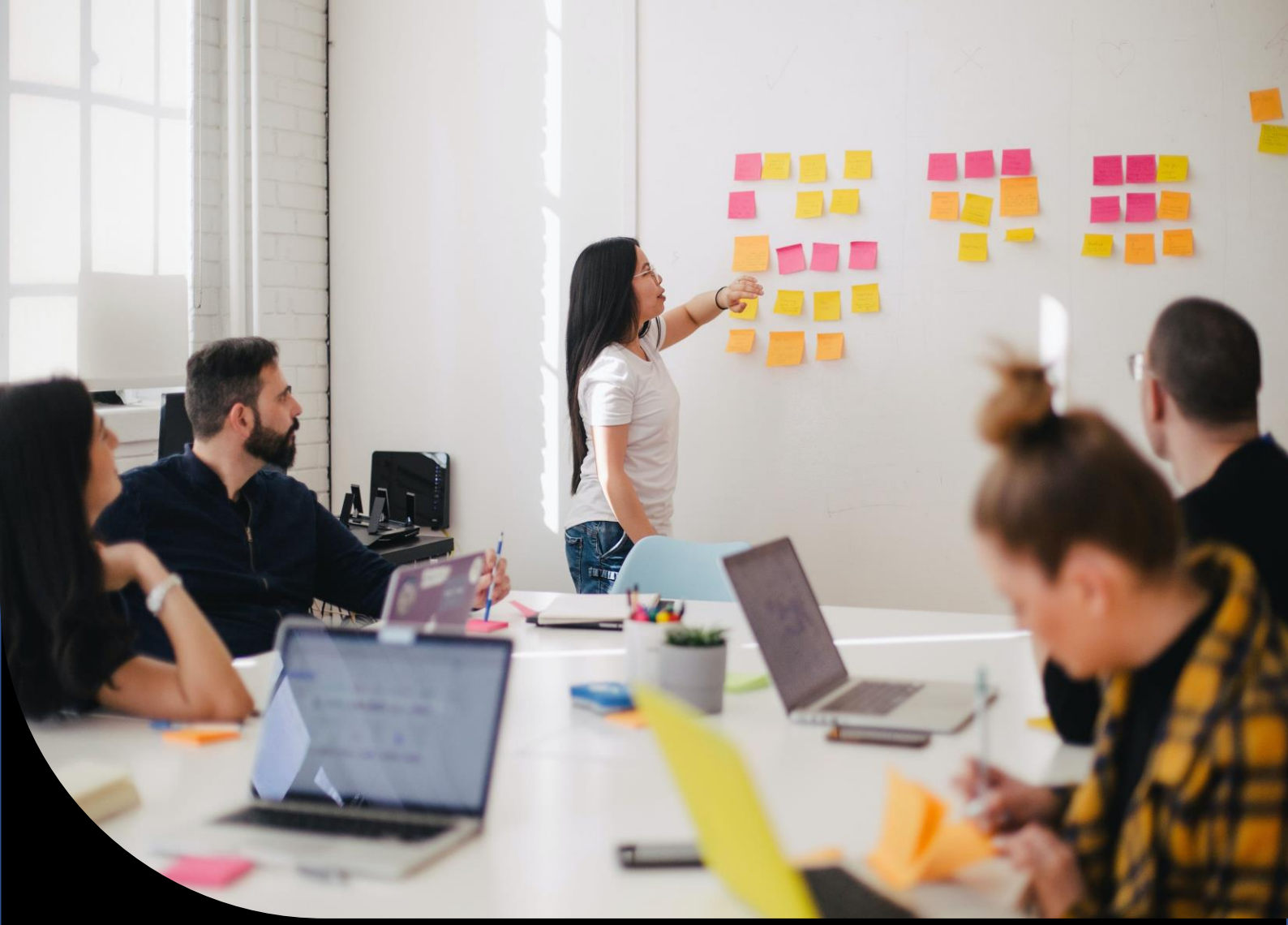

Information security and governance

# Frequently Asked Questions

# Sage 300

How we protect your data and
maintain the integrity and continuity
of critical systems

Sage

Sage and Sage 300's security and governance work to keep your system safe and reliable.

We've written this document to answer important security and governance questions in detail, covering policy, compliance (when applicable) and specific technical and organizational control measures for Sage 300 web screens.

*Our approach to security is under continual review, so we may change any descriptions in this document at any time without notice.*

Published Date: September 21, 2021 Revised Date: June 2, 2025

# Table of Contents

# Sage Governance

**Has Sage implemented a security governance program?**
Yes. We take the security of our customers' data very seriously. We know how important it is to keep this data safe, so we have put in place a set of protective measures, based upon recognized industry best practices. Further information is available here: Sage Governance

**What security policies does Sage have?**
Sage policies are published and available to all employees on our Intranet, supported by standards and procedures based on leading information security frameworks. These cover information security, acceptable use of Sage systems and applications, secure software development, information classification and data handling.

**Does Sage have a dedicated Security Team?**
Sage has a Deputy Chief Information Security Officer (CISO) reporting directly to the EVP Chief Risk Officer, who heads a dedicated Global Security team working across the enterprise. The team's functions cover Product Security and Architecture, Compliance, Security Engineering, Cyber Defence Operations, Business Continuity and Crisis Response. Sage also has a Global Risk and Compliance team overseeing all business risks.

**Does Sage follow industry best practices?**
Yes. Sage applies various industry-based guidelines and processes into our Secure-SDLC (SSDLC). The Sage SSDLC is based, in part, on the following:

- Microsoft security development lifecycle (MS SDL)
- Open Web Application Security Project (OWASP) Top 10 for security testing
- STRIDE methodology for performing threat modelling
- Security controls based on OWASP ASVS

**Do employees, contractors and temporary staff receive information security training?**
Sage conducts regular security training and awareness campaigns to embed and reinforce a culture of security throughout our organization. Training is a mandatory requirement for all new employees and includes online training, process-specific refreshers and best practice updates for security, risk, anti-bribery and corruption, and privacy and is updated annually or when a significant change occurs. The training program includes blended learning methods such as gamification, exercises without repetition, live invocation, and micro-learning to ensure that the security culture is deeply embedded into our daily working practices.

Certain roles, such as product engineers, receive additional annual mandatory training on secure software development best practices. We also have a Security Champion Program within Product Engineering. Security Champions work closely with our Global Application Security team to ensure our software remains secure and your data is protected.

### How do supplier contracts (for employees, contractors, or third-party suppliers) identify information security responsibilities?

We inform employees and contractors about their obligations for information security using specific confidentiality and non-disclosure clauses in their terms and conditions of employment. Employees must confirm acceptance of the terms of our Acceptable Use Policy (AUP) and partners are required to read and sign an annual security declaration of compliance.

### What recruitment screening processes are in place?

We take identification and right to work by taking copies of passports, driving licenses and any other relevant documents. We take up multiple independent employment references and carry out basic criminal records checks where legally permitted.

# Sage 300 Risk Governance/Management

**Is the application ISO 27001 certified?**
No. While various Sage offerings are ISO 27001 certified since the Sage 300 web screens are not hosted by Sage, the ISO 27001 certification is not applicable to this product.

**Is the application SOC2 certified?**
No. While various Sage offerings are SOC1, SOC2, SOC3 certified since the Sage 300 web screens are not hosted by Sage, the SOC2 certification is not applicable to this product.

**Is a risk assessment performed at least annually to identify potential threats and vulnerabilities that could negatively impact customer services or customer data?**
Yes. We have an automated weekly static code analysis scan which is constantly reviewed along with design/security/threat modelling reviews for each feature in a release. Additionally, we perform manual, static code analysis scans as we implement each new feature and issues are expected to be resolved within the development cycle.

A penetration test is performed annually by an external vendor arranged by the Global Security team with critical/high/medium issues to be resolved before the following release. Only the web screen code is scanned and tested.

.

**Does senior management review the results of the risk assessment effort and vulnerability report?**
Yes. Senior management is involved in the process.

# Sage 300 Business Continuity / Disaster Recovery

**Is there a formal business continuity / disaster recovery process?**
No. The Sage 300 web screens are not hosted by Sage; therefore, disaster recovery is the responsibility of the hosting provider.

**Are there contractual guarantees (SLAs) against product/service disruptions?**
No. The Sage 300 web screens are not hosted by Sage; therefore, service disruptions are the responsibility of the hosting provider.

# Sage 300 Access Control

**If end-user authentication is relevant, are claims-based authentication supported?**
No. Basic authentication (user and password) plus Windows Authentication with assigned roles are supported in the Sage 300 desktop, while only Basic Authentication is supported in the web.

**Does end-user authentication support strong methods (i.e., multi-factor, OTP, biometric, tokens, smartcards, etc.)?**
No.

**Are passwords at least ten (10) characters in length?**
No. Passwords can be less than 10 characters in length; however, the establishment of a complex password that is 8 characters or greater is required.

**Does usage history include the last 24 passwords?**
Since Sage 300 2024, Sage 300 users and passwords are SQL Server users and passwords (hashed and encrypted). SQL Server allows for the configuration of password policies for logins, including password history length. The number of previous passwords to be remembered are therefore configurable in SQL Server.

**Do passwords contain at least three of the following classes: English uppercase letters (A, B, C, ...); English lowercase letters (a, b, c, ...); Westernized Arabic numerals (0, 1, 2, ...); Non-alphanumeric (special) characters (#, &, !, %, ...)?**
Yes. Since Sage 300 2024, passwords are case-sensitive and must contain at least one number, one special character, one lower case and one upper case character with a minimum length of 8.

**Does the application provide the ability to configure login options?**
Yes. Since Sage 300 2024, where Sage 300 previously provided login configuration options (i.e., complex passwords, minimum and maximum policies, etc.), these configuration settings have been removed from Sage 300 and Sage 300 now relies on Local Machine Policies and leveraging SQL Server Authentication.

**Can the application use an external source of role and role assignment information such as Active Directory Security Groups for authorization?**
Yes. Windows Authentication with assigned roles is supported in the desktop, but not the web.

**Will the application contain any session lifetime (idle timeouts, maximum session time, etc.) controls?**
Yes. Idle timeouts and maximum session times are supported in the web screens.

**Does the application provide a quick way to remove authorization and/or authentication privileges to a user account?**
Yes. User deletion in the identify provider automatically invalidates tokens and therefore removes access to any application the user was authenticated to. Additionally, users can be evicted from currently active sessions by an administrator.

**Can the application be accessed via a default or test login id?**
No. The ADMIN password is required to be specified during setup.

**Can users be disabled or removed?**
Yes. Normal users can be disabled and/or removed while the ADMIN password can be changed, but not disabled or removed.

**Is there a formal process in place for Source Code version management?**
Yes. The application uses industry standard source management applications for the storing, securing, and management of source code.

# Sage 300 Application Security / Development / Operations / Maintenance

**Will the application be developed in whole or in part by a third-party?**
No. Sage 300 does rely on third-party libraries, while the application is developed entirely in-house.

**What percentage of the application workforce are not employed by Sage and where are they located?**
Sage 300 has a total of twelve (12) developer resources and four (4) QA resources located in Chennai India.

**Are third parties who are contracted to develop code for the application contractually required to adhere to your application security standards?**
Yes. All development must adhere to Sage Security policies and Sage 300 coding standards.

**Are third parties audited for security and coding standards?**
Yes. Any source code developed by either Sage developers or contract developers are audited for coding and security standards.

**Are separation of duties and practices followed during development, administration, and testing?**
Yes. Development and Quality Assurance are separate groups that work together for the development and testing of the Sage 300 application.

**Are industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, open Group ACS Trusted Technology Provider Framework, NIST, etc.) utilized to build-in security for the Systems/Software Development Lifecycle (SDLC)?**
No.

**Are developers required to undertake secure development training at least annually?**
Yes. See the Sage Governance section.

**Does the application comply with relevant secure coding standards (i.e., OWASP Top 10 Critical Risks)?**
Yes. See the Sage Governance section and part of the annual training is based on the OWASP Top 10.

**Is the application audited against secure coding standards?**
Yes. We have an automated weekly static code analysis scan which is constantly reviewed along with design/security/threat modelling reviews for each feature in a release. Additionally, we

perform manual, static code analysis scans as we implement each new feature and issues are expected to be resolved within the development cycle.

**When an issue is discovered, is just the remediation of the vulnerability checked or is the overall security of the application checked again?**
Issues are reviewed and remediated on a case-by-case basis and the entire application is reviewed on a weekly basis with static code analysis scans.

**Does the application undergo third party penetration testing activities at least annually?**
Yes. A penetration test is performed annually by an external vendor arranged by the Global Security team with critical/high/medium issues to be resolved before the following release. Only the web screen code is scanned, and penetration tested.

**Are the results of a penetration test available to tenants at their request?**
Yes. Summary, not detailed results are available upon request and may require an NDA. Only the web screen code is scanned, and penetration tested.

**Is automated vulnerability testing of the application performed prior to release?**
Yes. Automated weekly static code analysis scans and design/security/threat modelling reviews are performed during the development cycle. Only the web screen code is scanned for vulnerabilities.

**What method of development, if any, do you follow?**
The Agile method Kanban is followed using SDLC integrating with various vulnerability scanning tools.

**What tool is used for vulnerability scanning?**
Several Static Application Security Testing (SAST) tools are used to analyse the source code for security vulnerabilities. Scan results from the tools are centrally stored in a vulnerability management solution. Only the web screen code is scanned for vulnerabilities.

**Are code reviews performed on the code prior to inclusion in the application.**
Yes. Internal, manual code reviews are a requirement for all submitted code and static code analysis is performed on a weekly basis. Only the web screen code is scanned for vulnerabilities.

**Does the application perform signed builds?**
The individual binaries are not signed; however, the installation files are signed.

**Is source code of the application provided?**
We do not provide source code for the application; however, the desktop and web SDKs provide samples and examples of real application screens to assist with partner learning and development. The web SDK is also open source.

**Is there an SLA for remediating identified security vulnerabilities?**
Yes. A security matrix is in place that identifies the nature of the issue, how it is found, and its severity. The fix timescale is put in place by the sage Security team:

- Critical - 2 days or before release
- High - 1 week or before release
- Medium - 6 weeks or before release
- Low - 6 months or within 6 months of release
    - Existing Low issues (not introduced in the current release cycle) may not follow these guidelines.
- Informational - No requirement

**Are granular and comprehensive auditing and logging provided?**
Yes. Logs are categorized with severity.

**Are successful and/or unsuccessful login attempts logged?**
Yes. If the Enable User Activity Logs option is enabled, login actions are recorded.

**Are create, update, and delete activities logged?**
Yes. The web screens log these activities.

**Does the application log the IP address?**
No.

**Is additional software on the client system (i.e., agent or browser plugins) required?**
No.

**Is data accessed in a secure manner (i.e., minimum 2-tier architecture)?**
Yes. Data is accessed in a 3-tier architecture.

**Have your developers considered risk and threat scenarios during the development of the application?**
Yes. Threat modelling used to determine threats and risks. Solutions proposed are required to go through and architecture review board.

**During critical design reviews have your developers considered all applicable aspects of security (i.e., role segregation, authentication, account management, secure access, logging, personal data protection, etc.)?**
Yes.

**Has the application gone through any product assurance or quality checks where product assurance or quality checks include but not limited to security certification and accreditation?**
No. The Sage 300 application is not certified, but the internal Quality Assurance group, System Quality Assurance group, and Sage Security team are robust.

**Will the application be stable when deployed along with corporate anti-malware solutions?**

We do not test against external vendor products nor make any claims that they will work. The Sage 300 web screens are not hosted by Sage; therefore, co-existence with anti-malware or other software is the responsibility of the hosting provider.

**Is a technical description of the data format exchanged to and from the application provided as to enable WAF monitoring and filtering?**

No. The Sage 300 web screens are not hosted by Sage; therefore, any information required for setup and configuration of a firewall is the responsibility of the hosting provider.

# Sage 300 Cryptography and Logging

**Is encryption of data in-transit via TLS 1.2 or higher supported?**
The Sage 300 web screens are not hosted by Sage; therefore, the setup and implementation of TLS 1.2 or higher is the responsibility of the hosting provider.

**Is encryption of data at rest supported?**
Yes. Transparent Data Encryption (TDE) is supported.

**Is the data encrypted at rest, following state of the art encryption standards (i.e., encrypted disks, encrypted databases, etc.)?**
Yes. Sensitive like passwords and database credentials are encrypted at rest.

**What encryption algorithm is used by the application?**
The Sage 300 application uses multiple encryption algorithms depending upon the nature of the data, the area in the application, and the use-case.

**Is the application capable of field level encryption (i.e., GDPR, PII, etc.)?**
No.

**Does the application support a privileged user activity logging capability?**
Yes. But not by user. The web screens can log various activities and events based upon severity (Critical, Error, Warning, Informational).

**Are the application logs in a standard format?**
Yes. Events are logged to the Windows Event Viewer and other logging of application events and errors and messages are logged to a Microsoft Enterprise Library log file (plain text).

**How are email configurations established in the application?**
The Sage 300 application requires an external SMTP server, or an email client program, or Microsoft Graph information to send emails from areas such as customer statements. For an SMTP server, the application supports servers that require SSL/TLS on secure SMTP ports, like 587, which handle encryption in-transit. In the case of email clients like Outlook, encryption is handled by the hosting provider. In the case of Microsoft Graph, Office 365 information is supplied to the email configuration.

**How to confirm that encrypted, in-transit, at rest, is transmitted/stored properly?**
By default, the application does not encrypt data in-transit or at rest, except for sensitive information such as passwords. Data sent between the web server and the browser clients has been tested in Internet information Services (IIS) using both HTTP and HTTPS. Storage of critical data, such as passwords, are encrypted before storing in the database.

**Are credit card numbers stored in the application and properly tokenized?**
No. The application does not store credit cards numbers in the application database.

# Sage 300 Network Security

**Does the application require the use of any special ports or resources?**
Yes. HTTPS (port 443) is recommended for a secure environment.

**Will the application require access by third parties for any purpose (i.e., support, maintenance, general use, installation, configuration, etc.)?**
Yes. The Sage 300 application is generally purchased through partners who provide setup, support, and maintenance services.

# Sage 300 Platform / System Security

**How often are security patches released?**
Product updates are released 2-3 times per year which include defect fixes and security related fixes. Additionally, hotfixes may be made available at any time for critical or time sensitive defect and security related issues.

**Is the patch deployment process manual or automatic?**
Since the Sage 300 web screens are not hosted by Sage, the applying of product updates or hotfixes are manual and are the responsibility of the hosting provider.

**How quickly are critical software patches applied?**
Critical software patches are posted on the customer support portal and knowledge base as soon as they are available. Since the Sage 300 web screens are not hosted by Sage, the applying of critical software patches (hotfixes) are the responsibility of the hosting provider.

**Does the application/database support external privileged accounts?**
No. ADMIN is the only internal privileged account.

**Does the application/database support role-based authorization?**
No.

# Sage 300 Data Analytics Requirements

**Does the application help an enterprise to manage its data in a structured way?**
Yes. Data is stored in relational databases.

**Does the application provide real time analytics/reports in graph and tabular format?**
Yes. Tabular reports, graphs, and Key Performance Indicators (KPIs) are available.

**Does the application provide real time analysis/reports (i.e., dashboards)?**
Yes. Key Performance Indicators (KPIs) are available in the dashboard with customizable charts and graphs which report data in real time.

**Does the application allow an enterprise to customize reports based upon its business needs?**
Yes. Customers and partners can create and customize existing Crystal Reports to suit their business requirements.

**Does the application have the capability to clean and prepare data for analysis?**
Yes. The Sage 300 application has a feature called the Data Integrity Checker which analyses and cleans/repairs potential data issues. This feature is only meant for data cleaning and not analysis.

**Is the application able to identify patterns and trends in data in a way that can help an enterprise understand its business better?**
Yes. Key Performance Indicators (KPIs), dashboards, reports, inquiries, and other data analysis features of the application assist the enterprise in making informed decisions.

**Does the application provide connector/prebuilt integration tools to integrate with other enterprise applications?**
Yes. The Sage 300 application has an SDK for the desktop, an SDK for the web screens, and numerous APIs (COM, .NET, Web Services) to provide various means for integration.

# Sage 300 Data Privacy

**Does the application collect personal information as part of the service?**
Yes. Personal data can be entered and stored in the system. An anonymizer is available for anonymizing personal data.

**Does the application display a privacy notice for the users?**
Yes.

**Is the privacy notice customizable?**
No.

**Is it possible for users to view, amend, or delete their own data directly in the application?**
No. Sage 300 users do not have personal data within the application. However, an anonymizer is available for anonymizing personal information of the user's customers as required by GDPR policies.

**Is it possible for administrators to access, modify and delete user's information and any other personal information?**
Yes. Sage 300 users do not have personal data within the application. However, an anonymizer is available for anonymizing personal information of the user's customers as required by GDPR policies.

**Does the application store any cookies?**
Yes. Cookies are utilized in the web screens for storing information required to run the web screens, but do not contain any personal information (i.e., session date, user locale, last user, last company, etc.).

**Does the application provide a Cookie Consent Management mechanism?**
No.

**Does the application provide any Opt-In/Out mechanism?**
No.

sage.com
0191 479 5911