Quill's cyber security policy

As a provider of fully cloud based software services, security and data protection is of paramount importance to us.

We work hard to continually strengthen the security of our infrastructure and to continually raise awareness about cyber security to our staff and clients.

What we do to protect our infrastructure

Our primary data centre is ISO27K accredited (last audited in August 2016). A pair of next-generation firewalls (NGFWs) sit at the network edge and are fully managed by our data centre providers. An independent penetration test performed in March 2017 reported zero critical issues.

Data is replicated to a secondary co-location via Secure Shell (SSH), ensuring strong encryption during transport over the internet.

Further NGFWs are installed at each of our branch offices providing Intrusion Prevention (IP), Antivirus (AV), web filtering and spam protection at each location.

We ensure our PC's and Laptops are running Windows operating system versions that are well within Microsoft's mainstream or extended support phases and ensure 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. Bitlocker is employed on laptops to ensure all data is encrypted.

We ensure our Remote Desktop (RDP) Server operating system versions are well within Microsoft's mainstream or extended support phases. Updates are applied monthly during planned network maintenance windows. The RDP Servers are further protected with market leading AV software. Staff access to RDP outside of Quill office space requires a VPN.

Strong passwords with limited lifetimes are enforced throughout.

Independent network penetration tests are performed annually by CREST approved providers.

What we do to protect our Emails

Our email service is provided by G-Suite (formerly Postini) providing world class AV and anti-spam tooling. Infected or suspicious emails are filtered by the service before they reach the Quill network. Further filtering is carried out within our own infrastructure as mentioned above via our NGFW and AV tools. G-Suite also provides us with mobile device management allowing remote wiping of lost or stolen devices. DMARC is also implemented on our domain.

How we protect our software provision to our clients

- **Encryption and data protection**
  Industry standard SSL (TLS 1.2) encryption is enforced for all traffic to/from the Quill Web Applications and associated APIs. Standard “http” requests are always redirected to “https”. Our SSL certificates are issued and verified by GeoTrust Inc.

- **Identity and Authentication**
  All user accounts are authenticated using the industry standard OpenId Connect protocol.

  OpenId provides the authenticated user with a limited lifetime Identity Token which is required for all web requests to Quill. No user credentials are sent in web requests.

- **Authorisation**
  Further “access tokens” are required for authorised access to Quill applications.

- **Antivirus (AV)**
  Our users can upload documents via the "Interactive" Document Management application. All uploaded files are AV scanned and, on detection of a virus, immediately quarantined preventing further previewing or downloading by users.

- **Software lifecycle**
  We only support users that are using fully supported operating systems and web browsers. In other words, we only support products that are still receiving security updates.

People and training

Security awareness training for new staff is carried out during initial induction. Further refresher training is carried for all staff periodically.

We inform clients on a monthly basis about our software enhancements and include any important information about other software product life cycles that may affect them.

Last reviewed and updated: 28 March 2018