quadrangle

Quadrangle Research Group Limited: Security Measures Summary

Accreditations and memberships

- ISO27001 Cert 607606.
- Financial Services Qualification System (FSQS).
- The Market Research Society (MRS).
- Interviewer Quality Control Scheme (IQCS).

User password management

The allocation of passwords is controlled through a formal management process, users are initially issued with a unique temporary password which they are forced to change at first logon.

- 60-day password changes are enforced, re-use of passwords is prohibited for 12 subsequent attempts, and eight-character alphanumeric passwords are required.
- Passwords are stored separately from application system data and are protected by encryption or secure hashing.

Cryptographic Controls

- All workstations and laptops for staff use are full-disk encrypted 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 between the office and remote site by use of portable media (e.g. USB memory stick) or by email.
- Access to Quadrangle's IT network by insecure mechanisms (including but not limited to FTP, Telnet, etc.) is strictly prohibited.

Network Access

- Quadrangle Research Group Ltd protects its networked services in line with its access control policy from unauthorised access, ensuring that Firewalls with WAN and DMZ interfaces are in place between Quadrangle's network and the Internet, that two factor authentication mechanisms are applied for users outside the corporate network (connecting remotely) and equipment and that control of user access to information services is enforced.
- Authorisation procedures are used to ensure that users only have access to those services and networks which are appropriate for their role and to their business needs.

Access Rights

- Changes to individual user accounts are performed by the IT Department on authorisation from the Internal IT 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 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 a number of 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).