staffcircle

# Security Policy

**Revision 1.3b**

www.staffcircle.com

## AZURE CLOUD PLATFORM

- Hosted in UK based Microsoft data centres (UK South and UK West)
- Data centres compliant to ISO 27001, ISO 9001, HIPAA, FedRAMP, SOC 1 and SOC 2
- European data centre locations also available
- Jurisdiction restricted processing
- Highly secure cloud-based SaaS offering

## MULTI-TENANCY

- Multi-layer tenant data segregation
- Each tenant runs on separate domain
- Customer maintains control over their tenant

## CUSTOMER CONTROLS ACCESS

- Role-based permissions via Admin Dashboard
- Optional Integration with your existing Identity Management – example: Active Directory
- SAML 2.0 interface to Single Sign-On & Active Directory
- Access Control Reporting built into platform

## FULL ENCRYPTION & SECURITY

- Mobile and Web app data encryption
- Uses AES 256 and TLS 1.2 encryption
- Data is encrypted in rest and in transit
- VPN only access to production systems
- Regular Third-Party Penetration tests help prevent vulnerabilities

## REGULATORY COMPLIANCE

- UK Data Protection Act
- General Data Protection Regulation (GDPR)
- Data Protection Agreement with customers
- In house Data Protection Officer

## HIGH AVAILABILITY AND SCALABILITY

- Highly available clustered platform with planet-wide scaling ability.
- Contractually binding 99.9% availability with service credits.
- Our platform availability is monitored by a third party from outside our network.

## INTRUSION DETECTION AND DDOS MITIGATION

- Intrusion detection and prevention processes are performed by our hosting providers Microsoft Azure to ensure the maximum security of the StaffCircle platform. Distributed Denial of service (DDoS) is mitigated by our hosting provider Microsoft Azure to ensure the maximum uptime of the StaffCircle platform.

## LOGICAL AND PHYSICAL ACCESS TO PLATORM

- Logical access to the StaffCircle production systems are restricted to our core operations team and we log and monitor access to the systems on a regular basis. Our systems are protected by various layers of security including VPN access gateways and authorised personnel are granted access only using 2-factor authentication.
- Physical access to our platforms across the two Azure Data-centre locations are strictly controlled by Microsoft Azure security teams.
- All StaffCircle Customers are guaranteed a 99.9% uptime of StaffCircle platform services

## AVAILABILITY, RECOVERY AND SURVIVABILITY

- Platform services include Mobile, Web and PC access to platform services for end users and administrators.
- Platform service availability to monitored by external automated systems and reported at our service portal on https://status.staffcircle.com
- Our core systems are redundant meaning if one component system fails there is always another one available to take over. This is achieved using either clustering or failover strategies. Each core component on our platform is build using these strategies which minimises the impact of any such failure.
- Our platforms are backed-up to an off-site location a minimum of three times per 24 hours. In the extremely unlikely event of a catastrophic system failure or complete failure of the storage layers or loss of an entire data-centre we will trigger our disaster recovery procedures which involve loading up our DR cluster and re-importing back-up data from one of the three daily backups.

## APPLICATION SECURITY AND DEVELOPMENT QUALITY

- Application and Platform is externally tested (Pen Tested) with annual certification.
- Our code base has a high level of unit testing and we conduct peer-reviews on code changes.
- We separate our development, test, uat (user acceptance testing) and production environments.
- We implement automated builds and continuous integration.
- We operate in an Agile Scrum development environment.
- We pioneered “Secure Field” technology enabling two-factor authentication on individual fields.

## DATA PROTECTION AND CONFIDENTIALITY

- We adhere strictly to relevant UK and European data protection laws including GDPR.
- All employees sign a confidentiality agreement to protect customer data.
- We do not share any client data with any 3rd party.