stackby.com

Stackby Security Whitepaper

Stackby is an all-in-one cloud-based work management software for teams.

It is as easy to use as a spreadsheet but functions like a database. You can completely customize based on your needs, collaborate in real-time and connect it to 3rd party apps to automate your workflows.

The following is a high level overview of Stackby security practices, policies and user administration features.

Privacy Compliance and Data Processing

We take our privacy obligations & protection of your information seriously and comply with all applicable regulations and laws.

Your data is yours, and we guard it closely. We do not sell any of your information. For our full privacy policy, please see - www.stackby.com/privacy and learn more about our commitment to General Data Protection Regulation ("GDPR") here.

Here's the detailed list of all Stackby Sub-processors & Compliance Tasks here.

Service Security

Security Features Available to Customers

For identity and authorization, Stackby supports few login methods: 1) Email and password, and 2) oAuth using a Google email account and 3) Sign in with Apple 4) Sign in with SSO (Okta, Microsoft Azure AD, Google SSO etc.)

First 2 login mechanisms can be enabled simultaneously—a user will be able to login into their account with both an email and password and via Google.

For email and password logins, Stackby enforces a minimum password length of 8 characters. The password does not have an expiration and the user is able to reuse passwords. After multiple failed password attempts, Stackby will enforce a delay between retries.

After multiple additional failed attempts, Stackby will prevent any new attempts for 5 minutes.

For Google login, the password complexity, expiration, reuse, and lockout policies are enforced by the Google account's administrator.

Stackby does not store plaintext passwords; it stores only the salted and one-way hashed key that is generated from the plaintext password.

We recommend enabling 2FA ("Two Factor authentication") on your accounts if you're using Password based authentication.

Stackby supports Single Sign On ("SSO'') using SAML-based Single Sign-On and additional enterprise features for teams on our Enterprise plan. We currently support Microsoft Azure AD, Okta and Google Sign On.

Product Security

Secure Management of Your Account

Stackby allows you to securely share a workspace, stack or view with other users at Owner, Creator, Editor, Commenter and Read Only permission based access levels.

Access for collaborators can be added or revoked by clicking on the "Share" icon for a team or from a stack's "Sharing" menu item.

Stackby provides a revision history feed of changes made to each row, showing who made which changes, and when. Stackby also enables you to restrict access to a stack or a view share link via a password or email domain.

You can also restore your data using our Recycle Bin feature (available as a Stackby Powerup), using Undo/Redo for real-time restoration, exporting tables as CSV files and export complete stacks as Excel files (available as a Stackby Powerup). You can also access Stackby data using our Stackby Developer API.

The Account page also allows for an account to be deleted and export your complete workspace.

Protection of Data in Transit and at Rest

When you visit the Stackby website or use one of the Stackby applications, the transmission of information between your device and our servers is protected using 256-bit SSL/TLS encryption. As part of this client-to-server communication, the Stackby service uses the WebSocket protocol for sending real-time updates to you; this connection is secured using 256-bit SSL/TLS encryption.

The information that you store in Stackby is encrypted while the data is “at rest” on our servers and is protected by 256-bit AES encryption. The AES encryption standards are the same levels of encryption as used by banks.

Network & Cloud server security

Stackby is a multi-tenant cloud service that is hosted in AWS. Customer data is segregated via software which enforces role-based access control.

Stackby uses IAM (Identity & Access Management) functionality to manage the users who have access to the Stackby Production environment. We ensure that access permissions incorporate the principles of least privilege & separation of duties. These access controls are reviewed at least once quarterly.

Stackby servers are located in the US and Singapore, in data centers that are ISO 27001, SOC 1, SOC 2, and SOC 3 certified and utilize numerous physical security measures to protect them from unauthorized access. Stackby servers have round-the-clock security, automatic fire detection & suppression, fully redundant power systems and strict controls for physical access.

We regularly install security updates and patches to keep our servers upto date. Servers are segmented based on role and protected using restrictive firewalls.

Service Reliability & Durability

Stackby servers are hosted on industry leading Amazon Web Services (AWS) cloud infrastructure.

Some of the cloud security measures include every 24 hour database backups, geo-redundantly replicated across multiple availability zones for data durability, geo-replication of services across multiple geographies for disaster recovery, auto-scaling for servers to maintain server performance and more.

Stackby regularly reviews and maintains business continuity and disaster recovery plans and are in touch with AWS Account Managers & Technical Support Teams to do extensive periodic reviews and implement best practices to create a strong infrastructure.

We also have real-time notifications for our different servers to keep fast turnaround times for any server related issues (utilization, scaling, database patches and more). Stackby also implements extensive service monitoring and our server operations team is on call 24*7*365.

Operational Security

To prevent unauthorized access to systems and data, we implement multiple techniques throughout our systems and technology stack, which include:

- authentication and authorization layers to verify the identities and privileges of users
- security policies in AWS to restrict network traffic
- two-factor authentication for all access to production systems

• strict requirements for Stackby employee passwords
• secure password storage

As is necessary to operate Stackby services, a deliberately small number of technical employees have access to the servers and databases where user data is stored. For example, these employees might need to diagnose a performance issue or troubleshoot a customer impacting error. This group of employees is limited using a combination of employee policies and technical controls, and they are prohibited from using these permissions to view any customer data unless it is necessary to do so for operational reasons.

To access the production environment, two-factor authentication is enforced by a bastion host where one authentication factor is a per-user RSA-2048 SSH key, which can be individually disabled, and the other factor is a time-based one-time password.

Stackby's internal support and administration portal is restricted to a specific subset of Stackby employees based on their role, and those employees must use two-factor authentication to access it.

Information Security

Personnel Security

All Stackby employees have undergone a background check and are required to review IT and security policies; they must read and sign a document that consists of practical steps to avoid and mitigate security risks.

The review of this document is overseen by an assigned member of the Stackby security team.

On an ongoing basis, all employees are notified to changes or improvements to security processes.

Stackby employees' desktop computers and laptops must use full-disk encryption, and be protected by a security code or password with strict password requirements, must lock automatically after a period of inactivity, and must require a password to be unlocked.

Application Security

Stackby runs automated application level security scans , package dependency security advisory scans on a weekly basis and endpoint scans on a monthly basis. In addition, Stackby may also involve external penetration agencies to conduct penetration tests.

Secure Development

As part of the development process, code and configuration changes by Stackby's developers are reviewed before being deployed. Before deployment, these changes are tested during the Quality Assurance (QA) process to ensure consistent experience across all platforms, devices and browsers supported by Stackby.

Stackby maintains separate testing and production environments.

The code may also receive a specific security review by the Security Team. Changes are thoroughly tested before being deployed.

Stackby also runs a public bug bounty program to identify possible security vulnerabilities in Stackby, and review and remediate them on an ongoing basis. Security researchers can responsibly disclose security vulnerability by submitting via our secured form or email us directly at security@stackby.com.

As part of our Vulnerability Management Process, we review relevant security advisories on an ongoing basis and determine the steps to mitigate any relevant risks. Depending on the criticality of an advisory or report, we may perform an out-of-band deployment.

Physical Security

Physical access to the Stackby office is secured with fingerprint access and video monitoring, which have motion detection and alarm capabilities.

Governance

Stackby has a Security Team which plans and implements the company's security efforts and practices. This team meets monthly for a recurring status meeting; additional meetings and discussions as related to specific security efforts are also held more frequently. The Security Team is responsible for physical and operational security, training personnel, and other aspects of managing and adapting security risks as the threat and technology landscapes evolve.

Certifications

Given the nature, time-taken and cost for certifications, both ISO/IEC 27001 (Information Security Management System) certification and SOC 1 & 2 certifications are in the future roadmap. As a startup, we are constantly striving to be better, build a solid security foundation and scale to as many enterprise customers to be able to justify those costs & efforts.

Summary

This document is a high-level summary of Stackby's policies and practices related to security and privacy. We continuously adapt to the evolving security landscape, and will update this document as we add and improve new security measures. If you have any additional questions or concerns, please contact us at security@stackby.com.