SugarCloud
Information Security FAQs

Updated January 31st, 2024

CONTENT

Acronym or Term	Definition
The Platform	The SugarCloud suite of tools that we provide in the cloud. This includes Sell, Serve, Market, Identity, Mobile, and so on.
PII	Personally Identifiable Information. This is a privacy term used to denote data such as name, address, e-mail, phone number or other information that is used to identify individuals.
PCI	Payment Card Industry. This is typically used as shorthand to denote credit card information.

Question	SugarCRM Information

What types of data can be stored in the Platform?	The Platform collects, accesses, processes, and stores allce information input by our customers. This can include PII or other potentially sensitive information. Customers should not store or hold PCI or other regulated information not specifically approved. For more details, please see the Master Subscription Agreement: https://www.sugarcrm.com/legal/agreements/customers/master-subscription/ **Important Note Regarding HIPAA:** While SugarCRM's products are not configured for HIPAA compliance, we do have some partners who offer HIPAA compliance for our products. Please note that this is not available in all regions, so please check with our sales team to see if this solution will work for your specific situation. **Important Note Regarding PCI:** While SugarCRM's products are not configured for PCI compliance, we do have some partners who offer PCI compliance for our products. Please note that this is not available in all regions, so please check with our sales team to see if this solution will work for your specific situation. **Important Note Regarding FedRAMP:** While SugarCRM's products are not configured for FedRAMP compliance, we do have some partners who offer FedRAMP compliance for our products. Please note that this is not available in all regions, so please check with our sales team to see if this solution will work for your specific situation.
Will my company maintain ownership of our data throughout the life of the service contract?	Yes, customers maintain ownership of their data in the SugarCloudd Platform. After the service contract is terminated, you have up to 90 days of access to your data after the service contract. After 90 days (or sooner if you request it) all data is irrevocably destroyed.
Will my data be used for anything else?	SugarCRM will never sell or share your data with anyone outside of the company. For more details on how your data is processed and used by SugarCRM, please see our privacy policy: https://www.sugarcrm.com/legal/privacy-policy/
What data is stored when using the DocMerge function?	When using the DocMerge function, only the metadata about the template (field names, relationships definition) is stored for the purposes of completing the merge. Customer data is not stored in the

	server after the merge is completed. All data is encrypted in transit and at rest.

Hosting Information	SugarCRM Information
How is SugarCRM hosted?	SugarCRM partners with Amazon Web Services (AWS).
Where is SugarCRM hosted?	The Platform* is currently available in these regions: • USA • Ireland • Australia • Canada • Germany • UK • Singapore * Please note not all Sugar products are available in all regions listed above. For more details contact your account executive.
Does my data leave the hosting region?	No, the region you choose when you sign up for the Platform is where your data will stay. All snapshots and backups are kept in region as well. SugarCRM support personnel access the Platform via in-region, VPN connected bastion hosting. This allows our support people to be geographically dispersed but the data always stays in region. Personnel are also regularly trained in security and privacy best practices.
Is the hosting multi-tenant?	Yes, the Platform is multi-tenant where instances share resources, but each customer's data and files are stored in tables specifically to that customer. Each database has unique credentials and a wide range of security controls in place. The tech is multi-tenant with logical separation at the file system and database levels. This includes the use of unique encryption keys for each customer database. The technologies used to logically separate the Platform vary depending on the specific product. SugarCRM also offers a range of "Premium Cloud" options which provide you with a dedicated hosting environment. Please ask your account executive for more details.
How is access to my data controlled?	You have complete control over your user access and the Platform comes with robust out of the box role-based access controls (RBAC). SugarCRM also supports a portfolio of 3rd party identity solutions.

What controls are in place to ensure that your support team always accesses my data securely?	Sugar maintains a comprehensive information security program which includes a strict customer data access process. Access to customer instances can only be granted through a support ticket, ensuring all access is tracked and audited. Any connections made by support personnel are established through encrypted channels.
If your support teams accesses the Platform using privileged access, is this granted in a way that can identify the activities of each individual?	Yes, in addition to the above, each support engineer has their own, unique credentials used for privileged access. As such, we are able to identify the activities of each individual if required.
Does the Platform log privileged access to the system and our data?	Yes, in addition to the above all privileged access is logged.

Connectivity to Managed Systems	SugarCRM Information
Is the Platform a standalone service, or will it interface with any of the on-premises systems managed by my company?	The Platform is a standalone service, however you can interface with on premises systems via our APIs.
Who manages and owns the responsibility to ensure the interfaces between the on-prem service(s) and cloud service(s) are secure?	If you connect any external services to the Platform, you will be responsible for the security of that service. The Restful API integration tools which Sugar provide use industry standard encryption ensuring data is protected in transit.
How does the cloud service interact with systems hosted on-premises?	All API communications between systems use TLS 1.2 and TLS 1.3 encryption.

Internet Accessibility	SugarCRM Information
Will the cloud service be directly accessible from the Internet or will controls be implemented to limit access (e.g., geo-fencing, IP allowed list, secure cloud connect service, etc.).	The Platform is a web-based application that can be accessed via a web browser. A list of our supported browsers can be found here: https://support.sugarcrm.com/Resources/Supported_Platforms// The Platform also supports IP based allow lists and block lists should you require this.

Identity and Access Management	SugarCRM Information
How does SugarCRM provide authorization and 3rd party identity support?	The Platform supports both SAML and OpenID identity providers.
Does SugarCRM support password and access controls such as strength, length, and complexity?	Yes, you are able to configure the Platform to meet your password length and complexity requirements. The Platform also supports MFA*. ** Sugar Market coming in 2024 (H1)*
Does SugarCRM monitor for unusual or risky logins (e.g. impossible logins, brute force attempts, etc.)?	Yes, we utilize a range of security technologies for monitoring your instance, including in relation to unusual or suspicious login activities. These technologies are monitored by our operations and security teams 24/7/365.
Can the Platform automatically disable accounts after a certain period of activity?	Yes, the Platform can be configured to disable inactive accounts. This can be tailored to meet your own security or access control policy.
Does the Platform support Multifactor Authentication?	Yes, the Platform supports a range of Multifactor Authentication (MFA) options, for example via your existing SSO provider, or IDM native*. ** Sugar Market coming in 2024 (H1)*

Data Protection	SugarCRM Information
What security controls does SugarCRM use to help protect my data?	When it comes to protecting your data, SugarCRM uses the concept of “defense in depth”. This means we use a wide range of security controls to protect your data in line with industry standards. This includes (but is not limited to): - Endpoint Detection & Response (EDR). - Web Application Firewalls (WAF) and Network Firewalls. - Static, Dynamic and Interactive Code Analysis. - Vulnerability Scanning and Penetration Testing. - Data Loss Prevention (DLP). - Bug Bounty Program. - Comprehensive Employee Screening and Awareness Training. - Risk and Third Party Vendor Management Programs. - DDoS Protection.

	- External Audits and Certifications (currently SOC 2 and ISO 27001). For more information about our Information Security Program please contact security@sugarcrm.com
How is data in transit protected?	All data in transit is TLS 1.2 and TLS 1.3 encrypted to protect the confidentiality and integrity of your data.
How is data at rest protected?	Your data within the Platform is encrypted at rest using AES-256 encryption. Outside of the Platform itself, implementation of encryption at rest is the responsibility of the customer or partner (if required). The Sugar application also supports field level encryption using the blowfish cipher: https://en.wikipedia.org/wiki/Blowfish_(cipher)
How are backups secured against unauthorized access?	SugarCRM uses a combination of security controls to ensure backups are protected. This includes the principle of least privilege for all employee access, encryption at rest and integrity monitoring technologies including signatures. When it comes to giving you access to your backups, we provide an SFTP service allowing you to download backups over a TLS protected connection. This can either be done manually or based on a regular interval.

Application Security & Patching	SugarCRM Information
Does SugarCRM's software development practices adhere to, or comply with, industry recognized secure development practices?	Yes, SugarCRM embeds security throughout our entire Software Development Lifecycle (SDLC). Security is also a key area of focus for our developer training program. All of our security architects and engineers go through yearly "best practices" training and we hold monthly security focused meetings to discuss emerging trends. In addition to the above, SugarCRM uses several industry leading code analysis and web application security tools to test every pull request. We do this multiple times with several tools as it helps us reduce the likelihood of vulnerabilities being present in our applications. For any security issues that are found we also provide hotfixes for all supported versions in order to allow our customers to be running a secure instance.

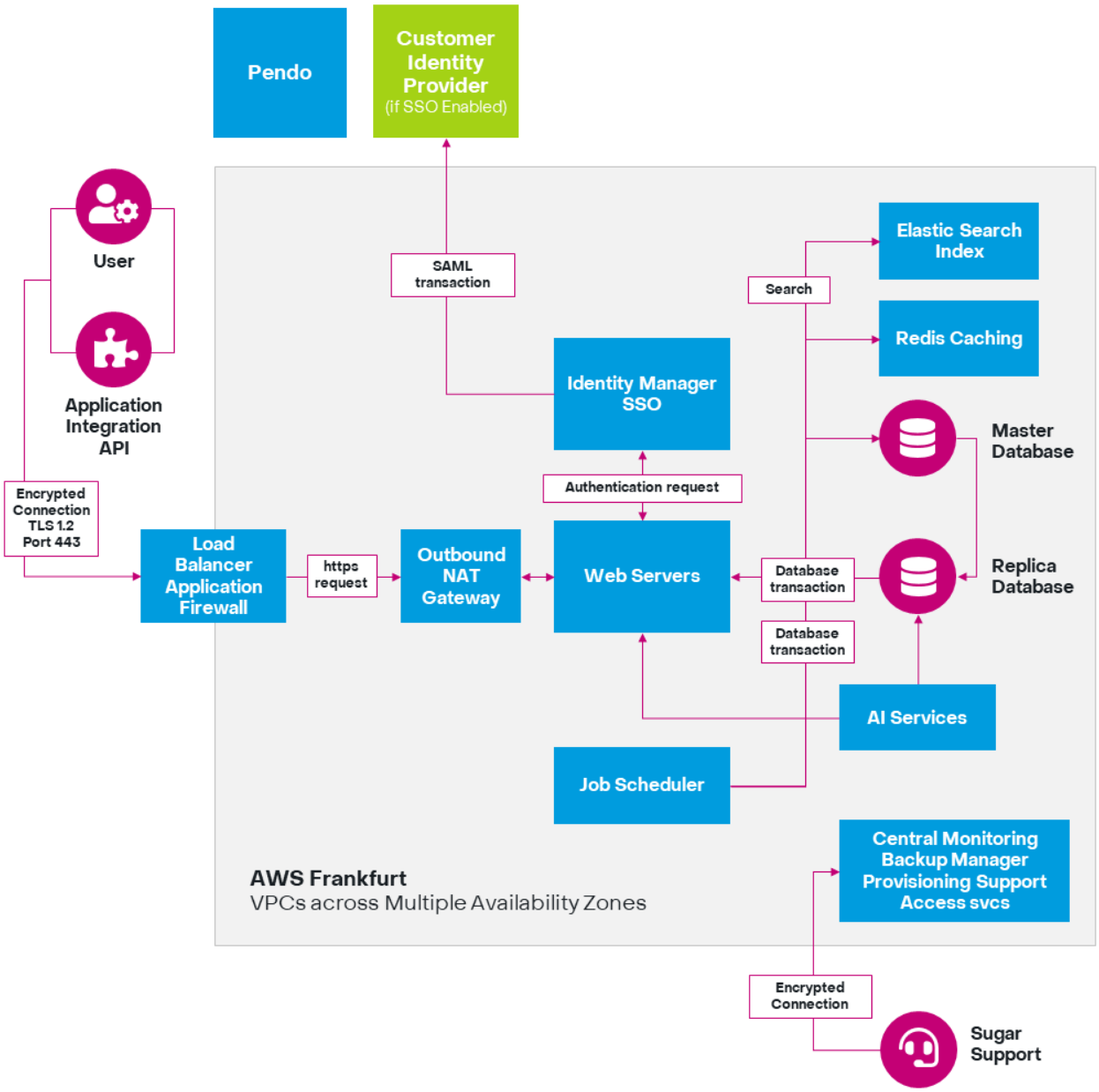
Do you ensure your applications and application programming interfaces (APIs) are developed and secured in a way that protects against the OWASP Top 10 vulnerabilities?	Yes, the Platform is designed with security in mind, which includes development and testing to identify vulnerabilities like those listed in the OWASP Top 10. The Platform is also penetration tested and vulnerability scanned regularly. A copy of pen test reports is available upon request.
Does SugarCRM undergo penetration testing?	Yes, both our corporate systems, and the Platform are penetration tested at least yearly. SugarCRM partners with an external provider for penetration testing and also conducts its own internal vulnerability scanning.
When are vulnerabilities patched?	SugarCRM's vulnerability management policy states that infrastructure based vulnerabilities are patched within the following timeframes: Critical – 14 Days High – 30 Days Medium – 90 Days Low – 180 Days Code based vulnerabilities are addressed in product release cycles. If a code vulnerability has been externally reported (for example via a Penetration Test or Bug Bounty report), we release hotfixes within the timeframes listed above.

Incident Response and Breach Notification	SugarCRM Information
Does SugarCRM have a formal security incident response plan or procedure?	Yes, SugarCRM has a documented incident response plan and ensures that a detailed security incident response test takes place every year. We believe in ensuring that everyone in our organization is prepared in the event of a cyber incident. We partner with a leading incident response preparedness company who provide a detailed, realistic exercise. Any findings are then integrated into our continual improvement program. Regular incident response tests are also a requirement for our SOC 2 and ISO 27001 attestation and this is verified by external auditors every year.
What malware protection do you have in place?	SugarCRM utilizes one of the security industry's top anti-malware EDR and MDR solutions. This software is deployed across all workstations and cloud environments, and both our

	internal security team and our managed security services providers monitor the Platform 24/7/365.
In the event of a data breach, how soon will I be notified?	Notifications to customers on suspected data breaches occur without undue delay.
Does SugarCRM have cyber insurance?	Yes, we have Cyber Liability coverage.

Compliance	SugarCRM Information
Is the Platform compliant with GDPR?	SugarCRM customers are the data controllers and are required to have their systems and processes in place to comply with GDPR. Even though Sugar is GDPR compliant, we are not responsible for customers' obligations as data controllers. If SugarCRM will be processing personal data of EU citizens on your behalf, please review our DPA: https://www.sugarcrm.com/legal/agreements/customers/data-privacy/data-processing-addendum/ GDPR requires that data controllers (which may include your company) and data processors (in this case SugarCRM) enter into an agreement setting forth the rights and obligations of the parties for data processing and access. More information on GDPR is available in our SugarClub community. We are unable to provide specific legal advice for your company. If you have questions about whether you are required to comply with GDPR, please contact your attorney(s). Additionally, SugarCRM is certified under the Data Privacy Framework. This means our customers based in the EU, Switzerland and UK can safely transfer (or allow access to) personal data to Sugar in the US without the need for putting Standard Contractual Clauses in place. For information on this please refer to the following link: https://www.dataprivacyframework.gov/s/participant-search If you have any questions please email dataprivacy@sugarcrm.com
Is SugarCRM ISO 27001 compliant?	Yes, in Q4 2023 SugarCRM passed its ISO 27001 audit.

Does SugarCRM comply with major security frameworks and standards?	SugarCRM is SOC 2 Type II and ISO 27001 compliant. The attestation is completed yearly by an external auditor and can be provided on request. Furthermore, our hosting partner AWS is ISO27001 compliant. In addition to the above, SugarCRM's information security and privacy programs are aligned to several industry standards including ISO27001, CCM, NIST CSF, GDPR and CCPA.
Do your employees receive training on security and/or privacy?	Yes, SugarCRM's security and privacy awareness program includes training for all new hires when they start with us, and all employees must complete annual refresher training. Developers also receive security specific training as part of monthly "tech talk" sessions. In addition to the above, our security team issues regular security awareness bulletins and performs quarterly phishing simulations. Any employees who fail the phishing simulations are given additional, constructive training to help them learn how to avoid being socially engineered in the future.
Does SugarCRM have a vendor or third-party risk management program?	Yes, our vendor risk management program ensures that all vendors, service providers, and other third parties are risk assessed before contractual agreements are put in place. Third parties are sent security questionnaires and our compliance team reviews their certifications and security policies regularly. The vendor risk management program is part of our yearly SOC 2 Type II and ISO 27001 attestation - a copy of the report is available upon request.
Does Sugar have subprocessors? What activities do they undertake?	SugarCRM's list of subprocessors can be found at: https://www.sugarcrm.com/why-sugar/trust/data-protection/sub-processors/.
What does the dataflow of information which could include PII look like for the Platform?	Please see diagram below.


Pendo
Customer Identity Provider
(if SSO Enabled)
User
Application Integration API
SAML transaction
Elastic Search Index
Search
Redis Caching
Identity Manager SSO
Master Database
Authentication request
Encrypted Connection TLS 1.2 Port 443
Load Balancer Application Firewall
https request
Outbound NAT Gateway
Web Servers
Database transaction
Replica Database
Database transaction
AI Services
Job Scheduler
Central Monitoring
Backup Manager
Provisioning Support
Access svcs
AWS Frankfurt
VPCs across Multiple Availability Zones
Encrypted Connection
Sugar Support