1. QUORUM Overview ............................................................. 2
2. Access Points ..................................................................... 4
3. User Types ......................................................................... 5
4. Security ............................................................................. 8
5. Settings ............................................................................. 11
6. Further Information .......................................................... 12
1. QUORUM Overview

1.1 Introduction

QUORUM is a Secure Business Communication solution which protects company communications (emails, messages, files) outside the corporate network. It works with any pre-existing corporate email configuration, requires virtually no set up, and enables secure, private, GDPR-compliant, two-way communication between a company and its external contacts.

QUORUM acts as a secure interface between the (secure) corporate network and the (unsecure) outside world, allowing companies to conveniently send and exchange information securely with external parties.

Each company is assigned its own independent, secure environment, including a company-specific URL, where all communications and information are safely stored. All information is protected using state-of-the-art (AES-256) encryption technology, held in EU-located, fully protected data centres, and subject to strict policy and security protocols.

QUORUM is designed to be simple to set up and convenient to use. Company users can send and receive secure messages directly from within their current email client. All users can access QUORUM from: (a) their email via any web browser on any computer or device; (b) directly in a web browser via the company URL; and (c) by downloading the white-labelled Secure Portal app, available free from iTunes, Google and Amazon app stores. For companies which wish to integrate QUORUM further, there is a well-documented API framework.

1.2 Functionality

QUORUM is designed to automatically adapt to any business environment. The default set up works straight “out of the box”. Nevertheless, QUORUM includes a comprehensive range of settings, enabling companies to tailor the functionality available to their users and to improve upon pre-existing business processes. All settings can be changed at any time. However, in terms of pricing, there is a distinction between QUORUM EMAIL and QUORUM.
1.3 From the point of view of the company user

Company users can send secure emails (plus attachments) via QUORUM directly from within their current email client. They follow a simple protocol to send the email to the QUORUM secure server, rather than sending it directly to the end recipient. This is not difficult to do manually, but it is typically automated by using one of the QUORUM ‘SecureMail’ add-ins. Add-ins are available for Outlook, Gmail and Office 365.

Replies and other notifications (copies of files uploaded, instant messages and notifications of electronic signature activity) are sent directly to the user’s existing corporate email account. This means that for day-to-day use, the typical company user has no need to access the QUORUM secure portal directly.

1.4 From the point of view of the external user

External users receive QUORUM emails directly into their current email accounts. The difference is that, depending on the level of security selected by the sender, either the attachments or the entire message can only be accessed by clicking a secure ‘smart link’ embedded in the email.

The smart link is designed so that when the external user clicks on it they are taken directly to their account’s PIN authentication screen in the company portal. The user enters their four-digit PIN to gain access to their information. (The first time a user logs in they are asked to set their own PIN – unless an Administrator has set it for them already.)
1.5 Private by design

One of the benefits of using QUORUM is that it is ‘private by design’. All communications and information are organised into distinct private channels. The first time a new recipient is sent a secure email, their QUORUM user account is set up automatically and a private channel is created within QUORUM for the sender and recipient(s). Only users who are members of a private channel can access the private channel. All members of a private channel can see all communication within the private channel.

QUORUM, therefore, not only ensures the security and privacy of all communications it carries, but it also provides clear, transparent evidence of this privacy.

2. Access Points

QUORUM is designed to offer maximum flexibility to users, so that companies and their contacts can reap all the benefits without changing the way they work. Users can access QUORUM from within their existing email client (either directly, or by using the ‘SecureMail’ add-in), from the web portal (using either a smart link, or by logging in directly with their username and password), or via the SecurePortal mobile app. Whichever route they choose, users are provided with a professional, modern interface, all branded to match the company theme.

2.1 Email

Company users can send and receive secure communications directly from within their existing email account. Note that for communications to remain secure it is important that the company email server is properly configured with a valid, up-to-date TLS certificate.

QUORUM add-ins are available for Outlook, Gmail and Microsoft 365. The add-ins make the process of sending a secure email as easy as clicking a button. Nevertheless, company users using an email client where the add-in is not available can easily send secure emails by changing the recipient email address to its secure equivalent: for example, for a company user with secure email address ‘employee@exampleco.secure-comm.com’ sending to ‘recipient@company.com’, the user sends to the secure email address: ‘recipient.at.company.com @exampleco.secure-comm.com’.

Note that the above functionality is only available to company users, but that all users can access the web portal from within their email, by clicking on a smart link.

Company users can also request an electronic signature (‘esign’) for any attachments they send. If an electronic signature is requested for a document, once each recipient downloads or reads the document they are prompted to either ‘confirm that they accept and agree with contents’ or to ‘decline’ the document contents.
2.2 Web Portal

Each company is provided with its own unique secure QUORUM domain which both acts as a host for the company and client secure email addresses and also provides the URL for the company web portal. The company URL is simply the company’s unique ID plus the suffix ‘.secure-comm.com’. For example, the web portal for a company with ID ‘exampleco’ would be accessed at the URL: ‘https://exampleco.secure-comm.com’.

Users log into the web portal using their username (or email address), password plus PIN. Alternatively, users can follow the smart link from a secure email which will take them straight into the portal and to the PIN screen, without needing to enter their username or password.

The web portal provides users with a secure, private and convenient way of viewing all their conversations, accessing attachments, organising their information, sharing files and, of course, communicating. It is fully responsive, and can be used equally well on phones and tablets as well as larger screens.

2.3 Mobile Apps

The ‘SecurePortal’ app is available free on iTunes, Google Play and Amazon app stores. It offers a convenient way for mobile users to access their secure environment. It works along very similar lines to the web portal, but as an installed app it has access to more functionality than a browser, and so can provide an even richer experience to the user.

2.4 Branding

Emails, the web portal, and the mobile apps are branded throughout (with the sole exception of the SecurePortal app icon, which cannot be changed) with the company name, logo, colours, and disclaimer. The result is that users not only receive a professional experience, but also have the confidence that ‘they are in the right place’.

3. User Types

QUORUM provides companies with control as well as security over their information. A key element of this is ensuring that users, both internal and external, only have access to the information they should. QUORUM achieves this simply and effectively via its five user types: Agent, Client, Controller, Administrator and System Administrator.
3.1 **Agents**

The typical company user is an ‘Agent’. Agent user rights are designed so that the user has everything they need to do business, but not so much that they can do anything potentially destructive.

Agents can communicate with other users, create new users (users are created automatically when they send an email to a new recipient) and set up new secure channels.

Agents can leave a channel to which they have access. However, they are not allowed to delete other users or channels. Furthermore, they are unable to see other channels and users to which they do not have access.

3.2 **Clients**

Client users are users external to the company. They have more restricted rights. They can access and communicate via existing channels to which they have access, but they cannot create new channels or users.

3.3 **Controllers**

The controller user is designed to enable compliance: for example, where a company needs to be able to gain access, see activity or get an overview of other accounts.

Controllers have all the rights of Agents plus the significant extra power that they can access (on a read-only basis) the account of any other user with whom they have a ‘one-to-one’ private channel. If they have access, they can see everything that user can see.

In the first instance, since QUORUM ensures that there is already a full audit trail of all communication in the existing corporate email account, there is typically no immediate need for a company to introduce Controllers. Companies usually add controller users as usage increases and as the need arises, operating separate, extra Controller accounts alongside their normal user (Agent) accounts. This means that a compliance department can use Agent accounts for their individual business communications, whilst still having the Controller functionality to provide oversight.
3.4 Administrators

Administrators have enhanced user rights (although note that they do not have the oversight rights of Controllers; to ensure privacy and transparency, Administrators are not allowed to be Controllers).

Administrators can set up new Agent, Client, Administrator and Controller users, edit and delete users under their administration, and add, edit and delete channels. Each company environment has one System Administrator (SA). The SA can amend the company’s branding and colours, change system settings and transfer their SA rights to another Administrator.

Administrators can only make changes that affect only users under their administration (this includes both users directly under their administration and users under the administration of Administrators under their administration). This allows the company environment to be segmented into separate areas, with different Administrators taking responsibility for different sections. Every user (other than the System Administrator) is administered by an Administrator, and the Administrators form a strictly cascading hierarchy with the System Administrator at the top.

3.5 Delegating Access

Agents can grant access to their account to one or more other users. This allows another user to do work on behalf of the Agent. This can be useful if, for example, a user has a PA, or if they are on holiday. To preserve the integrity of the audit history, QUORUM records the name of the user who actually performed the activity as well as the person it was performed on behalf of. (This information is hidden from CLIENT users.)

3.6 New Users

New users are automatically added to QUORUM environment as they are required. Each time a secure email is sent to a new recipient, the recipient is set up as a new user. If the recipient email address matches the corporate domain, the user is set up as an AGENT; otherwise they are set up as a CLIENT.

All company users can also set up new users directly from within the web portal or the app. As well as being able to set up users, Administrators can edit users, including changing their user type, password and PIN from within the web portal.
4. Security

4.1 Stability

QUORUM runs on StayPrivate’s fully managed, dedicated servers, located in secure Tier 4 data centres within the UK. Tier 4 data centres adhere to the most stringent standards and are designed to host mission critical computer systems. Our data centres operate fully redundant subsystems (such as air conditioning, network access, power supply, fire protection) and have separate security zones controlled by biometric access. To further ensure durability, we back up encrypted versions of all our systems and data daily to the cloud and, periodically, in physical format too.

4.2 File Storage

All files shared or stored using QUORUM are individually encrypted (using a different key for each document) before being stored in the Amazon S3 Cloud in Ireland, which is designed to provide 99.999999999% durability over a twelve-month period. Amazon S3 is designed to sustain the concurrent loss of data in two facilities.

4.3 Deletion and Versioning

We use versioning, which means that we preserve every version of every file stored, so that users cannot accidentally delete or overwrite important data. All old versions of files are stored fully encrypted in a restricted access area and are deleted after an appropriate period of time.

4.4 Encryption

All communications and information are encrypted both in transit and in storage. We use one of the most secure encryption algorithms available (AES 256) and all files are further encrypted by before being stored in the Amazon, meaning that Amazon does not have access to any of your information. Encryption keys are not shared, but are derived dynamically for each document, meaning that even in the unlikely event of a catastrophic breach of data security, all information should remain fully encrypted.

Emails between QUORUM and the company email server are encrypted using TLS. It is important that the company email server is properly configured and TLS certification is kept up to date.
4.5 Password, PIN Access, Controls

Access is secured by password and PIN (two-step authentication). Users can log out from other devices remotely and there are a range of other security settings, including, for example, the option to automatically receive email notifications each time their account is accessed.

Users can reset their password via email. They can also reset their PIN. However, to maintain the security of the platform, there is a 24-hour quarantine period before a user PIN reset is processed. Administrators can over-ride this on a user’s behalf.

If there is no activity in the QUORUM web portal or app for more than five minutes, the user is returned to the PIN authentication screen, and asked to log back in again. In the web portal, if there is still no response, the user is completely logged out of QUORUM. Users can also log out themselves and can also ‘log out elsewhere’, which enables them to cancel all other current sessions on any other devices.

It is also possible to disable all existing smart links for a user – simply by changing the user password.

4.6 Confidentiality

All communications and information are shared only between the sender and the recipient(s). In other words, users only have access to their own information. The QUORUM user interface is built around the concept of private channels, and therefore reduces the risk of accidentally sharing information inappropriately by, for example, sending an email to the wrong recipient.

4.7 Location

All data reside in the European Union and are protected by European Union Data Protection laws. StayPrivate Ltd is registered under UK Data Protection laws with the Information Commissioner’s Office. QUORUM and StayPrivate Ltd are GDPR-compliant.

4.8 Legal, Default and Failure Protection

We have been awarded ISO 27001 accreditation, the international standard for best practice for information security management systems.
All company files are individually encrypted before being stored in a unique secure space within the Amazon S3 Cloud and all information remains the legal property of your company at all times. In the unlikely event of StayPrivate Ltd defaulting or otherwise failing to deliver the QUORUM service, we will create a single account granting you direct access to your company’s secure area.

We also offer an additional back up service, whereby we can send a copy of all information to a company’s own entirely independent back up area, encrypted using a key provided by the company.

4.9 Private Channels

All communications are associated with a private channel. All participants in a channel can see (with a few minor exceptions) all activity associated with that channel, including the identity of other members of the channel. This is what we call transparent privacy. It means that information is not only private, but that users can see that it is private.

Company users also have their own individual private channel, for their eyes only, called ‘My Area’, where they can store information and send emails to themselves. This channel also carries certain system emails and notifications.

4.10 Primary Channels for Clients

QUORUM automatically creates a primary communication channel between the company and each client (or group of clients) the first time a secure email is sent to the client. This ensures that all communications stay in one place and are available to all the necessary users.

In the standard QUORUM configuration, additional company users can be added to the primary channel by a company user who is already a member copying in the new user on a secure client communication.

If a company user who is not a member of the primary channel attempts to contact the client securely, they receive an error message explaining that a primary channel already exists with this client. To send a secure email to the client they need to either get themselves added to the primary channel or to create a separate private channel with the same client – which they can do by including ‘#private’in the subject field of the secure email.

This set up works well for most businesses, as it provides a single channel to carry most communications between the client and the company, whilst also providing the flexibility to allow private communications as required.
4.11 Strict Primary Client Channels

For companies which wish an extra level of control, it is also possible to enforce ‘strict’ primary channels. In this case, only an administrator can change the members of a primary channel.

Additional private channels can still be established by including ‘#private’ in the subject field as above.

4.12 No Primary Client Channel

Companies can also choose to switch off the primary channel behaviour entirely, so that a separate private channel is created every time a new company user contacts a client.

5. Settings

5.1 Company level settings

The QUORUM default configuration is designed to work with any corporate set up. However, it is possible to tailor the way QUORUM works to fit the exact business need. As well as various branding, naming, content and technical options such as deletion rules, there are several system behaviour settings available to System Administrators:

a. Functionality
   Companies can choose whether to activate Vault (file sharing), Instant Messaging, and Electronic Signatures.

b. Primary channel behaviour
   As described above, in its standard configuration, QUORUM creates a primary channel the first time a client user receives a secure email from the company. Company users are automatically added to this channel when they are copied in on subsequent client communications. It is also possible to add further channels for the same client, either from within the portal, or by sending an email with the phrase ‘#private’ in the subject field.

(this is not the case for strict primary channel configurations where additional members can only be set by the administrator).
There are two alternative settings available. Companies can either switch off the default channel behaviour (so that all channels are private) or they can make the default channel behaviour ‘strict’ so that only Administrators can add users to default relationships.

c. Deletion
There is a comprehensive range of settings allowing companies to specify whether and under what circumstances users are able to delete items.

d. Reply-to email address
The default setting is for the ‘reply-to’ email address to be the original sender’s email address, rather than the email address for their QUORUM secure company domain. This enables external contacts to reply directly outside the secure environment as an alternative to sending a secure reply.

This setting can be changed so that the ‘reply-to’ address is the secure email address, meaning that all subsequent communication should go through QUORUM. Note that any emails that are sent into the secure domain directly from the external user’s email account are not necessarily secure and are automatically marked as originating from outside the secure system.

The setting can also be changed so that emails are sent directly from the corporate email account. To enable this, the company simply needs to add a one-line MX record to their email server.

5.2 User Settings
Company users have a range of settings available to them, such as what notifications they receive and when.

All users have a range of ‘preferences’ which enable them to tweak the behaviour of the web portal and app to suit their requirements.

6. Further Information
For more information and user guides (for the add-ins, portal etc.) please see: https://www.stayprivate.com/quorum/resources.php.