Quantum: Information Security

Serverless architecture

The application is implemented using serverless technologies and is hosted at Amazon Web Services (AWS).

The application makes use of the following AWS services:

- Identity and Access Management (IAM)
- Amazon API Gateway
- Amazon Simple Storage Service (S3)
- AWS Lambda
- Amazon Cognito
- Secrets Manager
- AWS Key Management Service (KMS)

Further information on the security characteristics of each of these services can be found in the AWS Security Portal.

Control of confidential information

Information is classified and labelled to indicate both the level of confidentiality and organizational compartmentalization.

Users are authenticated using an email, password and Two Factor Device by Amazon Cognito. Users are authorized to access only confidential information labelled for their organization.

Organization associations are stored and managed by Amazon Cognito.

Information compartmentalization is provided using Amazon Cognito and AWS Key Management Service together. A unique cryptographic key is created for each organization and all confidential information provided by that organization is encrypted with their unique key.

Access to the KMS key is provided only to users who are members of the organization. No other users are authorized to decrypted confidential information provided by another organization.

Administrative users are not authorized to decrypt confidential information.

Data Sovereignty

All data is held in the UK and all processing is conducted within the UK

User Access control

User access provisioning

There is no self-registration process. Users are invited to the system by Class Legal administrators. Users are assigned to organizations by system administrators at the point of invitation.

User deprovisioning

All access roster management is provided by Class Legal. When a user leaves an organization, or no longer requires access, Class Legal should be informed to disable the associated user account.

Authentication

Users are authenticated by Amazon Cognito using an email address, password and two factor device.

Two Factor Authentication will be enabled by default for Organizations and uses the standard Time-based One-Time Password algorithm (TOTP).

Password management

Passwords are stored securely within Amazon Cognito and Class Legal have no access to extract passwords.

Protection from compromised credentials

Amazon Cognito helps protect users from unauthorized access to their accounts using compromised credentials. When Amazon Cognito detects users have entered credentials that have been compromised elsewhere, it prompts them to change their password.

Password policy

Passwords are required to have a minimum length of eight characters. This is enforced by Amazon Cognito.

Cryptographic controls

Encryption in transit

All data is encrypted with Transport Layer Security (TLS) version 1.2. Less secure versions of TLS will be rejected.

Encryption at rest

All data is encrypted at rest using the Amazon Key Management Service using the KMS SYMMETRIC_DEFAULT configuration profile. Currently, this represents a symmetric algorithm based on Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) with 256-bit keys, an industry standard for secure encryption. The ciphertext that this algorithm generates supports additional authenticated data (AAD), such as an encryption context, and GCM provides an additional integrity check on the ciphertext. For technical details, see the AWS Key Management Service Cryptographic Details whitepaper.

Penetration testing

The application is penetration tested by a third party on a quarterly basis and the results are reviewed and remediated as necessary.

Data durability

All data is held within Amazon S3, which provides 99.999999999% durability of objects within a given year.

Administration

Network Intrusion Detection Systems

As a purely serverless application there are no dedicated network resources to monitor.

Required levels of intrusion detection are provided by continuous compliance tools.

Continuous compliance

AWS Config provides compliance monitoring.

AWS Cloudtrail monitors activity within the AWS environment and alerts for defined suspicious activity.

AWS GuardDuty provides continuous threat monitoring and alerts for suspicious activity or changes in the cloud environment.

Patch management

As a serverless application there are no dedicated computer resources that require patching.

All patch management is therefore provided by AWS.

Software vulnerability management

Software dependencies are actively monitored for known security vulnerabilities using third party vulnerability management software. Known vulnerabilities are regularly triaged and updated as necessary.