Q5 Systems

Data Handling and Data Protection Statement

Q5 Statement

The Q5 quality management system is based on ISO 9001:2015 standards. Q5's development, customer delivery and data protection is based on adherence to the highest standard of ISO quality principles. Q5's overall management system includes thirteen integrated quality management procedures that ensure that Q5's products are designed, delivered and controlled as per the highest standards.

In particular, Q5 has clearly defined that all employees who handle customer data, whether in physical or electronic form, have a duty of security and confidentiality towards that data. All employees have the explicit duty of care for ensuring that data security arrangements are sufficient to prevent breaches of confidentiality.

Q5 Quality Procedure – QP 13 Infrastructure Maintenance & Security (QP13)

One of the 13 quality procedures that specifically relates to data protection is QP 13 Infrastructure Maintenance & Security (QP13). QP13 defines the quality procedures followed by Q5. Included in QP13 are the following: (Document available upon request)

1. Responsibility and Authority
2. Process Documents
   - Work Procedures & Instructions
   - Hosting Providers
3. Backup Procedures
   - Backup Processing
   - Monitoring
   - Backup Frequency
   - Offsite Storage
   - Backup Validations
   - Backup Retention
4. Application Monitoring
   - Services Monitoring
   - Apache Tomcat Self-Monitoring
   - Web Application Monitoring
   - Server Monitoring

5) Encryption
   - Policy
   - Web Server to Client
   - HTTPS Protocols

6) Incident Reporting, Data breaches and Detection Procedure
   - Identify Potential Threats
   - Notify Appropriate Parties
   - Rectify the Problem
   - Recovering from the Intrusion
   - Audit trail analysis criteria

Server Hardening Policy

Q5 relies on 3rd Party hosted servers to deliver data in a secure and reliable fashion. Q5 assures that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is ensuring that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service. Q5 ensures that vendor supplied patches are routinely acquired, systematically tested, and installed promptly. Q5 regularly updates security features including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections. Access to servers is restricted to server Administrators.

Security and Data Center Overview

Q5 utilizes the data centers provided by Canadian Web Hosting (CWH). CWH is a SSAE 16 Type II provider. The entire CWH service offering utilizes industry leading security tools, and best practices, to ensure Q5 servers and systems are protected. The primary goal in every situation is to minimize exposure to common threats, identify and assess system and application vulnerabilities and provide continuous 24/7 monitoring, management and response. The "Security and Data Center Overview" document (available upon request) describes some high-level security components including our physical security at each of our data centers as well as an overview of available security services to augment your security infrastructure.

CWH is audited against the "AT 101 SOC 2 Type 2" standard. This examination is based on standardized tests of infrastructure power, physical and network security, backup and recovery procedures, maintenance procedures, infrastructure change management, environmental safeguards, communications, management and user controls. Essentially, all aspects of our hosting providers' core capabilities have been tested and meet the international standards that existing and potential customers deserve and expect. The audit was a success and no audit exceptions were noted. (This audit document is available upon request. Due to the secure nature of this document, a non disclosure agreement is required.)

Data Security

To ensure that when data security is transmitted to / from and stored on Q5 servers the following measures have been implemented:

- Q5 data transmission is secured via HTTPS, using the latest TLS protocols where available, and restricting access to any vulnerable protocols.
- Q5 databases are encrypted at rest with a minimum of 128 bit AES encryption.
- No plain text unencrypted protocols are used to communicate to the Q5 servers over public networks

Personal Information Held by Q5

Q5 holds limited personal information which includes: first name, last name and email address. A user name and (encrypted) password to the Q5 application are also held.

This limited, personal information is not manipulated in any way. The username and password are used for login authentication and to determine the security access level for the specific user. The first name & last name appear on internal reports. The email address is used to notify users concerning Q5 tasks and Q5 events.

This personal information is provided to Q5 by the Customer's Application Administrator. Any deletions or changes are requested by the Customer's Application Administrator.

No information related to children is held by Q5.

No personal information held by Q5 is shared with 3rd party entities.