INFORMATION SECURITY POLICY

This Policy sits alongside our Data Protection Policy to provide the high-level outline of and justification for QCC's risk-based information security controls

PURPOSE

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

Information may be put at risk by poor induction and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against QCC.

OBJECTIVES

The QCC's security objectives are that:

- our information risks are identified, managed and treated according to an agreed risk tolerance
- our development and procurement of IT systems will consider information security as a fundamental principle
- our authorised users can securely access and share information in order to perform their roles
- our physical, procedural and technical controls balance user experience and security
- our contractual and legal obligations relating to information security are understood and met
- our teaching, research and administrative activities consider information security
- individuals accessing our information are aware of their information security responsibilities
- incidents affecting our information assets are resolved, and learnt from to improve our resillence.

SCOPE

The Information Security Policy and its supporting controls, processes and procedures apply to all information used at the QCC, in all formats. This includes information processed by other organisations in their dealings with the QCC.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to QCC information and technologies, including external parties that provide information processing services to the QCC.

COMPLIANCE

Compliance with the controls in this policy will be monitored by the Business Process Manager and reported to the Senior Management Team.

REVIEW

A review of this policy will be undertaken by QCC senior management team annually or more frequently as required, and material changes will be approved by the Managing Director.

POLICY STATEMENT

It is QCC's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required

QCC will also reference other standards as required, mindful of the approaches adopted by its stakeholders and clients.

QCC will adopt a risk-based approach to the application of controls:

1. INFORMATION SECURITY POLICIES

2. ORGANISATION OF INFORMATION SECURITY

QCC will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within QCC.

QCC will appoint at least:

- A Senior Management Team who will assess and discuss policy changes and requirements.
- A Company Process Manager - who will assess compliance of the data protection and information security policy effectiveness.
- an Executive to chair the Information Governance Board and take accountability for information risk

3. HUMAN RESOURCES SECURITY

The QCC's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security and training will be made available to all staff, and poor and inappropriate behaviour will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

4. ASSET MANAGEMENT

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

5. ACCESS CONTROL

Access to systems and information will be controlled and audited, and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors and device settings as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented where practical.

6. CRYPTOGRAPHY

QCC will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, integrity and authenticity of information and systems.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Information processing facilities will be housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive. This includes where we use third party services to process information.

8. OPERATIONS SECURITY

QCC will ensure the correct and secure operations of information processing systems. This will include documented operating procedures; the use of formal change and capacity management; controls against malware; defined use of logging; vulnerability management.

9. COMMUNICATIONS SECURITY

QCC will maintain network security controls to ensure the protection of information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

10. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to mitigate any risks identified will be implemented where appropriate.

Systems development will be subject to change control and separation of test, development and operational environments.

11. SUPPLIER RELATIONSHIPS

QCC's information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

12. INFORMATION SECURITY INCIDENT MANAGEMENT

Guidance will be available on what constitutes an Information Security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. Appropriate corrective action will be taken and any learning built in to controls.

13. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

QCC will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs.

This will include appropriate backup routines and built-in resilience.

Business continuity plans must be maintained and tested in support of this policy. Business impact analysis will be undertaken of the consequences of disasters, security failures, and lack of service availability.

14. COMPLIANCE

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes data protection legislation and QCC's contractual commitments.

The QCC will use a combination of internal and external audit to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures.

REVIEW

A review of this policy will be undertaken by the Senior Management Team annually or more frequently as required, and will be approved by the Managing Director.

Joanna Goode

Managing Director

Dated: 1st April 2025

Version:	1.3
Release date:	01/04/2024
Review date:	01/04/2025