



The Stable House,  
Priory Street,  
Hertford,  
Hertfordshire.  
SG14 1XX  
Tel: 01992 500355

## INFORMATION SECURITY POLICY

QRS recognizes that information and the associated processes, systems and networks are valuable assets and that the management of data has important implications. Through its security policies, procedures and structures, QRS will facilitate the secure and uninterrupted flow of information, both within the company and in external communications. QRS believes that security is an integral part of the information sharing process and the policies outlined below are intended to support information security measures throughout the company.

This Policy is the responsibility of the Board of Director's, supervision of the Policy will be undertaken by the Board.

### **Information Security / IT Security**

#### **1. Introduction**

The purpose of this policy is to define a framework on how to protect confidential Company computer systems, information **and all data contained within**, or accessible from all threats whether internal, external, deliberate or accidental.

It is the policy of the Company to ensure that:

- All computers and information contained within them will be protected against unauthorised access.
- Information kept in these systems is managed securely, not only to comply with relevant data protection laws, but also in a professional and dependable manner.
- All employees of the Company are aware that it is their responsibility to adhere to this policy. Senior management to ensure awareness through regular communication.
- All staff are under obligation to ensure confidential information is not divulged to 3<sup>rd</sup> parties.
- All parties accept total responsibility for maintaining, adhering to and implementing this policy within their areas.
- The integrity of all computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of senior management.
- All regulatory and legislative requirements regarding computer security and information confidentiality and integrity will be met by the Company.
- All breaches of security will be reported, investigated & escalated to include 3<sup>rd</sup> party notification where necessary.

- Security requirements will be built into terms & conditions of employment contract with disciplinary procedure for non-compliance.
- All relevant suppliers & partners adhere to the policies & procedures as outlined in this document.

## **2. Statement of Authority, Scope and Responsibilities**

In addition all users have a responsibility to report promptly any incidents which may have security significance to the Company / data. Incidents should be logged. If escalation required then all affected parties to be notified immediately.

## **3. The Computing Environment**

The computing environment is defined as all computing resources. It includes all computing devices that can physically connect, and have been authorised to connect, to this environment. All are covered by this policy, including computing hardware and software, any Company related data residing on these machines or accessible from these machines within the company environment and any media such as DVDs and backup drives that may at times be accessible.

## **4. File / Data Storage & Physical Security**

Reasonable and appropriate physical controls must be in place and applied to protect against unauthorised access and access to computer infrastructure housing system containing customer data restricted further. Confidential customer information must be adequately protected at all times.

## **5. Access to Computers / Data**

Access to each computer should be via individual user accounts with each machine password protected. Access rights to confidential data will be limited to those with a genuine business need. Access must be removed if need becomes redundant e.g. reassignment, cessation of employment etc.

### **5.1 Internet Access**

The IT Manager is responsible for operating and maintaining the firewall with the aim of protecting the company and its computers / files / data from unauthorised or illegal access or attack from the external environment.

Wireless access is restricted to authorised users with password permission / network key.

### **5.3 External Equipment**

Individuals must seek permission from a senior representative before connecting any external machine/drive/disk to computer equipment.

### **5.4. Remote Access to Systems**

All network access is authenticated and authorised. No direct external access to the organisations internal network. All external connections must pass through a DMZ. Software

is in place to detect attempted unauthorised access. Remote connection is logged, monitored and terminated in a DMZ.

## **6. Privacy & Data Security / Portable Storage / Wireless Communications**

Employees given access to confidential / sensitive information / data are to be aware of their responsibilities under data protection law. (See Sections 6.6 & 6.7)

A copy of data taken outside the Company's systems should only be done if absolutely necessary, and all other options should be exhausted before doing so. This includes putting sensitive data onto laptops, memory sticks, CDs/DVDs or into emails. If data does need to be taken outside the Company, this should only be done with the authorisation of senior management. Steps should be taken to mitigate against compromising the security of the data. This will almost certainly include pass-wording the information

Highly sensitive data e.g. customer sample / records should not be taken off the premises. Sample should be securely deleted from machines / storage devices as soon as physically & viably possible if requested by a client or otherwise in compliance with MRS guidelines.

Wireless communications must be encrypted to industry security standards and restricted to authorised IP addresses.

### **6.1 Data Classification**

All client customer information / documentation which has been classified (e.g. marked as "confidential") must be treated as such.

### **6.2 Data Integrity**

All staff are obliged to ensure the integrity of any data / information worked upon. Staff must not amend, alter or change any records without credible and verified reason for doing so.

### **6.3 Electronic Data Transfer / Back-up**

These security measures cover all aspects of electronic data transfer, disposal and data storage. Confidential data / customer records must be

- Password protected and client encrypted files.
- Recipient forewarned to expect delivery.
- Password delivered to key named person.
- Return files (if ever required) to follow same protocol.
- Transferred via QRS/Client FTP site if possible

### **6.4 Physical Data Transfer**

Any hard copy client customer files / DVD / CD etc will be clarified with client and where necessary, a secure courier service will be utilised.

### **6.5 Data Disposal**

All waste treated as confidential.

The company will destroy all confidential customer records / materials as soon as physically & viably possible if requested by a client, or otherwise in accordance with MRS guidelines. Sample data should only be held for the minimal time possible before deletion. All other materials (questionnaires, files etc) to be destroyed 2 years from the completion of the project unless agreed in writing otherwise. Hard copy files and documents to be securely disposed of. It is the responsibility of each employee working on each project to ensure compliance.

### **6.6 Confidentiality & Data Protection**

All staff are under obligation to ensure confidential information is kept private and not divulged to 3<sup>rd</sup> parties. The company undertakes therefore to keep secret and confidential all information that it acquires whether directly or indirectly in relation to the client to the best of its ability.

### **6.7 Market Research Society & Data Protection Act**

Employees must adhere to both Data Protection Act & MRS guidelines, as well as all confidentiality procedures outlined in this document. If any employee is unsure of any aspect of these then advice must be sought. Clients & respondents privacy must be protected.

### **6.8 Clear Desk Policy**

To minimise confidential information being seen / accessed by anyone unauthorised to do so, no files containing unprotected customer sample/data to be left out at the end of the working day.

## **7. Security Programmes/Software**

The IT Manager to ensure that all machines are protected with regularly updated and industry recognised anti-virus, anti-malware and intrusion protection software.

Alerts supplied on patches and security fixes and applied immediately where necessary subject to criticality. Updates downloaded as and when appropriate.

All software purchased from approved vendors.

## **8. Email / Internet Acceptable Use Policy**

Use of email by employees is permitted and encouraged where such use supports the goals and objectives of the business. Employees must ensure that they:

- Comply with current legislation
- Use email/internet in an acceptable way
- Do not create unnecessary business risk to the company by their misuse of the internet
- Do not use auto complete – to ensure that emails go to the correct and intended recipient

### **Unacceptable behaviour**

The following behaviour by an employee is considered unacceptable:

- Use of company communications systems to set up personal businesses or send chain letters
- Forwarding of company confidential messages to external locations

- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- Accessing copyrighted information in a way that violates the copyright
- Breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

### **Sanctions**

Where it is believed that an employee has failed to comply with this policy, they will face disciplinary procedures. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

### **10. Records Management Policy**

Staff will create and maintain records of business activities and file and maintain incoming and outgoing records. Physical files to be kept in a designated area unless required for specific business purposes. The location of physical files will be kept up to date at all times.

### **11. HR Security Policy**

Pre-employment screening is required for all new staff. Checks where appropriate ie CRB check or references from previous employers to be undertaken. Subcontractors to have similar screening policies in place.

### **12. External Visitor Policy**

All visitors to QRS's offices will be granted access via the entry phone system and immediately collected from the Reception area. Visitors must be accompanied at all times. Visitors should not be left alone in the offices. Visitors should be accompanied if moving around the premises and until they have left the building.

*These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.*