Quill Security Whitepaper

Introduction

When you use Quill's services, you're trusting us to process your information. We acknowledge this responsibility and work hard to protect you by continually strengthening the security of our systems and raising security awareness to our teams and users.

This paper outlines our security strategy for Quill's suite of cloud software products and services.

People

At Quill, we cultivate an inclusive security culture throughout our organisation. All Quill employees undergo security awareness as part of their induction process and receive ongoing refresher training periodically.

Background checks such as references and previous employment verification checks are carried out on new employees. Depending on the role, we may also conduct further checks such as psychometric tests, Disclosure and Barring Service (DBS) checks, and credit checks. New employees are required to sign Quill's contract of employment incorporating a confidentiality agreement prior to starting their new role.

Quill's office space is protected with access control and alarm systems. Only approved Quill employees and invited guests may enter. Our clean desk policy is enforced throughout the organisation.

We keep our users informed of software and security enhancements via the "What's New" sections within our applications and via email where users have opted in. We also include important information about third party product life cycles that may affect them.

Suppliers

Before engaging with any supplier, whether a corporate organisation or an individual, we carry out thorough due diligence and risk assessment. Depending on the supplier size and level of engagement, this may include (but is not limited to): analysis of board members, key shareholders and beneficiaries, references, screening checks, review of incorporation documents and accounting records.

Infrastructure

Quill's server infrastructure is built on the Google Cloud Platform (GCP) **London UK region**. Google builds and runs award winning[1] highly secure data centers throughout the world, providing fast, scalable and consistent performance.

Server administration

- Only a very limited number of trained Quill network administrators with multi-factor authenticated accounts are permitted to manage Quill's GCP environment over secure https connections.
- Specialist contractors may be given limited and time bound access under special arrangement

Data security

Our clients own their data, not Quill, not GCP. You are the data controller and Quill is the data processor.

- Information you store in Quill Interactive is always **encrypted at rest** using the Advanced Encryption Standard (AES)
- Multi-versioned and cross-regional backups are employed for Business Continuity purposes
- Your data and backups are always **stored within the EEA**
- Access to your data by Quill technical support employees may be required from time to time as defined within your contract
- Please see our Privacy Policy for further information on how Quill processes your data

Physical protection

GCP data centers (DC) are physically protected with laser beam intrusion detection, vehicle access barriers, perimeter fencing, metal detectors, electronic access cards and biometrics. They are monitored 24x7 by high-resolution interior and exterior cameras that can detect and track intruders. DCs are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Only approved employees with specific roles may enter. All entry and activity is logged.

Compliance

ISO 27001 compliance https://services.google.com/fh/files/misc/gcp_iso27001_fall_2018.pdf
GDPR compliance https://cloud.google.com/security/gdpr/
Privacy Shield compliance https://cloud.google.com/security/compliance/privacy-shield/

[1] Forrester Insight PaaS https://cloud.google.com/forrester-wave-leader/

Quill Interactive Software Suite

Encryption in transit

Industry standard TLS encryption is enforced for all internet traffic to/from the Quill Web services i.e. only “https” traffic is permitted. Our SSL certificates are issued and verified by market leading providers.

Some services are delivered via Remote App, such as Quill Interactive Accounting and, in this case, access is permitted via Microsoft RD Gateway over https with Network Level Authentication and the highest encryption enforced.

Identity, authentication and authorisation

Quill Interactive user accounts are authenticated using “OpenId Connect”, an industry standard identity layer built on OAUTH 2.0. OpenId grants an authenticated user access to Quill Interactive via identity and access “tokens”. User credentials are never sent in web requests. Further role based authorisation can be configured within the application.

Device cache

In the case of Quill’s smart apps (e.g. Microsoft Office Add-ins), some data will be cached locally on the user’s device in the AppData or Downloads folders per user identity. You are responsible for securing your local devices. We recommend the use of strong passwords and enabling encryption features (i.e. BitLocker).

Antivirus (AV)

Documents that you upload to Quill Interactive are AV scanned. If a virus is detected, the file is quarantined and viewing/downloading is denied preventing further infection. However, we strongly recommend that AV is also deployed to your own devices.

Updates

The Quill Interactive software suite is under continual development: security and feature updates are released seamlessly as soon as they pass quality and assurance testing. We keep our users informed of these updates via the “What’s New” area in the application.

Independently verified

Independent CREST approved providers carry out “penetration tests” on our systems annually.

Third party software lifecycle

We keep our server operating systems well within the vendor's mainstream or extended support phases and critical updates are applied as they become available.

We will only support clients that are using fully supported operating systems and web browsers i.e. only products that are still receiving the vendor's security updates as defined within your contract.

PCs, laptops and devices

Internally at all Quill's offices, our PCs, laptops and devices run operating system versions that are well within the vendor's mainstream or extended support phases and critical security updates are applied frequently. Each device is further protected by market leading AV software configured to automatically receive definition updates as soon as they become available. Encryption at rest is enforced on laptops and mobile devices. Strong passwords with limited lifetimes are enforced throughout.

Information exchange

Exchange of sensitive documentation with our clients is handled via a secure portal where possible. Otherwise, if documents must be shared via email, we will always strongly encourage attachment encryption with a pre-shared key.

Email

Our email service is provided by G-Suite providing world class AV and anti-spam tooling.

- G-Suite is ISO27001 compliant
- Infected or suspicious emails are filtered by the service before they reach the Quill network
- DMARC and DKIM are implemented on our domain
- Further filtering is carried out within our network using market leading AV software
- Mobile device management is handled via G-Suite allowing remote wiping of lost or stolen devices

Working together

As demonstrated throughout this document, at Quill, we take security very seriously and we expect you and your teams to do the same by following data protection law and recommended security practices, such as:

https://ico.org.uk/for-organisations/data-protection-act-2018/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Changes to this document

Quill's Business Continuity and Security strategies are dynamic and evolving processes undergoing constant scrutiny and evaluation and are therefore subject to change without notice.