Staffbase

Security Whitepaper

Table of Content

Infrastructure & Systems Security

Physical Security - Azure

Facilities

Staffbase servers are located on Azure by default. Microsoft Azure facilities are compliant to ISO 27001 as well as SSAE-16 certification.

Location

The Staffbase servers hosted on Azure are located in East US (Virginia).

Physical Security - Profitbricks

Facilities

Alternatively, we offer hosting in a EU-based data center. Thus, Staffbase servers are located on Profitbricks. Profitbricks facilities are compliant to ISO 27001 and ISO 9001.

Location

The Staffbase servers in the EU-based data center are located in Frankfurt/Germany.

Network Security

Protection

Our network is protected by redundant layer 4 firewalls, secure HTTPS-transport communication over public networks, VPN only access to our production and testing systems as well as key-based authentication for system administrators for maintenance purposes.

Architecture

Staffbase network architecture is designed to minimize the risk of a security breach by permitting access only to the minimal required systems, while other systems, such as database servers, are only accessible internally. Every traffic to our application servers is routed through our proxies and gateways. All other systems in our data centers have never direct access to the internet neither inbound nor outbound.

Third-Party Penetration Tests

We allow customers to do their own penetration tests on request. Additionally, we provide a summary of previous penetration tests on request.

Security Incident Event Management

A security incident event management (SIEM) system gathers all available logs from our systems to analyze these for correlated events. The SIEM system notifies the Staffbase Security team about the event and the Staffbase Security team responds to that event.

Intrusion Detection and Prevention

Intrusion detection and prevention is done by our hosting providers Microsoft Azure, and Profitbricks to ensure the maximal security in both the international system as well as the German system.

DDoS Mitigation

Distributed denial of service (DDoS) is mitigated by our hosting providers Microsoft Azure, and Profitbricks.

Logical Access

Access to the Staffbase Production Network is restricted to the core operations team. This includes frequently auditing and monitoring the accesses. All productive systems are secured by VPN and require key-based authentication.

Security Incident Response

In case of system alert, security incidents are escalated 24/7 to our Staffbase Security team. Our employees are trained on security incident response, including communication channels as well as escalation paths.

Encryption

Encryption in Transit

All communication of our systems over public networks is encrypted using HTTPS with Transport Layer Security (TLS 1.2) and Perfect Forward Secrecy (PFS). We disabled SSLv3 on all systems to prevent security breaches.

Encryption at Rest

We encrypt user passwords by using best-practice one-way hash functions to minimize the impact of a data breach.

Availability & Continuity

Uptime

For all Staffbase services we guarantee a 99.9% uptime.

Redundancy

We perform backups on all relevant systems in daily frequency and store these backups op to a month for restoring based on identified incidents. Also, all productive systems of Staffbase run at least in dual-mode to provide a fast performing failover.

Disaster Recovery

Our disaster recovery program includes plans for different disaster scenarios and training the recovery team to recover timely our systems in case of a disaster.

Application Security

Secure Development

Security Training

We train our developers in a periodic manner to be aware of common security risks for development as well as to be aware about data privacy of our customers data.

Framework Security Controls

Our applications are protected by best-practice mechanisms against common risks in Web applications, such as CSRF, SQLi, and XSS.

QA

For ensuring a maximum level on QA we perform a lot of automated tests on our code base. Also, we peer-review all code changes that are submitted by our developers to the code base.

Separate Environments

Staffbase' testing and staging systems are separated logically from production systems.

Application Vulnerabilities

Security Penetration Testing

While customers are allowed to perform their own penetration tests on request, our employees perform annually penetration tests internally for increasing the security level of our application.

Product Security Features

Secure Development

Registration

We offer several ways for onboarding your users into Staffbase. Users can be invited directly by email. You can also use registration based on domain bonding. That is, every user with a certain email domain can register without inviting them individually. Even when you do not know the email address of your users, you can invite them by generating unique access codes for one-time registration. Finally, you can use SSO for registration.

Single-Sign-On (SSO)

For authentication as well as onboarding you can also use our SSO integrations. Therefor, you can integrate your systems into Staffbase by utilizing SAML and OpenID.

Configurable Password Policy

You can use a customized password policy when using SSO. We provide configurable password policies also on request.

Two-Factor Authentication

Two-factor authentication is available when using SSO.

Secure Credential Storage

Passwords in Staffbase cannot be extracted, as they are stored in the database using bcrypt, a one-way-hash function that is designed to be collision free.

API Security & Authentication

Our API that is available for customers is secured by HTTPS and an API token that leverages HTTP Basic authentication.

Additional Product Security Features

Access Privileges & Roles

You can customize access privileges and roles fine-granular in Staffbase regarding your needs individually.

Transmission Security

We utilize HTTPS connections for every communication between Staffbase clients and servers.

Email Signing

We facilitate DKIM (Domain Keys Identified Mail) for signing outbound emails from Staffbase.

Session Lifetime

In Staffbase you can configure the maximum lifetime of a user’s session to adjust the security based on your company policies.

Data Privacy & Data Security

Policies

Our security policies are maintained and audited frequently by our data protection officer.

Security Training

For our employees we provide an annual security awareness training as well as frequent security awareness updates about recent security risks.

Confidentiality Agreement

All employees of Staffbase have signed a confidentiality agreement to protect the customers data, and agreements obligating them to comply with the data secrecy provisions of § 5 of the BDSG (Bundesdatenschutzgesetz) and the confidentiality of telecommunications (§ 88 Telecommunications Act).

Reduced Access

Access to our production systems is reduced to a minimum set of persons, who are responsible for maintenance and operations.

Sharing with 3rd Parties

We do not share any client data any 3rd party. As plugins are optional in Staffbase, they may be excluded from this guarantee.

Data Processing Agreements (DPA)

Where required under applicable data protection law, we will conclude an agreement on commissioned data processing.

You have a question?
Email us at:

hi@staffbase.com

www.staffbase.com