Security Information Sheet

Support document

Security Information Sheet

This document aims to provide a general overview of technical security measures undertaken at a company level.

Identity & access

- All access to production systems is administered by the Infrastructure team.
- Access is provisioned in adherence with the “least privileges” principle.
- Access is reviewed regularly to ensure its appropriateness.
- Permissions templates are used to define a base level of access.
- MFA and SSO is enforced
- Comprehensive password policy that aligns to industry best practice

Application security

- A full CI/CD pipeline is implemented to ensure our application continues to align to best practice
- Application security is regularly assessed throughout the development lifecycle.
- Vulnerability scanning and penetration testing is performed regularly as part of a comprehensive security testing programme

Infrastructure security

- Access to the cloud environment is delegated through AWS SSO.
- Infrastructure is managed by terraform, any changes are subject to peer review and approval before being deployed.
- Firewalls for enforcing IP whitelisting and access through permitted ports only to network resources
- A web application firewall (WAF) for content-based dynamic attack blocking
- Infrastructure is monitored for potential disruption, and the infrastructure team is alerted of this.
- DDoS mitigation and rate limiting
- Logs are maintained and monitored for network traffic, both internal and edge

Encryption & Key management

- Data at rest is encrypted at AES-256. Data in transit is encrypted using TLSv1.2 and suitably strong cipher suites.
- All cryptographic keys are managed and stored securely
- Incoming encrypted data is terminated on WAF / load balancer.

Awareness & Training

- All staff are required to undergo DBS and background checks
- All staff complete Data Protection and Information Security training at least annually
- Additional training is provided to all staff that may directly handle data

Resilience

- Critical systems scale horizontally to handle demand.
- Critical systems are deployed in a multi-AZ distribution to ensure geographical redundancy.
- Regular backups are performed and data integrity tested.
- A disaster recovery plan, business continuity plan and an incident management process is in place.

Supplier management

- All vendors are assessed via our supplier management process to identify security risks ensuring that our security posture is maintained

Endpoint security

- EDR solution in place to provide visibility and ensure endpoints maintain appropriate security

Compliance

- We are ISO 27001 certified, and maintain an Information Security Management System
- We hold valid Cyber Essentials and Cyber Essentials+ certifications