QRS Access Controls Policy

Contents

1. Policy Objectives

1.1 To define the requirements of QRS to ensure that access to information assets is authorised and subject to identification and authentication controls.

1.2 To establish the requirements for controlling access to QRS information or information that it is responsible for, including computing and physical resources. Computer systems, networks and allied hardware and other peripherals are an integral part of our operations and represent substantial investment.

1.3 It is the purpose of the Access Control Policy to ensure that all access to information assets is properly authorised, maintained and reviewed.

2. Policy Scope

2.1 This Access Control Policy shall apply to all access to QRS's information assets.

2.2 All Users provided with access to QRS's information systems shall comply with this Access Control Policy as indicated in the Use of Company Facilities Policy.

2.3 Access to physical and non-physical assets will be governed under the same principles.

2.4 This Access Control Policy shall establish the Logical and Physical Access control requirements for protecting the entire company's information systems and hardcopy data.

2.5 The Access Policy controls forms part of the wider ISMS and associated Policies.

3. Policy Statement

3.1 This policy should be read in conjunction with QRS's Use of Company Facilities Policy, which summarises what QRS deems to be acceptable use of information systems. It forms part of the wider ISMS of the company.

3.2 It is the responsibility of every User with access to the company's information systems to ensure that they have read and understood this document. All Users are obliged to adhere to this policy. Any deliberate or informed breach of this Policy may lead to disciplinary action up to and including dismissal from the company in accordance with the Use of Company Facilities Policy.

3.3 QRS's information systems are provided for business purposes only and this Access Control Policy is used to ensure that Users:

- Comply fully with current legislation;
- Comply with other relevant QRS policies;
- Do not introduce unnecessary risk to QRS;

3.4 Access allocation shall be monitored to ensure compliance with this Access Control Policy.

3.5 All Users, who use the company's information assets and information systems, shall be responsible for safeguarding those resources and the information Owners hold, from disruption or destruction.

3.6 The Access Control Policy shall apply to all Users who have access to the company's information assets, including remote access.

3.7 Failure to comply may result in the offending employee being subject to disciplinary action up to and including termination of employment as per the Information Security Policy.

3.8 The use of the company's information assets and information systems indicates acceptance of this Access Control Policy.

4. Implementation Responsibilities

4.1 The IT Director and DPO shall ensure that Users are provided with education and training to ensure compliance with this Access Control Policy.

4.2 The IT Director and DPO shall develop, maintain and publish standards, processes, procedures and guidelines to achieve compliance with this Access Control Policy.

4.3 Annually review the Access Control processes, standards and procedures, to achieve compliance with this Access Control Policy and shall support the Access Control Strategy and provide security specific input and guidance where required.

4.4 IT asset owners and authorised users shall be assigned for each identified IT asset in order to approve or reject requests for access to their system.

4.5 IT asset owners and authorised users shall check the validity of all user access requests to information assets owned by them before implementation.

4.6 IT asset owners and authorised users shall authorise employees requiring access to information assets owned by them.

4.7 The HR Director shall inform the IT Director or IT Manager of users starting, moving and leaving the company.

4.8 All appropriate managers shall authorise any requirement to changes to user's access rights on the information systems.

4.9 Users shall not share access codes and/or passwords, if access to other information systems are required then a formal request shall be put forward for authorisation by an appropriate manager.

4.10 Users shall not share their network login or access codes; if physical access to restricted areas is required then a formal request shall be put forward for authorisation by the line manager.

4.11 Users shall be responsible for the security (and secrecy) of their own secret authentication information. In no circumstances is secret authentication information to be shared.

4.12 Users shall ensure incidents are reported to their line manager and a Director immediately. Staff shall refer to the Company's 'Data Breach Policy', 'Data Security and Data Protection Policy', 'Information Security Policy', 'Mobile Device Policy' and 'Cyber Security Incident Procedure'.

5. Logical Access Controls

5.1 All information assets shall be "owned" by a head of department and/or the most senior relevant person with responsibility within QRS.

5.2 A process for user access requests, which mandates the steps to be taken when creating or modifying user access shall be defined, documented, and reviewed on a quarterly basis by the IT Director. The scope of this process must include network and specific directory/folder access within SharePoint 'Company Drive – Documents'

5.3 Access to information assets shall be restricted to authorised employees and shall be protected by appropriate physical and logical authentication and authorisation controls.

5.4 Users shall be authenticated to information systems using accounts and passwords. See QRS's Password Policy for further details. Passwords will be stored and managed within Azure AD.

5.5 Users are required to satisfy the necessary personal security criteria, as defined by QRS's Recruitment Policy, before they can be authorised to access information assets of a corresponding classification.

5.6 Users who have satisfied all necessary criteria may be granted access to information assets only on the basis that they have a specific need to know, or to "have-access-to", those information assets.

5.7 The classification of an information asset does not, in itself, define who is entitled to have access to that information. Access is further filtered by any applicable privacy restrictions as dictated by other QRS Policies (such as the Data Protection Policy).

5.8 Access privileges shall be authorised by the appropriate information Owner and allocated to an employee, based on the minimum privileges required to fulfil their job function.

5.9 Administrator accounts shall only be granted to those users who require such access to perform their job function. Administrator accounts shall be strictly controlled and a log of the personnel who have admin account privileges shall be kept.

5.10 Users with administrator access shall only access sensitive data if so required in the performance of a specific task.

5.11 Users with administrator access shall also have an unprivileged account, which shall be used for all purposes not requiring administrator access, including but not limited to electronic mail.

5.12 Line managers, information asset owners and authorised users shall ensure rights and privileges granted to Users of information assets are reviewed on a quarterly basis to ensure that they remain appropriate and to compare user functions with recorded accountability. The IT Director shall manage the review. This shall include a review of access to specific directories as well as user accounts, which shall be revoked at the earliest opportunity if a member of staff leaves the employment of the company.

5.13 Access shall be granted only to those systems or roles that are necessary for the job function of the user. Regular maintenance will address the management of privilege creep.

5.14 Detailed processes shall be developed and followed for terminating, modifying or revoking an employee's access, as part of the Movers/Leavers process.

5.15 In certain instances, particular access may be required for emergency reasons, such as undertaking emergency system maintenance. Requests for emergency access shall be directed to the QRS IT Director and shall be approved by the information asset owner or authorised user. Requests and approval should be documented, if possible, before the change is required stipulating an expiry period, which shall be enforced, for the access rights. A request for change shall be documented retrospectively where it is not possible to do this in advance.

5.16 All third party access (Contractors, Business Partners, Consultants, Vendors) shall be authorised by an appropriate information Owner and, if necessary, monitored.

5.17 Third Party Access to information assets shall be granted in increments according to business need and identified risks. Information asset owners shall specify access timeframes and be prepared to offer justification for such access.

5.18 Remote access to QRS's networks shall be appropriately authorised on a least privilege basis, with access only granted to systems and resources where there is an explicit business requirement.

5.19 Use of privileged utility programmes shall only be conducted by an administrator with administration rights.

5.20 Users access to the Company network and actions within SharePoint shall be recorded and kept for a minimum of 60 days.

5.21 On a quarterly basis the IT Director shall undertake the following tasks which will be logged in the Audit Log:

- Review of User Access Controls in Azure. SharePoint and key access controls will be updated in the User Access Controls and Permissions – latest.

5.22 The results of the Audit log will form part of the 6 monthly Management Review.

6. Physical Access Controls

6.1 Access to the main building and office areas is controlled by key-pad entry systems. Only authorised personnel shall be given access to secure areas of the company's premises and any third party premises where sensitive information is processed or maintained, or physical assets are held.

6.2 All access to areas hosting systems that store, process, or transmit sensitive data shall be controlled and monitored (CCTV).

6.3 The QRS demise shall have a monitored alarm that includes both key holder and Police (URN) response. The alarm shall include motion detectors that cover all entry/exit points and secured areas.

6.4 All visitors shall require authorisation from a QRS Director prior to entering any area where sensitive data is processed or maintained. Visitors shall be accompanied at all times.

6.5 All visits shall be logged and details of logs retained for a minimum of one month, unless otherwise restricted by law.

6.6 Employees shall challenge and/or report any visitors found unsupervised or acting suspiciously at any site where sensitive QRS data is processed or maintained.

6.7 The QRS demise and secure areas shall have fire extinguishers and fire alarm call points at all entry/exit points.

6.8 Fire exit doors shall be of the push bar type.

6.9 A log shall be held by the HR Director of personnel who have access to secure areas (secure room). This shall be maintained in accordance with the Company's 'Joiners, Movers and Leavers Policy'.