Information Security Policy

Contents

QRS recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data and information 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.

1. Roles & Responsibilities

The key roles within the Company to maintain information security are :

- IT Director,
- Data Protection Officer (DPO),
- Information Asset Owners (IAOs).

Information security is everyone's responsibility. Problems with any information we hold can cause issues for colleagues, business, customers, and third parties.

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

2. Information Security / IT Security

2.1 Introduction

The purpose of this policy is to define a framework on how to protect confidential Company computer systems, information **and all personal 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 3rd 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 3rd party notification where necessary, in-line with our Data Breach Policy.

- ⇨ 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.

3. 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 including Personal data. In such instances the requirements are per our Data Breach Policy shall be adhered to. This includes notification to clients at the earliest opportunity.

4. 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 removable media and backup drives that may at times be accessible.

5. 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.

6. Information Classification

Information classified by the client as confidential information must be maintained as such at all times. Personal Data will be given the highest classification. Personal data will be held in an encrypted state when at rest at all times. Files containing personal data will be password protected when in transit, as per our password policy.

7. Access to Computers / Data

Access to the computer network will be granted by individual user accounts. Access rights to confidential personal data will be limited to those with a genuine business need through Access Permissions. Access must be removed if need becomes redundant e.g. reassignment, cessation of employment etc. Staff must lock their computers, when leaving their desks and the machines on.

The use of MFA on software used by the company shall be reviewed and applied as necessary. O365 shall use MFA on all user accounts. Xero shall use MFA for those who have been granted access.

8. 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.

9. External Equipment

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

10. Remote Access to Systems

All network access is authenticated and authorised. Only Senior Personnel (Senior Account Manager status and above) and Assign-IT (IT Consultants) will have access to the company network via secure VPN.

Employees shall take extra care when using a public access Wi-Fi. Employees are to ensure that their login credentials remain secure and unseen by a 3rd party.

11. Privacy & Data Security / Portable Storage

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)
It is company policy not to use removable media. 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 require the use of passwords (as per our password policy). Company laptops will have Windows BitLocker enabled.

Highly sensitive data e.g. customer sample / records should not be taken off the premises. Files containing personal data will be securely deleted when no longer required and in accordance with MRS and ISO20252 guidelines.

12. Data Classification

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

13. 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.

14. 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:

- ⇨ In an encrypted state when at rest.
- ⇨ Password protected when in transit.
- ⇨ Transferred via QRS/Client secure FTP whenever possible.
- ⇨ Recipient forewarned to expect delivery.
- ⇨ Password delivered to key named person.
- ⇨ Return files (if ever required) to follow same protocol.

15. Physical Data Transfer

Personal data will only be transported by removable media as a last resort and clients will be notified. All files shall be password protected and a secure courier service will be used.

16. Data Disposal

All waste treated as confidential.

The company will destroy all confidential customer records / materials as soon as physically & viably possible. 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 using a secure destruction company that issues destruction certificates. It is the responsibility of each employee working on each project to ensure compliance.

17. Confidentiality & Data Protection

All staff are under obligation to ensure confidential information is kept private and not divulged to 3rd 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.

18. MRS Code of Conduct, MRS Guidelines & Data Protection Act/GDPR

Employees must adhere to both the MRS Code of Conduct, MRS Guidelines, the GDPR, as well as all confidentiality procedures outlined in this document. All employees will be provided with and must sign the Company Data Protection and Privacy Notice policy and adhere to it at all times. If any employee is unsure of any aspect of these then advice must be sought. Personal data must be protected with 'Privacy by Design' put before all else.

19. 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 on desks at the end of the working day. Please refer to our Clear Desk Policy.

20. Security Programmes/Software / Patch Updates

All Office Staff PCs and Servers will check for the latest anti-virus and anti-malware software every 60 minutes. CATI workstations will check for the latest definitions every 24 hours. Window updates will be distributed by the Kaseya Agent and only updates that have been approved by Assign-IT will be provided. PCs and Servers will check for the latest Windows Updated every 7 days.

When the Company is notified of critical alerts on patches and security fixes they will be applied immediately where necessary subject to criticality.

All software will be purchased from bona fide vendors.

21. 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:

- ⇨ Sign and adhere to our email and internet usage policy.
- ⇨ 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.
- ⇨ Do not automatically save passwords entered into internet browsers.

Staff should refer to our Use of Company Facilities policy for further information.

22. Unacceptable behaviour

The following behaviour by an employee is considered unacceptable:

- ⇨ Any breach of data protection policies and laws.
- ⇨ Any breach of the MRS Code of Conduct or MRS Guidelines.
- ⇨ 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 due to negligence.

This list is not exhaustive.

23. 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, level of intent, and the employee's disciplinary record.
This policy remains in force on termination of employment.

24. 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.

25. HR Security Policy

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

26. 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 and asked to sign the visitor book. 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.

27. Staff Training

Staff shall receive regular information security training so that they can identify information security risks. KnowBe4 shall be used to deliver the training and assessment. KnowBe4 will be used to periodically distribute key policies that relate to the companies information security objectives.

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.