cloud Infrastructure:** SugarCRM leverages secure hosting partners including AWS and Microsoft Azure, both of which maintain extensive certifications (e.g., SOC 2, ISO 27001) and strong security controls.

These frameworks and partnerships form the foundation of our security governance, risk management, and compliance programs.

Do employees receive security training?

Yes. All employees complete onboarding and annual security & privacy training. Developers receive monthly security briefings and phishing simulations are conducted regularly.

Is there a vendor risk management program?

Yes. SugarCRM maintains a formal Vendor Risk Management Program to assess and monitor third-party service providers. Vendors are evaluated before engagement based on the sensitivity of the data or services involved and are regularly reassessed thereafter. As part of this process, SugarCRM reviews the vendor's security, privacy, and compliance posture, and ensures that contracts include binding commitments to maintain appropriate security and data protection measures. The program is documented and independently verified through our SOC 2 Type II and ISO 27001 audits.

Are subprocessors used?

Yes. A list of subprocessors is available here: https://www.sugarcrm.com/why-sugar/trust/data-protection/sub-processors/.