Computer and information security policy	
NZQA Quality Management System Policy	

Purpose

To define the requirements and approach for ensuring the security of NZQA-held information.

To ensure that NZQA information and information technology assets (including paper documents), are protected from unauthorised access, use, disclosure, disruption, modification or destruction whilst enabling use by NZQA personnel to support NZQA interests, customers and services.

To provide management direction and support for information security and to maintain appropriate protection of organisational information and information technology assets.

Scope

This policy applies to:

- all information (classified and unclassified) either owned by NZQA or that NZQA is responsible for, in either physical or electronic form
- all NZQA information and communications technology including the computer network, server and desktop computers, remote and portable devices (e.g.: laptops, smartphones), operating systems, software, and portable media (e.g.: USB sticks, CDs, backup tapes)
- any personal equipment connected to NZQA systems
- all permanent and fixed term staff, contractors, and consultants providing products and services to NZQA, and non-employees acting as agents of NZQA, collectively referred to as NZQA personnel
- and will comply with the following security principles:
    - Confidentiality – ensuring that information is only accessed by authorised persons
    - Availability – ensuring that information and services are accessible when required by authorised users and
    - Integrity – ensuring that information is not altered without authorisation.

This policy must be read together with the NZQA Code of Conduct and the Acceptable Use Guidelines (AUG) attached to this policy.

Compliance with this policy is required under the NZQA Code of Conduct.

Policy

1 NZQA information and information systems must only be accessed and used in a manner that complies with this policy, and national laws and regulations (including the key external references listed below).

2 NZQA's information security policy and procedures shall be based on the current release of New Zealand Standard 27001[1] and will use the guidelines for protection of official information described in the New Zealand Information Security Manual.

3 NZQA will review information security policy and procedures annually and conduct compliance audits at planned intervals.

4 NZQA personnel must take all reasonable care in their actions and work practices to ensure information is kept secure at all times.

---

[1]AS/NZS ISO/IEC 27001 :2007.

5 All information and information technology assets must be accounted for and have a nominated owner. NZQA will use information security classification and access rights placing restrictions based on those classifications, to ensure confidentiality and appropriate usage of information.

6 Information security procedures and controls will meet NZISM requirements for handling information classified as IN-CONFIDENCE and SENSITIVE. Any information classified at a national security level (i.e.: RESTRICTED or above) must be referred to the Chief Security Officer for special handling.

7 All NZQA personnel must be appraised of, and formally agree to, their computer and information security responsibilities:

- NZQA staff through the Code of Conduct, Acceptable Use Guidelines, role descriptions, and induction and training
- External customers through registration for access
- Sector partners through Memoranda of Understanding and information sharing agreements and
- Vendors through contractual relations.

8 Information systems must be physically protected from unauthorised access, damage and interference including natural and man-made hazards.

9 To ensure the secure operation of information processing facilities, procedures for their management and operation will be established.

10 Access to information and information systems must be restricted according to business need. Users must be individually identified using appropriate registration and authentication mechanisms. Access rights must be reviewed at regular intervals and formal de-registration procedures must be in place.

11 Risk analysis will be conducted and appropriate security requirements and controls identified and agreed prior to development or implementation of information systems. Risks will be documented in a risk register and managed in accordance with the Risk Management policy. Systems design and implementation must be compliant with the standards specified in the NZISM manual.

12 Information security incidents and vulnerabilities must be reported and actively managed to resolution according to established processes

13 Classified information stored on portable devices or transmitted via external or public networks (including the Internet) must be encrypted using an authorised encryption mechanism. Information classified as SENSITIVE should also be encrypted when stored or transmitted within NZQA systems and networks.

14 NZQA Information Services will, in accordance with the NZQA Business Continuity Plan, prepare, periodically update, and regularly exercise and test Information Technology Service Continuity Management plans (S:\IS\Operations\BCP & DR) which must provide for the continued operation of critical systems in the event of an interruption or degradation of service.

15 Only approved software and hardware may be installed on or connected to the NZQA network or systems. Installation of software may only be performed by Information Services staff, or other staff by approval of the Chief Information Officer (CIO).

16 The design, control, and management of all NZQA information technology will be centralised under Information Services.

Responsibilities

NZQA's Computer and Information Security policies are implemented throughout NZQA by the Chief Information Security Officer (CISO) and the Chief Security Officer (CSO) and monitored by the Strategic Management Team (SMT). The CISO role is held by the Chief Information Officer (CIO). The Deputy Chief Executive Strategic & Corporate Services is the CSO.

Policy requirements are mandatory for all NZQA Personnel.

Position	Responsible for
All NZQA personnel	• Compliance with all Computer and Information security policies and procedures. • Protecting and not sharing credentials (eg: passwords), and using their account only for authorised tasks and functions. • All actions undertaken with their account credentials. • Obtaining formal approval from the CISO before bypassing any security procedures or controls.
CISO (held by the Chief Information Officer)	• Review and maintenance of information security policies, procedures and guidelines, and their alignment with legislation and e-Government directives. • Implementation of and ensuring compliance with the Computer and Information Security Policy and NZ Information Security Manual including monitoring of key performance indicators. • Developing and maintaining a strategic level cyber security and risk management programme, communications plan and cyber security awareness and training. • Design, accreditation and management of all NZQA information technology, and • Development and maintenance of Information Technology Service Continuity Management plans.
Manager, People and Capability	• Inclusion of Computer and Information Security policy and Acceptable Use Guidelines in NZQA Induction and training programmes.
Senior Advisor, Procurement	• Inclusion of Computer and Information security policy references within vendor contracts.
Manage, OP & CI	• Development and maintenance of NZQA-wide Business Continuity Plans.
SMT	• Monitoring implementation of all Computer and Information security policies and procedures. • Promulgating Acceptable Use Guidelines and ensuring that all NZQA personnel who report to them (directly or indirectly) read and agree to the guidelines and this policy.
CSO	• Formulating and implementing general security policy • Issuing instructions on security, and ensuring that the instructions are complied with and, • Investigating breaches of security using established procedures.

Information Security and Risk Advisor	• Work with the CISO to develop a cyber security programme. • Work with staff to identify and report security risks, select appropriate treatment strategies and security controls, and undertake and manage projects to address the risks. • Work with other IS personnel to ensure cyber security is factored into all aspects of ICT work, • Work with system owners to ensure appropriate Security Risk Management Plans (SRMPs), Systems Security Plans (SSPs) and Standard Operating Procedures (SOPs) are developed and maintained. • Coordinate, measure and report on technical aspects of cyber security management. • Provide expert advice on cyber security (and where necessary obtain external assistance for this).
System Owner(s)	• Develop, maintain and implement complete and accurate SRMPs, SSPs and SOPs for systems under their ownership. • Obtain and maintain security accreditation for their system.

References

Key external legislation, standards and government frameworks include:

- New Zealand Information Security Manual
- Privacy Act 1993 (defines how personal information can be collected, used, stored and disclosed)
- Official Information Act 1982 (may require the release of classified information)
- AS/NZS ISO/IEC 27001 and AS/NZS ISO/IEC 27002
- AS/NZS 4360, HB 436 Risk Management
- NZS 6656 Code of Practice for the Implementation of a Trustworthy Computer System
- NZQA Code of Conduct

Key internal references are:

- Acceptable Use Guidelines
- Security policy
- Risk Management policy, 10.1.4.1 Manage and monitor risk
- Asset Management policy and 8.3.3.3.1 Acquire fixed and/ or attractive assets
- Business Continuity Plan
- Information security incident response plan
- Security incident handling steps
- IS Disaster recovery plan
- 10.1.4.1.1 Identify and manage IS risk

See the Information and records management policy for references of wider applicability to information management.

Definitions

For the purposes of this policy, unless otherwise stated, the following definitions apply:

Business Continuity	Plans that ensure the delivery of the key outputs of a Business Unit following a significant disruption to work.
IT Service Continuity Management	The process by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur.
NZQA personnel	(a) employees of NZQA, whether permanent or fixed-term; and (b) others, whether individuals or organisations or both, carrying out work for or on behalf of, or providing services to or on behalf of, NZQA, where the agreement or arrangement for the work or services requires compliance with all or some of NZQA's policies, directives, process maps, or procedures.
SENSITIVE, IN-CONFIDENCE	Information security classifications relating to policy and privacy concerns i.e. not considered to be matters of national security[2].
RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET	Information security classifications relating to matters of national security. NZQA information security controls do not normally allow for this level of security[2]. Special arrangements must be made through the DSO.
UNCLASSIFIED	Information that does not require classification as sensitive, in confidence or higher.

Measurement Criteria

- All NZQA Personnel are aware of and work within their responsibilities and obligations to these policies and this is indicated in regular audits.
- Information security systems, procedures and processes are comprehensive and assist NZQA Personnel to manage their obligations.
- The CIO and ICTSC receive regular reporting on information security and conduct a regular programme of review and updating.
- NZQA's Computer and Information Security Policy, and associated systems, procedures and controls, meets the requirements of government regulations (NZISM).

[2] See New Zealand Information Security Manual (https://www.nzism.gcsb.govt.nz/) for formal definitions and further information on handling requirements.