Security Overview

How we ensure the safety and privacy of your data.

Document generated 04/08/2024

PDF VERSION

Tags | **Security** | **Privacy** |

Applies to: Free, Basic, Business Enterprise

Overview

Our mission at Stack Overflow is to help developers learn, share, and build their careers. After great success with the public Stack Overflow site, we built Stack Overflow for Teams to allow developers to ask and answer questions with their coworkers in a completely private area. We understand the value of your private data, so we designed Stack Overflow for Teams to have the best privacy and security right from the start.

Architecture

From the beginning, Teams data is kept isolated from public Stack Overflow data.

- **Cloud Hosted**: Teams data is stored on Microsoft Azure which includes a robust list of security features.
- **Data isolation**: Teams data is stored in a separate set of databases from Stack Overflow public, and each individual customer's data is logically separated into its own SQL schema and tables with unique logins for each Team.
- **Application isolation**: Teams data can only be accessed by an isolated replica of the Stack Overflow application, which the main public application accesses via an API.
- **Network isolation**: Teams data and applications exist on a separate network within our production data center, with strict firewall rules, and which is only accessible to members of our Site Reliability and Architecture teams.

These protections are in addition to our normal protections around our production data center, which include strict firewall rules, a secure VPN that only Stack Overflow employees have access to, and automated vulnerability scanning of all hosts.

Physical Security

All of our production infrastructure runs in in Microsoft Azure. You can read more about Microsoft Azure's physical security.

Organizational Security

As an organization, we are committed to ensuring that your private Teams data is never accessed by unauthorized personnel or for unauthorized reasons.

Access by technical personnel is limited only to members of the engineering team who need access for the purpose of maintaining the security and availability of the service. Members of those teams have access to the underlying systems which store and process your data (via secure VPN), and never view sensitive Teams data which may contain company proprietary information, such as questions, answers, and tags, without the approval of the customer.

Encryption

Stack Overflow requires the use of HTTPS in order for clients to communicate with the site. All customer data is encrypted using recommended cipher suites and protocols when in transit over public networks and within our network between the private Teams network zone and the rest of our infrastructure. Customer data is encrypted at rest.

Availability and Disaster Recovery

All data and infrastructure is built to be fault-tolerant and redundant. We also maintain encrypted offsite backups and routinely test restoring from backups.

For availability updates, see stackstatus.com or @stackstatus on Twitter.

External Security Audits

Stack Overflow Teams undergoes regular penetration testing performed by respected third-party security firms, and any findings that present a risk to our environment are remediated. For more information on our external penetration tests, reach out to support.

Need help? Submit an issue or question through our support portal.