Staff Squared – How we secure your data

www.staffsquared.com

Last updated: July ‘18

Contents

Introduction

Here at Staff Squared, we recognise our legal obligation to ensure that we are fully compliant with the latest data protection legislation, GDPR. In addition, we feel that we also have a moral responsibility to customers to guarantee the utmost security of the personal data they entrust to us.

Security is, therefore, something that we take very seriously at Staff Squared and is always in the forefront of our minds.

This document answers the most commonly asked data security related questions that we receive. We will also cover the systems and policies we have in place to keep your data protected.

If you have any questions that we have not answered here, please do contact a member of our Customer Care Team on 0800 033 7569 or support@staffsquared.com.

Where is my data stored?

All data is held on Microsoft's Azure Cloud platform. Specifically, we use the South UK datacentre so we are certain that all of the data we retain is held within the UK.

How safe is my data?

In keeping with our desire to use the latest hardware and software security technology, we chose to use Microsoft Azure as our software host.

Microsoft leads the industry in establishing and continuously meeting clear security and privacy requirements. Azure meets a broad set of international and industry-specific compliance standards, including:

- General Data Protection Regulations (GDPR)
- ISO 27001
- ISO 27018
- HIPAA
- FedRAMP
- SOC 1
- SOC 2

Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls that those standards mandate.

In addition to server security, physical security measures are also in place to protect the data stored from unauthorised persons or improper access by use of compartmentalised security zones, controlled by biometric access methods. This means that only authorised personnel can access the physical location of your data.

We use industry-standard protocols to encrypt all data in transit, which means that the data travelling between your browser and our Microsoft Azure servers is as secure as the online banking platforms you use. We also encrypt all data held in our database via a process called Transparent Data Encryption.

We perform regular backups of our database to ensure all data is kept safe. All backups are also encrypted. Backups are performed every 5 to 10 minutes and we retain backups for a period of 35 days.

Finally, our database is IP restricted so that no one can access the data from outside our office or the Azure data centre - making it as secure as possible.

Who can Access my Data?

Despite the obvious need for us to have access to the data in Staff Squared for support and technical purposes, we still take great care to ensure that only people in our company are given levels of access specifically required to perform their duties, and nothing more.

The specific roles and access to Staff Squared data are outlined below.

Role	Access
Senior Management and Development	Access to data for diagnostics, release or development.
Customer Care Team	Access to customer data to assist with support issues.

Sales and Marketing	Access to customer data to assist with account queries and upgrades.

It should be noted that anyone you invite to your Staff Squared account will have some degree of access to your account data. Admin level users can see all data in your account, while standard users have access to a very limited amount of data. To learn more about permissions in Staff Squared, click here.

Will you ever Sell or Share my Data?

No, absolutely not. We do not share or sell your data to any third parties, ever.

Azure Access to Network and Data

Microsoft Azure does not access or use Staff Squared content for any purpose than as legally required and to provide the Azure services to Staff Squared and its end users. Azure never uses customer content or derives information from it for other purposes such as marketing or advertising.

How is the Staff Squared Application Secured?

As we run Staff Squared on Microsoft Azure, all operating system and platform security patches are automatically applied by Microsoft.

Staff Squared supports SSL (TLS 1.1 and above), which is the standard security technology for establishing an encrypted link between a web server and a browser. This means that your data cannot be intercepted in

transition. We also encrypt all passwords to ensure optimum security using the salted SHA-265 hashing model.

A secure system is only as secure as the passwords used to access it. Often, it is a weak password within an otherwise secure system that an attacker will leverage to gain access. To reduce the likelihood of weak passwords, we have specific requirements password complexity. All new users must create a password that is strong (we use a password strength estimator developed by Dropbox to measure this Dropbox/zxcvbn), which can be achieved by using a combination of upper and lower-case letters, numbers and special characters (@%?!). We recommend that you ask your staff to check their passwords against password security websites such as https://howsecureismypassword.net/.

How is Staff Squared Hardened Against Software Hacking?

Staff Squared considers all suggestions made in the OWASP Top 10, which is a powerful awareness document for web application security and represents a broad consensus about the most critical security risks to web applications.

How robust is Staff Squared from DDoS attacks?

Thanks to the Azure cloud, we can scale up when under heavy load or attack.

Furthermore, Staff Squared uses Cloudflare, a service that protects from all manner of attacks, while simultaneously optimising performance. Cloudflare mitigates DDoS attacks, including those that

target UDP and ICMP protocols, SYN/ACK, DNS and NTP amplification and Layer 7 attacks.

Compliance

We are fans of GDPR and believe that this new legislation is an important step forward to clarifying and enabling individual privacy rights. As such we have made the relevant movements to ensure complete compliance with the latest data protection law. You can read more about the ways Staff Squared supports GDPR here.

Staff Squared is already Cyber Security Essentials Plus certified; however, we are always striving to be as secure and compliant as possible, therefore, we are also currently pursuing an ISO27001 accreditation, for which we will be externally assessed in Q3 2018.

Staff Squared and its payment partners are fully PCI DSS compliant.

Summary

We are registered with the Information Commissioner's Office (ICO) for the purpose of handling your confidential data. Strict data handling procedures are in place to ensure that our staff do not have access to passwords or beyond their ability to provide development or support for your HR software. We will never undertake any work involving your data without your express consent.

Our internal processes are audited in correlation to any new legislation changes, and the Staff Squared Terms and Conditions.

www.staffsquared.com

hello@staffsquared.com

0800 033 7569