QMS Client Data Security Statement

All data captured by QMS International is processed to enable us to provide you with our consultation and certification services.

Data Security Measures

QMS International have invested heavily both the physical and virtual security of our client servers. All client data servers are held offsite in enterprise-grade highly secure data centres. These data centres are protected by layers of defence-in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communication networks. This multi-layered security model is in use throughout every area of the facility, including each physical server unit.

Technical controls that are in place include, but are not limited, to the following:

- The access to servers are restricted to the company's network using dedicated hardware firewalls
- The access lists on firewalls are based on specific open ports for applications only. All other ports are blocked
- The web servers are highly secure, which have inbuilt features capable of protecting various threats e.g. Event Tracing for Windows (ETW), enable and configure request filtering rules, security configuration wizard and the security compliance manager features
- The Dynamic IP Restrictions (DIPR) module provides protection against denial of service and brute force attacks on web servers and web sites
- Servers and PCs are protected and regularly scanned with best available updated antivirus / spyware/ malware which are updated in line with our patching policies and processes
- Servers and PCs have inbuilt features e.g. dynamic rules-based policies to protect shared folders and files and BitLocker hard drive encryption to enhance data security and management
- Security auditing is enabled as a risk assessment feature, which helps identify attacks (successful or not) that pose a threat to our network, or attacks against resources

System Access

Access to client data is strictly controlled through our Role Based Access Controls, which are maintained in line with our Information Security Policy, IT Policy and Administrator Accounts Policy. Only when a client specifically requests that change is made, or a request for support relating to specific client data is made, will a qualified member of the Client Support Team access the client data set. Data is only processed under the instruction of the client (unless another legal basis for processing applies).

Training and Awareness

All employees with access to either personal or client data are given appropriate data protection and information security training. This is supported with awareness campaigns and group workshops to promote best practice and promote information governance as a business enabler.