Data Security

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.

Quill 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 & Subcontractors

All suppliers and subcontractors we employ are contracted to ensure the high security standards set out in this paper are met.

In the case of our US based suppliers, we ensure the **adequacy and security** requirements of the UK General Data Protection Regulation (UK GDPR) through the use of Standard Contractual Clauses (SCC's).

Prior to engaging with any new Supplier or Subcontractor, whether a corporate organisation or an individual, we carry out thorough **due diligence** and **risk assessments** depending on their size and level of engagement, such as: analysis of board members, key shareholders and beneficiaries, references, screening checks, review of incorporation documents and accounting records.

Infrastructure

Quill's core server infrastructure is built on Google Cloud Platform (GCP) **London UK region**. Google builds and runs award winning[1] highly secure ISO27001 compliant data centers throughout the world, with sophisticated intrusion detection and prevention measures.

Physical protection

Physical access is strictly controlled and limited to approved employees with specific roles with all entry and activity logged. The data centers are monitored 24x7 by high-resolution interior and exterior cameras and routinely patrolled by professional security staff who have undergone rigorous background checks and training.

Server administration

Only our **trusted in-house network administrators** are permitted to manage Quill's infrastructure. However, specialist contractors may be given limited and time bound access under special arrangement.

Data security

- Your data is **encrypted-at-rest** using the Advanced Encryption Standard (AES)
- We employ multi-versioned and cross-regional backups for Business Continuity purposes
- Our servers process your data within the **European Economic Area (EEA)** only
- Access to your data by Quill technical support engineers may be required from time to time
- Our Privacy Policy details how we protect the privacy of individuals i.e. "data subjects"

General Data Protection Regulation (UK GDPR)

You (our client) are the data controller and Quill is the data processor. You and you alone are responsible for the accuracy and completeness of your records. As your data processor, we have taken time to understand and ensure our compliance with the UK GDPR as should you. Please also see Working together at the end of this paper.

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

Interactive Cloud

Interactive Cloud is accessed from your web browser (we recommend Chrome or Edge) with all data encrypted both in-transit, i.e. via **https**, and at-rest.

Some services are delivered via RemoteApp, such as Quill Interactive Accounting and, in this case, access is permitted through Microsoft RD Gateway (again via https) with Network Level Authentication and the **highest encryption** enforced.

Third party CREST approved providers carry out independent **Penetration Testing** on our systems on a biennial basis.

Identity, authentication and authorisation

User accounts are authenticated using **OpenId Connect** (based on the industry-standard protocol for authorisation: OAuth 2.0) and further authorisation based on roles can be configured within the application.

Device cache

Quill's desktop apps e.g. Microsoft Office Add-ins, cache some data locally on the user's device in the AppData and/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 (e.g. BitLocker).

Antivirus (AV)

We strongly recommend that AV is implemented on your own devices and this is your responsibility (see Working Together). However, from time to time, the Quill Interactive system will AV scan Documents you upload. If our systems detect a virus, the document is quarantined and viewing/downloading is denied alerting you to the problem.

Updates

Interactive Cloud 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.

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.

At all Quill's offices, our **PCs, laptops and other 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

One-Time Secret

If we need to share a password or key with our users, we may create a self-destructing message that can only be read once by the recipient via a One-Time Secret link. Alternatively, we may send a text message (SMS) to the account owner's mobile phone. **Never send Passwords in plain text within emails or chats**.

Exchange of reports or other sensitive documentation with our clients is handled via a secure portal where possible. Otherwise, if documents must be shared via email, we strongly encourage attachment encryption with a pre-shared key, using one of the above mechanisms.

Email

Our email service is provided by Google Workspace (formerly G-Suite) providing world class AV and anti-spam tooling.

- G-Suite is ISO27K compliant
- G Suite's SCC's ensure UK GDPR compliance
- 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

Business continuity

Please see our “Business Continuity” document for further details.

Working together

As described in this paper, we have put tough measures in place to protect our systems and your data.

However, your teams must also take responsibility by adhering to sound security practices e.g. choose strong passwords, keep your sign-in details secret, ensure there is no unauthorised access to your devices, employ the built-in security features of your device (auto-lock, encryption etc.), implement an anti-virus solution, and ensure your devices are kept up-to-date.

Further guidance on best security practices can be found here:

About Cyber Essentials - NCSC.GOV.UK
Data Protection Act 2018
Guide to the General Data Protection Regulation (UK GDPR)

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.