quadrangle

Quadrangle Research Group Limited: Security Measures Summary

Accreditations and memberships

- ISO27001 Cert 221049.
- Financial Services Qualification System (FSQS).
- The Market Research Society (MRS).

User password management

The allocation of passwords is controlled through a formal management process.

- Re-use of passwords is prohibited for 12 subsequent attempts, and twelve-character alphanumeric passwords are required.
- Passwords are stored separately from application system data and are protected by encryption or secure hashing.

Cryptographic Controls

- Staff laptops are full disk encrypted using Bitlocker as part of the standard setup by the IT Department.
- All servers are encrypted using Bitlocker as part of the standard server build.
- All communication to and from the Exchange server is via encrypted SSL.
- All communication using the FTP server is via FTPS, HTTPS or SFTP (preferred).

Security Procedures

- It is forbidden to transfer information by use of portable media (e.g. USB memory stick).
- Access to Quadrangle's IT environment by insecure mechanisms (including but not limited to FTP, Telnet, etc.) is strictly prohibited.

Network Access

- Quadrangle protects its networked services in line with its Access Control Policy from unauthorised access.
- Two factor authentication mechanisms are applied for all users who connect to Quadrangle's resources.
- Authorisation procedures are used to ensure that users only have access to the services which are appropriate for their role and business needs.

Access Rights

- Changes to individual user accounts are performed by the IT Department on authorisation from the Internal IT and Information Security Manager, who acts in turn on request from the user's manager.
- Group IDs should not be used for accessing any information asset within Quadrangle.
- Group IDs are only permissible where an application cannot provide for the use of Individual User accounts, in this event, the creation of the Group ID needs to be approved by the Internal IT and Information Security Manager.

- Minimal privileges should be assigned to the Group IDs.
- Anyone classified as a supervisor or Administrator must have a separate User ID for these purposes, distinct from the individual user ID that they use for day-to-day purposes.

Protection and procedures

We deploy the latest Antivirus and Malware protection across all our platforms and have a strict policy to ensure all our machines have the latest security updates and patches.

Internally, we operate several policies to ensure maximum protection is applied to any classified material, including a strict Clear Desk Policy.

Information Security Committee

Quadrangle takes information Security very seriously and as such, we have an Information Security Committee (ISC) which has a clear a charter focused on managing the development, execution, and executive acceptance of the Information Security Management System (ISMS).