Staffbase HIPAA compliance based on ISO 27001 certification

Requirement	Mapping to ISO 27001	Staffbase Approach
Administrative Safeguards	• **Human resources security** – controls prior to employment, during, and after the employment • **Access control** – controls for the management of access rights of users, systems and applications, and for the management of user responsibilities • **Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy.	Staffbase audits access to production systems at least annually by following the least privilege principle. Our disaster recovery program focuses on technical disasters for operation of the Staffbase platform and includes plans for different scenarios as well as regular training for the recovery team.
Physical Safeguards	• **Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.	Access to the Staffbase Production Network is restricted to the core technical operations team, which includes frequently auditing and monitoring all access.
Technical Safeguards	• **Asset management** – controls related to inventory of assets and acceptable use; also for information classification and media handling • **Operational security** – controls related to the management of IT production: change and capacity management, malware, backup, logging, monitoring, vulnerabilities, etc. • **Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.	Our network is protected by redundant layer-4 firewalls; secure HTTPS-transport communication over public networks; and VPN-only access to our production and testing systems. Our applications are protected by best practices against common web risks such as CSRF (cross site forgery request), SQLi (SQL injection), and XSS (cross site scripting), following the OWASP recommendations.
Organizational Requirements	• **System acquisition, development and maintenance** – controls defining security requirements, and security in development and support processes • **Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers • **Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence	We conduct a detailed review of all vendors to Staffbase that may have a potential impact on security of the service. This is a two-stage review, involving both Staffbase Security and Staffbase Legal. Identified vendors must agree to specific security language, incident reporting, and controls on handling data.
Policies, Procedures, and Documentation Requirements	• **Information security policies** – controls on how the policies are written and reviewed • **Organization of information security** – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking	For our employees, we provide annual security awareness training as well as frequent security awareness updates to be up-to-date for common security risks in development, as well as the privacy of our customers' data. All employees and contractors agree to comply with defined security policies, which include confidentiality, data privacy, and incident reporting.

If you have further questions, please reach out to your Customer Success Manager or contact us via **staffbase.com/en/contact/**

Staffbase