

Computer and Information Security Policy

(CISP v 2.1)

v 2 Approved by the NZQA Board on 26 July 2005
Minor amendments creating v2.1 approved by the Chief Executive on
21 August 2006

Contents

1	Introduction	4
2	Definitions used in this policy	4
3	Revision History	4
4	Other relevant documents	4
5	Board and Management's support of Computer and Information Security	4
6	Governance.....	5
7	Responsibilities	5
	7.1 Users' Responsibilities	5
	7.2 Violation.....	6
8	Compliance and Disciplinary Action	6
9	Security Policy Scope	6
10	Governing and Overriding Policy.....	6
	10.1 E-Government	7
	10.2 The Qualifications Authority Information property rights.....	7
	10.3 Individual Rights and Responsibilities and "Acceptable Use".....	8
	10.4 Use of Disclaimers for Electronic Communications Channels.....	9
	10.5 Classified Information.....	9
	10.6 Information Classifications	10
	10.7 Disposal.....	11
11	Resource Usage and Access	11
	11.1 Network Access.....	12
12	Access to Information.....	12
13	External Access.....	12
	13.1 The Qualifications Authority Network Perimeter.....	12
	13.2 Remote Access	13
	13.3 Access Points.....	13
	13.4 Acceptable Use of the Internet	13
	13.5 Services through Network Connections	14
	13.6 Third Party Access	15
	13.7 Electronic Mail	15
	13.8 Virus Detection	16
14	Business Continuity.....	16
	14.1 Business and Computer Continuity Planning Process	16
	14.2 Preparation and Maintenance of Computer Emergency Response Plans	17
	14.3 Backing Up of Critical Data.....	17
	14.4 Regular Testing of Stored Data Media	17
	14.5 Off Site Storage of Backup Media	17
15	Hardware.....	17
	15.1 Hardware Inventory	17
	15.2 Hardware Responsibility.....	18
	15.3 Hardware Physical Security.....	18
	15.4 Authorised Hardware Changes	18
	15.5 Hardware Deployment.....	19
16	Software	19
	16.1 Software Inventory	19
	16.2 Installation Media	19
	16.3 Unlicensed Software	19
	16.4 Authorised Software Changes.....	19
	16.5 Software Deployment and Procurement	20
17	Network Services Procurement & Deployment	20
18	Configuration Principles	20
	18.1 Desktop Computers.....	20
	18.2 Server Class Computers	21
	18.3 Portable Computers	21

19	Design Principles.....	21
19.1	Systems High Availability	21
19.2	Software Development	21
20	Partners and Third Party Suppliers	22
20.1	Non Compliance	22
20.2	Minimum Requirements	22
21	Recovery Action	23
22	Software Security	23
Appendix A.....		24
	Definitions used in this Policy.....	24
Appendix B.....		25
	E-Government Guiding Principles.....	25
Appendix C		26
	Specific policies relating to Passwords	26
Appendix D		27
	Specific policies relating to Internet Usage	27

1 Introduction

This document provides direction for the protection of the information assets of the New Zealand Qualifications Authority (the Qualifications Authority) by defining a common policy for the security of the Qualifications Authority's Computer Networks, and computer-based Information across all the Qualifications Authority offices and departments.

Because this is a common policy document, it is generic in nature and therefore does not provide technical recommendations or procedures. Instead, this document describes what the policies are, why they have been set and what the consequences of failing to comply with policy are.

This document sits above all other the Qualifications Authority departmental or office policies relating to computer and information security and provides a benchmark for measuring their compliance and alignment.

The Computer and Information Security Policies (CISP) apply to all employees of and contractors to the Qualifications Authority and to any individual, or organisation which the Qualifications Authority permits the use of or access (including by connecting remotely) to the Qualifications Authority's Computer Network (in this policy referred to collectively as "Users"). These policies are the Qualifications Authority's intellectual property and are not to be redistributed, or used for any other purpose.

2 Definitions used in this policy

Please read Appendix A - Definitions.

3 Revision History

Version 2.0 approved by NZQA Board on 26 July 2005

Version 2.1 incorporating minor amendments approved by the Chief Executive on 9 August 2006.

4 Other relevant documents

This policy document is to be read in conjunction with:

- IS Handbook (which includes the Acceptable Use Guidelines);
- The Qualifications Authority Code of Conduct (which includes the User sign-off);
- The Qualifications Authority Policies Manual ("Security" section);
- The Qualifications Authority Human Resources Policy Manual (sections: "Managing Poor Performance and Dealing with Disciplinary Matters" & "Ending Employment"); and
- The Qualifications Authority System Development Life Cycle Standard Methodology.

These documents can be found on the Qualifications Authority's intranet under the Policies and Procedures menu

5 Board and Management's support of CISP

The Qualifications Authority Board and Management formally support the content, management and implementation of this policy. Version 2.0 of this policy was approved by the Executive Management Committee (EMC) on 19 July 2005, the Audit and Finance Committee on 21 July 2005 and the New Zealand Qualifications Board on 26 July 2005.

6 Governance

This policy document is monitored by the Security Monitoring Group (“**SMG**”) and applies to all Users within the Qualifications Authority. The SMG reports to the Strategic Management Team (“**SMT**”). The Chief Information Officer (“**CIO**”) is accountable for ensuring the Qualifications Authority Computer and Information Security Policy is implemented throughout all the Qualifications Authority business units.

Any circumstances arising that appear not to fall within the terms of , or require exceptions to, this policy document, are required to be escalated on a case-by-case basis to the SMG for consideration. As appropriate the SMG will decide the circumstances either do not fall within the policy, do fall within the policy, or warrant an exception or variation to the policy. Variations to this policy can be approved by the Chief Executive under the delegation from the NZQA Board dated 26 July 2005.

7 Responsibilities

Every User is responsible for safeguarding the Qualifications Authority’s Computer Network and Information. Every User is also responsible for using the Qualifications Authority’s Computer Network and Information in an effective, ethical, and lawful manner, and to comply with this policy at all times.

7.1 Users’ Responsibilities

To secure the Qualifications Authority’s Computer Network, it is vital for the everyday behaviour of all Users to reflect awareness of security and individual responsibility for preventing security from being breached.

Some examples of how this may apply include keeping passwords private, logging out of computers when leaving them unattended for long periods of time, ensuring that sensitive information displayed on monitors can only be viewed by authorised people and/or securely disposing of waste media that contains sensitive information within the guidelines and the requirements of, and only as permitted by, the Public Records Act 2005.

Security is everyone’s job. If a potential security breach is observed, reasonable and appropriate measures should be taken to address it. Some examples of this include retrieving sensitive documents that someone else may have inadvertently left in an insecure area and/or reporting observations of unusual computer activity to appropriate personnel.

Policy: “Users must take all reasonable care in their actions and work practices to ensure that Information is kept secure at all times. Users are also responsible for taking appropriate and reasonable actions to secure any part of the Computer Network or Information observed to be at risk, whether or not they have direct responsibility for those resources.”

Department managers must ensure that all Users employed or working in, or engaged by, their department, are also aware of, are provided with or have access to, and comply with the Qualifications Authority’s Acceptable Use Guidelines and other security policies.

Induction programmes will communicate security issues and policies to new Users. Users are required to formally acknowledge their understanding of their responsibilities in this area, by signing an acceptance form attached to the Acceptable Use Guidelines.

7.2 Violation

The Qualifications Authority takes the security of its Computer Network and Information extremely seriously. This policy document has been created to protect the Qualifications Authority's interests by protecting that Network and Information, and its use.

Any non-compliance with this policy, therefore, will be viewed seriously and as a direct threat to the Qualifications Authority's interests. The Qualifications Authority will respond with any or all means at its disposal to counter such threats to its interests.

8 Compliance and Disciplinary Action

The consequences for Users who do not comply with this policy can be severe.

If a User is a Qualifications Authority employee, a breach of this policy could result in disciplinary action – including dismissal in appropriate cases. Details of the Qualifications Authority's disciplinary procedures can be found in the [Human Resources Policy Manual](#). In appropriate cases other legal remedies available to the Qualifications Authority may also be pursued.

If a User is a contractor to, or an organisation engaged to provide services to, the Qualifications Authority, a breach of this policy could result in the Qualifications Authority having a right to seek damages against the contractor/organisation, and/or it being able to terminate the contractor/organisation's contract, depending on the actual terms of the contract.

In addition, usage that may be in breach of New Zealand criminal legislation may be referred to the Police, and/or other appropriate authorities.

9 Security Policy Scope

The Qualifications Authority will create the necessary security measures and assign responsibilities to protect Information from loss, theft, and unauthorized modification or disclosure.

The Qualifications Authority's security measures apply to all the Qualifications Authority owned Information and all Information for which the Qualifications Authority is otherwise responsible, either physical or electronic. All Users must comply with these security measures.

All security measures must conform to the established Qualifications Authority policies and applicable Government regulations/directions and those outlined in this document. The security policies in this document are consistent with, but independent of, other Qualifications Authority policies.

10 Governing and Overriding Policy

The Qualifications Authority, its management and all Users (whether employees (full time, part time, casual, or temporary) or contractors or other organisations) are subject to a higher authority in the form of legal and statutory requirements. For the Qualifications Authority's computer environment, this includes but is not limited to:

- The Qualifications Authority Code of Conduct
- Human Rights Act 1993
- NZ Bill of Rights Act 1990
- State Sector Act 1988
- Privacy Act 1993
- Official Information Act 1982

- Copyright Act 1994
- Defamation Act 1992
- Crimes Act 1961
- Public Records Act 2005
- Education Act 1989
- Crown Entities Act 2004
- Public Finance Act 1989
- Common law, particularly as it relates to maintaining obligations of confidence
- Contractual commitments

The following policy statement overrides all other policy statements that make up this Computer and Information Security Policy.

Policy: “The Qualifications Authority’s Computer Network and information must only be accessed and used in a manner that complies with national or applicable international laws and regulations.”

10.1 E-Government

E-Government is an initiative designed to use technology to enhance the access to and delivery of government services to benefit citizens, customers, business partners and employees. It is about strengthening the relationship with customers by facilitating faster, easier and more direct services. E-Government particularly focuses on transactions between a citizen and an agency or between agencies. The Internet will overwhelmingly deliver these initiatives.

Policy: “The Qualifications Authority’s Information Security Polices must align with all E-Government directives”

Policy: “The Qualifications Authority’s security policy will be based on the current release of New Zealand Standard 17799¹ and must conduct annual audits based on the current release of NZ Standard 6656”

Refer to Appendix B for E-Government Guiding Principles

E-government policies that must also be complied with include:

- E-Government Strategy;
- New Zealand Government Web Guidelines;
- New Zealand e-Government Interoperability Framework (NZ e-GIF).

A full list of the e-government requirements and expectations, as at November 2004, can be found on the e-government website.

10.2 The Qualifications Authority Information property rights

The Qualifications Authority has a substantial investment in its Computer Network and Information. In the interests of the security of that Network and Information, it is important to be very clear about its ownership and how it may be accessed and used.

Policy: “The Qualifications Authority’s Computer Network, and the Information it stores, generates, or which is transmitted over that Network, and all intellectual property in that Information, are the exclusive property of the Qualifications Authority (unless the Qualifications

¹ The New Zealand Standard 4444 has been renamed to: NZS-17799 to align with the name of the British standard on which it is based.

Authority agrees otherwise with the provider of the Information). This Information may only be accessed and used exclusively for the support of the Qualifications Authority's interests, except as allowed for by section 10.3."

This does not preclude the use of rental or lease equipment where the ownership of the physical asset may remain with another company. However, any Information or configuration stored on such assets remains the property of the Qualifications Authority.

In accordance with section 10.7 of this policy, such Information must be irrecoverably removed from equipment no longer owned by or in the control of the Qualifications Authority before ownership or possession of the equipment passes to another party.

10.3 Individual Rights and Responsibilities and “Acceptable Use”

The Qualifications Authority's Information may only be accessed and used exclusively for supporting the interests of the Qualifications Authority. Private use or unauthorised disclosure of the Qualifications Authority's Information is strictly prohibited.

The Qualifications Authority's Computer Network should primarily only be accessed and used exclusively for supporting the interests of the Qualifications Authority. Incidental personal use of the Computer Network is permitted, provided it does not consume more than a trivial amount of resources, does not interfere with productivity or the Qualifications Authority business functions and complies with the other rules set out in the Qualifications Authority's policies (including rules as to illegal and inappropriate use).

Using the Qualifications Authority's Computer Network for any purpose – whether business or personal - automatically grants the Qualifications Authority the right to actively monitor and audit the usage to protect its interests. Because monitoring and auditing computer usage may provide evidence to support disciplinary or commercial actions, the Qualifications Authority's position will be strengthened if a warning of possible monitoring is issued in advance. Warnings of possible monitoring will also act as a powerful deterrent to inappropriate computer resource use. Accordingly, Information Services (IS) is to ensure that such a warning is incorporated in the Acceptable Use Guidelines and displayed during all system login processes.

Users also need to be aware that:

- It is always inappropriate and can be unlawful to use the Qualifications Authority's Computer Network to import, store, view or distribute offensive, objectionable or illegal material;²
- Information held on the Qualifications Authority's Computer Network – whether business-related or for a User's private use – may be made available to the Police and/or other appropriate authorities at the Qualifications Authority's discretion;³
- They must not download Internet files for personal use; and
- The use of the Qualifications Authority's Computer Network automatically grants the Qualifications Authority full rights to access any resulting files and information and, at the Qualifications Authority's discretion, ownership of those files and that information. The User – whether an employee or a contractor – must on request by the Qualifications Authority execute an assignment of the copyright in any such file or information in favour of the Qualifications Authority.

² This includes defamatory, harassing, threatening, obscene, discriminatory, pornographic, sexist, racist or abusive material.

³ Whenever it is practicable and would not jeopardise any ensuing Police investigation, the Qualifications Authority will consider notifying Users in the event that any action is taken.

Policy: *This policy is to be read in conjunction with the Acceptable Use Guidelines. SMG will resolve any questions about “acceptable use” of the Qualifications Authority’s Computer Network and Information. IS must maintain and frequently update the Qualifications Authority “Acceptable Use Guidelines” and distribute those Guidelines to all Users. The Qualifications Authority, through the SMG, is solely responsible for determining what constitutes acceptable personal use.”*

Policy: *“IS is responsible for ensuring that all Users of the Qualifications Authority’s Computer Network will, in advance, be made aware that their usage may be monitored and audited to protect the Qualifications Authority’s interests, and that information held on the Qualifications Authority’s Computer Network may be made available to Police and/or other appropriate authorities at the discretion of the Qualifications Authority.”*

Policy: *“IS must publish and keep up-to-date the Acceptable Use Guidelines detailing the acceptable use of the Qualifications Authority’s Computer Network, including the policies on acceptable use set out in this section. Management of the individual departments are responsible for ensuring that all Users under their control read and understand the Acceptable Use Guidelines.”*

10.4 Use of Disclaimers for Electronic Communications Channels

Using the Qualifications Authority’s letterhead on a document implies that the content of the document is the official view of the Qualifications Authority. Similarly, communicating externally using the Qualifications Authority’s Computer Network, such as e-mail, implies the content of the e-mail is the official view of the Qualifications Authority. For this reason, the Qualifications Authority’s letterhead may not under any circumstances be used for private purposes, and any private use of external communications such as e-mail, or any external communication that represents a personal view, must be clearly identified as such by way of a disclaimer. The disclaimer should automatically appear on the bottom of all outgoing emails.

Policy: *“Any unofficial external communications, making use of Qualifications Authority electronic communications channels, must include an approved disclaimer.”*

Policy: *“IS must publish the form of disclaimer to be attached to any unofficial communications a User is permitted to send, in the Acceptable Use Guidelines. IS must configure a User’s systems so any email carries this disclaimer.”*

10.5 Classified Information

The Internet is an inherently insecure environment that not only supports business, research, and educational organisations, but also attracts a number of people with questionable intentions and activities. It must be assumed at all times that material transmitted via the Internet is being read by parties other than the intended recipient. Any other information transmitted via the Internet, which includes the use of email, must be assumed to be in the public domain.

Commercially sensitive or in confidence Information must therefore be appropriately encrypted if the Internet is being used as a communications medium, to prevent the Information from being intercepted by anyone other than the intended recipient.

Policy: *“Classified information transmitted via the Internet must be encrypted using an authorised encryption mechanism.”*

The automated nature of communicating electronically has made it relatively easy to misdirect messages. It is important for the Qualifications Authority to protect itself from the outcome of any communications that are directed to an unintended recipient, especially an external recipient. This is to be done by placing a statement at the front of each message declaring confidentiality, claiming the Qualifications Authority’s rights to the Information contained within and issuing instructions for disposing of the message should it be received by anyone other than the intended recipient.

Policy: *“IS will ensure a statement of confidentiality, copyright and disposal expectations is automatically inserted in all electronic communications.”*

Policy: *“IS must publish the standard text to be used in the Qualifications Authority for the statement of confidentiality, copyright and disposal expectations in the Acceptable Use Guidelines.”*

10.6 Information Classifications

An effective measure for securing Information is to restrict access to that Information. By restricting Information access to those who need it to perform their duties, the potential for corruption, deletion or unauthorised distribution and use is also restricted. Applying access restrictions can be both time consuming and expensive; therefore a group wide system of Information classification is required to ensure access privileges can be applied efficiently and the degree of restriction relates directly to the sensitivity of that Information.

Failure to successfully secure information may have a corporate and/or a national impact. The Department of the Prime Minister and Cabinet maintains a publication titled “Security in Government Departments” (www.security.govt.nz/signs/) which, among other things, defines a system for ensuring appropriate protection for official information⁴.

Policy: *“The Qualifications Authority will use the guidelines for protection of official information described in the “Security in Government Departments” manual, where appropriate.”*

Policy: *“The Qualifications Authority will use the following classifications for Corporate Information:*

UNCLASSIFIED (Public): *Information regarded as being in the public domain or not needing to be restricted in any way.*

CORPORATE CONFIDENTIAL: *Information that has access rights granted only on a need-to-know basis to allow authorised Users to perform their duties. Public and internal access is otherwise restricted because it may seriously compromise the Qualifications Authority’s interests if this Information is destroyed, altered or misused.*

IN CONFIDENCE: *Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.*

SENSITIVE: *Compromise of information would be likely to damage the interests of New Zealand or endanger the safety of its citizens.”*

⁴ as approved by Cabinet on 18th December 2000 in “Cabinet Minute CAB (00) M 42/4G(4)”. This system introduces a framework for information that requires protection in the public interest and to preserve personal privacy with security classifications of SENSITIVE and IN CONFIDENCE. Classifications of TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED are used to protect information concerned with national security.

Classifying Information only provides effective protection if information systems are designed to enforce the classifications. IS is responsible for ensuring that data storage facilities within the Qualifications Authority are capable of supporting Information access restrictions.

Policy: *“Storage media for the Qualifications Authority’s Information must provide facilities for storing Information by classification as is appropriate for its use.”*

10.7 Disposal

The life cycle of storage hardware is relatively short. Escalating demands for capacity is a significant factor in this. An inevitable result is the growing requirement to reuse, or dispose of media once used to store classified information. The Government Communications Security Bureau (GCSB) maintains a set of publications titled the “New Zealand Security of Information Technology” (<http://www.gcsb.govt.nz/nzsit/>), of which “NZSIT207” is a set of guidelines on the declassification of storage media. Compliance with these guidelines is mandatory for the protection of Information on hardware which is to be disposed.

Policy: *“Any media containing classified Information which is no longer required must be disposed of in a secure manner.”*

Storage media may include paper, floppy disk, CD-ROM, DVD, Magnetic Tape and appropriate disposal mechanisms would include shredding and secure waste bins. In disposing of hardware or media a User must ensure that no Information is disposed of unless its disposal is permitted by the Public Records Act 2005.

11 Resource Usage and Access

When a User uses the Qualifications Authority’s Computer Network, both the physical Network, and the Qualifications Authority’s Information, may be accessed and used. These resources are secured during three main types of activities:

- A User profile is a template of what parts of the Computer Network, and what Information, an individual User has the authority to access and use. Every User has a profile unique to them, which is applied system-wide regardless of how the systems are accessed;
- User Authentication is a mechanism of ensuring that the person accessing the Computer Network and Information made available through a User profile, is the User the profile was created for. Different authentication mechanisms can be used depending on the method of communication (connection), used to access the Network;
- It is important to distinguish between the Administrative User and a General User, for the purposes of auditing and minimising the number of people with high-level privileges. Any User who has the ability to perform administrative functions should not be using the administrative account for day-to-day usage – they will also have a general account which must be used in those circumstances; and
- “Communications” refers to the way in which a User connects to the Computer Network. Different security measures can be applied to the communication mechanism depending on what mechanism is chosen. Securities are applied to ensure that only the authenticated User can view Information, or use the Computer Network over the communications mechanism.

Policy: *“Access to and use of the Qualifications Authority’s Computer Network will be secured through a combination of authorised unique User profiles, authenticated User access and applied security measures appropriate to the communication mechanism.”*

11.1 Network Access

Passwords are generally the last security barrier before a potential intruder gains access to the Computer Network. To get to the point of being able to enter a password, an intruder should have had to get past a number of physical or technical barriers. Because passwords are linked with User account names, they also validate an audit of User's actions whilst logged in under their User account name. Keeping Network access details confidential is therefore essential.

Shared User accounts defeat the principle of accountability, which attempts to attribute all system events to specific individuals. Use of an individualised User account & password, along with specific access control privileges, will prevent "secondary dissemination" of passwords because passwords must remain the exclusive knowledge of the involved Users.

Policy: *"All User accounts must be unique to each individual User of the Qualifications Authority Computer Network. User accounts contain the User's profile."*

Policy: *"Access to the Qualifications Authority Computer Network via shared User accounts is prohibited."*

Policy: *"Reusable group, or business unit based User accounts are prohibited."*

Refer to Appendix C for specific policies regarding passwords. Users are responsible for taking all reasonable precautions to ensure any material they introduce to the Qualifications Authority's Computer Network is suitable for the Qualifications Authority's business use.

Special care is required when the Qualifications Authority's Information is being used on equipment not owned by the Qualifications Authority. Because the equipment is out of the direct control of the Qualifications Authority security mechanisms, the Users using that Information are responsible for taking all reasonable steps to protect the Information's integrity and preventing unauthorised access to it. All requirements of this policy must be applied to the use of that equipment.

12 Access to Information

An individual User's access to Information is a function of the role they perform for the Qualifications Authority. Access rights are only granted for the period that the User holds the role. As Users move into different roles their User profile must change to reflect the access rights of their new role. When they no longer perform a role for the Qualifications Authority all of their User rights must be removed. Responsibility for providing access control lies with IS.

Policy: *"Access rights must be controlled to ensure that they are appropriate for each User's current role."*

13 External Access

13.1 The Qualifications Authority Network Perimeter

Many major security risks can be averted if access to the Qualifications Authority's Computer Network remains secure from unauthorised external access by being confined within its perimeters. A perimeter is anywhere that the Qualifications Authority's Computer Network may come in contact with people or resources outside of the Qualifications Authority. Examples of perimeters are Internet connections, modems connected to public networks, floppy disks/CDs/DVDs/Memory sticks/USB keys from outside of the Qualifications Authority, (including a User's home) and even a computer monitor that is in an area accessible to the public.

Perimeters represent a double risk to the Qualifications Authority because they provide a potential exit point for the unauthorised escape of Information from the Qualifications Authority's Computer Network and an entry point for compromising the integrity and availability of the Qualifications Authority's Information. This includes computer viruses, malicious damage and unauthorised access to, or use of, the Qualifications Authority's Computer Network.

Policy: "All the perimeters of the Qualifications Authority's Computer Network must be secured against unauthorised access."

13.2 Remote Access

The most effective way to secure a perimeter is to remove any external access to it. However, removing all external access is not a viable option for the Qualifications Authority as there are many valid requirements for such access (examples include agent's access, remote access for staff, e-mail, web browsing, e-commerce and access for third party support and business partners). Points of access therefore are permissible but only if they are able to (i) authenticate and allow access for third party support and business partners, and (ii) authenticate and allow access for legitimate Users and deny all other access.

The very existence of networks creates a security risk for the Qualifications Authority, given that their purpose is to access, share and move information. Fundamental to the success of any efficient, secure and well run network is centralised design and management.

Policy: "The design, control and management responsibilities for all networks within the Qualifications Authority will be centralised under IS."

13.3 Access Points

Because Network risk is increased dramatically when external access to it is permitted, centralised control of external access to the Qualifications Authority's Computer Network is an inherent responsibility of network management.

A major concern in this area is the control of an end user's use of modems, or other similar devices, (these include connection devices to "Broad Band" services, eg ADSL, DDS, Frame Relay), to access external third party services. Inherently these types of services are designed for the residential market, where security is not a high priority. Additionally, if allowed, they represent uncontrolled high-risk connections to the Qualifications Authority's internal Computer Network. Centralising control of external access points ensures that no "back doors" or alternative unofficial access points exist that can compromise the security of the Network.

Policy: "The only access points into the Qualifications Authority Computer Network or connections to external networks that are to exist are those supplied and managed centrally by IS."

13.4 Acceptable Use of the Internet

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of information on the Internet is outdated, inaccurate, and in some cases deliberately misleading. Similarly, it is relatively easy to spoof the identity of another user on the Internet. As a result, Users should not rely on the alleged identity of a correspondent via the Internet unless the identity of this person is confirmed through methods approved by SMG (digital certificates, digital signatures, etc).

Refer Appendix D for specific policies relating to Internet Usage

In all instances, the User name, electronic mail address, organisational affiliation, and related contact information must reflect the actual originator of a message or posting. The use of anonymous "remailers" or other identity hiding mechanisms is forbidden and is not in keeping with the Qualifications Authority culture of straight and honest communication. The use of web browsers, anonymous FTP log-ins, and other methods established with the expectation that Users do not need to identify themselves is permissible.

The Internet has been plagued with hoaxes alleging various security problems like viruses, which will erase hard drives. Many of these hoaxes take the form of chain letters, which request that the receiving party send the message to other people. All Users in receipt of information about system vulnerabilities should forward this information to IS, and IS will then determine what, if any, action is appropriate.

Policy: "Users must not redistribute electronic mail or other information relating to viruses or other forms of system vulnerability information, except to IS to enable IS to verify the information and take any appropriate action."

13.5 Services through Network Connections

Once a direct connection has been established to a network the degree of security that can be exercised is limited. For an internal network connection, additional security is provided by virtue of the access mechanism (workstation) being physically housed inside the Qualifications Authority's premises. Because this protection is not available for external network connections, they must be appraised on a case-by-case basis to identify, define and implement the appropriate controls required at the level of the service accessed through each connection.

13.5.1 Remote System Administration

External access to make administration changes to the Qualifications Authority's Computer Network poses a particular threat. Authentication and authorisation may restrict access to those who have the appropriate logon information - however the transfer of that logon information is not completely secure. Although risk may vary depending on the access mechanism used, the potential for logon information being intercepted is real. If the logon information can provide access to administration rights then the impact could be extreme.

The very existence of external administrative access creates a risk of unauthorised access. Any unauthorised person accessing the Qualifications Authority's Computer Network with administrative rights could effectively have a free reign over the entire Network. Given that the access is unauthorised it must be assumed that any such access is with the intention of harming the Qualifications Authority's interests. The potential for damage is so great that nothing short of removing the ability to make administration changes via external access will mitigate the risk.

For these reasons, access to the Qualifications Authority's Computer Network for remote administration purposes must be rigorously controlled - identifying, defining and implementing the best controls available. Once approved and connected, the equipment used would be considered to be part of the Qualifications Authority's Computer Network and therefore inside an extended perimeter.

Policy: "IS is responsible for appraising each service being accessed via external network connections, to determine and implement the appropriate levels of authentication, authorisation, and auditing required to control access to and enable remote administration of the Qualifications Authority's Computer Network."

13.6 Third Party Access

This includes trusted third parties with administrative rights. If support is outsourced, the third parties providing support services are considered an IS resource. Accordingly, as with other IS resources, trusted third parties providing support services and the network infrastructure used to deliver those services must also be considered part of the Qualifications Authority's Computer Network and inside an extended perimeter. As a matter of course, all trusted third parties with access to the Qualifications Authority Computer Network are required, as part of their conditions of engagement, to agree to comply with this policy, as well as signing a Confidentiality Agreement.

13.7 Electronic Mail

Policy: *"Electronic mail accounts are for specific individuals and must not be shared."*

If a User goes on vacation or is otherwise unable to check their mail for extended periods, proxy access can be given to another member of that team. Likewise, notices can be established which will automatically notify correspondents that the recipient will not be responding for a certain period of time.

Policy: *"Upon departure from the Qualifications Authority, a User's electronic mail account must be terminated. External emails will be archived, internal emails will be held for a period of 6 months and then deleted, unless a request is made for them to be transferred to another User's email account."*

To restrict the dissemination of sensitive information, forwarding of electronic mail is to be carefully considered.

Policy: *"If an electronic mail message contains sensitive information, a User must not forward it to another recipient (including to addresses outside the Qualifications Authority) unless the User complies with section 10.5 and (1) the other recipient is authorised to view the information, or (2) the originator approves the forwarding."*

The internal use of the blind carbon copy feature in electronic mail systems is discouraged because it is inconsistent with the Qualifications Authority culture of straight and honest communication. The blind copy feature does have an acceptable use for external email, where it is used to keep addresses private when emailing to a large list. Broadcast electronic mail message facilities should not be employed except with the department manager's prior approval, but the use of selected distribution lists is both advisable and permissible without such approval.

Policy: *"Electronic mail should be directed to the smallest appropriate group of Users."*

Electronic mail is not protected from prying eyes by default. Electronic mail is the equivalent of a post card. Accordingly, Users must be careful about the inclusion of sensitive information in electronic mail messages that are not protected by encryption. To protect information from unauthorised disclosure, Users must employ approved encryption facilities (see section 10.5).

By default, all electronic mail messages are recorded in logs and back-ups. This means that even though an electronic mail message may have been deleted from a User's in-box, it may still be retrievable with other methods. Users are responsible for saving important messages, which might be needed at a future date. Electronic mail systems are not intended to be used as databases. Accordingly, any Information that constitutes a public record under the Public Records Act must be retained on the required electronic management systems.

Policy: *"Space restrictions must be placed on the storage and archival facilities provided for the corporate email system. All Users must ensure Information is retained in accordance with the Public Records Act."*

Policy: *“Users must not use language or material that infringes upon the rights of others or which a reasonable person might consider to be abusive, profane, discriminatory, sexually explicit, offensive or defamatory. All communications must comply with the Qualifications Authority’s requirements and legislative standards.”*

Users must be careful not to use derogatory or defamatory remarks in any electronic mail messages discussing employees, clients, competitors, politicians or others involved with the Qualifications Authority. Such remarks, even when made in jest, may create legal problems such as defamation, and may lead to legal proceedings against the User or the Qualifications Authority and to disciplinary action.

Further, Users must not use the Qualifications Authority’s information systems for any type of harassment, including sexual, ethnic or racial harassment. Such behaviour is strictly prohibited and will be cause for disciplinary action. If you are the recipient of this kind of harassment you should report the harassment to your manager and/or a member of the Human Resource Services team. Please refer to the HR Policy Manual section on Workplace Harassment for further guidance.

Policy: *“The Qualifications Authority’s Computer Network and information systems - including telephone calls, electronic mail, and internal mail - must not be used for any type of harassment, such as sexual, ethnic, or racial harassment.”*

13.8 Virus Detection

Any data received from an external source has a degree of risk associated with it such as introducing viruses or malicious code. To guard against this, virus detection is built into any external access mechanism. Responsibility for providing protection mechanisms for viruses lies with IS. Users must ensure data from an external source is scanned for viruses before introducing it to the Qualifications Authority’s Computer Network.

Policy: *“Any data introduced to the Qualifications Authority’s Computer Network from an external source must be screened for the presence of malicious code (including viruses).”*

14 Business Continuity

The policies set out below are to be read in conjunction with any emergency response plans comprised in the Qualifications Authority’s Business Continuity Plan. These policies are designed to ensure that there is a continuity plan available and it is regularly tested and updated to represent the current status of the organisation.

All Users must ensure that any Information resources that are required in the course of their work are adequately covered by a backup plan. For example, Information should not be stored on Users local PC hard drives, as these are not typically included in the system backup process.

14.1 Business and Computer Continuity Planning Process

This policy requires that a formal process exists for the preparation and maintenance of the computer and communications Information Technology Service Continuity Management (ITSCM) Plans. Corporate Services are responsible for maintaining the corporate Business Continuity Plans (BCP). IS is responsible for maintaining the Disaster Recovery Plan (DRP).

Policy: *“The Qualifications Authority’s Information Technology Service Continuity Management (ITSCM) Plan must be documented and maintained by IS.”*

14.2 Preparation and Maintenance of Computer Emergency Response Plans

A distinction between emergencies and disasters is helpful. Emergencies require immediate attention but may not have long-term implications or serious financial consequences. Disasters have long-term implications, have serious financial consequences, and may or may not require immediate attention. The requirement of this policy is that IS prepare, update and test ITSCM plans in accordance with the Qualifications Authority's BCP.

Policy: "For computer and communications systems, IS must prepare, periodically update, and regularly test Information Technology Service Continuity Management plans. These plans must provide for the continued operation of critical systems in the event of an interruption or degradation of service."

14.3 Backing Up of Critical Data

The intention of this policy is to specify a minimum acceptable backup timeframe and also to specify what type of Information needs to be backed-up. Certain types of Information will need to be backed up more frequently, but these decisions must be made on an organisational and Information type basis. These decisions should be covered in the Qualifications Authority's Business Continuity Plan. These decisions should also be reviewed regularly as the critical back-up requirements may change over time.

Policy: "All critical business information and critical software resident on the Qualifications Authority's Computer Network must be periodically backed-up. These backup processes must be performed with sufficient frequency to support documented Information Technology Service Continuity Management plans."

14.4 Regular Testing of Stored Data Media

The intention of this policy is to ensure that archival Information will be readily recoverable if and when it is needed.

Policy: "Critical business information and critical software on computer storage media for a prolonged period of time must be tested periodically to ensure that the Information is still recoverable."

14.5 Off Site Storage of Backup Media

This policy ensures that backups are protected from local environmental disasters.

Policy: "Backups of essential business information and software must be stored in an environmentally-protected and access-controlled site which is a sufficient distance away from the originating facility to escape a local disaster."

15 Hardware

15.1 Hardware Inventory

To secure the hardware assets, an accurate inventory (the Fixed Asset Register), which includes the location of all hardware, must be kept. The purpose of this inventory is to ensure that all hardware can be accounted for physically and financially. The Fixed Asset Register is maintained by Finance.

Policy: “An accurate inventory of hardware must be maintained and reconciled annually with the Qualifications Authority’s fixed asset register.”

15.2 Hardware Responsibility

Being a physical asset, hardware is at risk from physical damage and physical removal. While the cost of replacing damaged, lost or stolen hardware is easily quantified there are also less tangible costs such as the loss of Information stored on the hardware and lost productivity and opportunity caused by unavailability of the hardware.

To protect the Qualifications Authority’s investment in hardware, individual Users are responsible for taking all reasonable steps to protect hardware from damage or loss. Special care is required when any part of the Qualifications Authority’s Computer Network is removed from the Qualifications Authority’s premises. Notebook computers are particularly vulnerable being both highly portable and highly desirable to thieves. In removing any of the Qualifications Authority’s Computer Network resources from the protection of the Qualifications Authority’s premises, individuals must take all reasonable steps to ensure the resource’s physical security. When travelling, Users should carry hardware as hand luggage (ie. not checked in) wherever possible.

Portable devices add another dimension to the problem of information security. NZQA supplied USB keys are password protected and encrypted and this is the minimum standard for these devices. Always protect a portable device with a password and configure the device to shut down (or lock in some other way) after a period of inactivity. That way, if the device is mislaid or stolen, access to the data will be made more difficult. Encrypt any sensitive data that is stored on your portable device or media such as a “USB key” that you may use. Doing this may require technical expertise, please obtain assistance from Information Services if needed.

If Qualifications Authority equipment (e.g. laptop, USB key) is lost or stolen, the CIO must be advised immediately and a report forwarded to the CIO and the staff member's manager as soon as practicable detailing the circumstances of the loss and Information stored on the device.

Policy: “All care must be exercised to ensure Computer Network hardware is not subjected to conditions, circumstances or acts that may cause damage or loss.”

15.3 Hardware Physical Security

Particular care must be taken to ensure the physical security of mission critical hardware since the impact of its damage or loss is greater than other hardware.

Policy: “Mission critical hardware must be securely housed and appropriate physical access restrictions applied.”

15.4 Authorised Hardware Changes

Hardware that is incorrectly repaired or configured or is configured without paying due care to appropriate work practices, can cease to function and can pose a threat to the function and integrity of other hardware, software and data. It is therefore important that only appropriately skilled and authorised people work on hardware.

Policy: “Hardware may only be installed, configured, modified, repaired, or uninstalled by appropriately skilled and authorised personnel in accordance with a documented change control procedure.”

15.5 Hardware Deployment

Because the Qualifications Authority's Computer Network resources are deployed exclusively to support the Qualifications Authority's business requirements, a strategy for deployment must exist to ensure optimum balance of efficiency, effectiveness and responsiveness. To preserve the integrity of the strategy, hardware can only be acquired after the appropriate expenditure and management approvals have been given.

Policy: *"There must be adequate controls over the procurement of hardware to ensure purchases comply with the deployment strategy and are appropriately authorised."*

16 Software

16.1 Software Inventory

To secure these assets, an accurate inventory, which includes the licences and installed instances of all software, must be kept. The purpose of this inventory is to ensure that all software can be accounted for physically and financially.

Policy: *"An accurate inventory of software licenses and instances must be maintained and reconciled annually by IS."*

16.2 Installation Media

Access to the original software installation media should be restricted to those with responsibility for installing it, should re-installation be required.

Policy: *"Software installation media containing mission critical software must be stored securely to prevent loss or corruption."*

16.3 Unlicensed Software

Software is not always purchased. It can be proprietary, meaning it has been developed and used for a specific requirement by the owner, or it is licensed, meaning a license can be obtained from the developer to use the software but ownership remains with the developer.

Using unlicensed non-proprietary software can expose the Qualifications Authority and individual Users to significant claims of breach of copyright. Such software is also unsupported by the vendor and endangers the integrity of the Qualifications Authority's other software through an increased risk of instability and viruses.

Policy: *"Only licensed software or software for which the Qualifications Authority has proprietary rights may be used on the Qualifications Authority's Computer Network."*

16.4 Authorised Software Changes

Software that is incorrectly installed, configured, modified or uninstalled, can cease to function and can pose a threat to the function and integrity of other software, hardware, and Information. It is therefore important that only appropriately skilled and authorised people work on the installation and configuration of software.

Policy: *"Software may only be installed, configured, modified, repaired or uninstalled by appropriately skilled and authorised personnel in accordance with change control procedures."*

16.5 Software Deployment and Procurement

Because the Qualifications Authority's Computer Network resources are deployed exclusively to support the Qualifications Authority's business requirements, a strategy for deployment must exist to ensure the optimum balance of efficiency, effectiveness and responsiveness. To preserve the integrity of the strategy, software can only be acquired after the appropriate expenditure and management approvals have been given.

Policy: *"There must be adequate controls over the procurement of software to ensure it complies with the computing resource strategy and is appropriately authorised."*

17 Network Services Procurement and Deployment

Because the Qualifications Authority's Computer Network resources are deployed exclusively to support the Qualifications Authority's business requirements, a strategy for deployment must exist to ensure the optimum balance of efficiency, effectiveness and responsiveness. To preserve the integrity of the strategy, network services can only be ordered after the appropriate expenditure and management approvals have been given. This is especially important in the case of network services as each new network connection potentially provides an external access point to the Qualifications Authority's Computer Network.

Policy: *"There must be adequate controls over the procurement of network services to ensure they comply with the deployment strategy and are appropriately authorised and controlled."*

18 Configuration Principles

The security of the Qualifications Authority's Computer Network will be greatly improved by reducing the dependency on everyday User behaviour through hardware and software configuration. Hardware and software configurations can automate many security practices such as User authentication, disconnection from the network after a predefined period of inactivity, and automatic file backups. Taken to an extreme, security configuration could also severely disrupt normal workflows and cause undue expense. Therefore the needs of the business should be considered as part of any default security configurations.

The Qualifications Authority operates a naming convention for the naming of network devices and resources.

Policy: *"The Qualifications Authority naming conventions should be followed where the identification of a resource is required."*

Policy: *"Where it is practical and cost effective, secure options for hardware and software configurations should always be chosen."*

18.1 Desktop Computers

The Qualifications Authority has in place a Standard Operating Environment (SOE) that dictates the initial configuration of a standard desktop computer. Without current standards for operating environments for the main computing platforms used on staff computers within the Qualifications Authority, the result would be considerable diversity, confusion and difficulty in controlling IT support costs. A Standard Operating Environment (SOE) policy provides a framework for minimising IT hardware and software acquisition and support costs.

Policy: *“In all cases where a new or re-used computer is inducted into the Qualifications Authority’s computer network, the Qualifications Authority Standard Operating Environment (SOE) build must be used.”*

18.2 Server Class Computers

Default installations of server software comprise the most common security risk to networked systems. All services not specifically required for the function of that server should be disabled as a matter of course. Many weak points in IT systems cannot be exploited in isolation by a potential attacker. It is often only a combination of vulnerabilities that makes successful infiltration of a computer a possibility. One recommendation for the operation of secure servers is therefore that different services should be located on different computers. Advantages of this philosophy are:

- Easier configuration of the individual computers
- Simpler and more secure configuration of an upstream packet filter
- Increased resistance to attacks
- Greater operational reliability

Policy: *“Individual network servers, including public servers, must be configured to offer only essential services.”*

Policy: *“Each network service must be on a dedicated, single-purpose host where practical.”*

18.3 Portable Computers

Removable resources such as notebooks and remote PCs which are at greater risk from unauthorised physical access, require an additional level of protection to prevent unauthorised access to the Information they contain.

Policy: *“Portable or remote PCs must be configured to require User authentication before allowing access to its stored data or resources.”*

19 Design Principles

19.1 Systems High Availability

The risk of losing the integrity or availability of the Qualifications Authority’s Computer Network will be reduced through good operational procedure and a rigorous system design. The procedures and designs need to ensure that Information is recoverable in the event of accidental or malicious loss. Mission critical systems need to be designed in such a way as to minimise the likelihood of failure and must also comply with hardware and software procurement policies to ensure an overall alignment with the Qualifications Authority’s needs.

Policy: *“The Qualifications Authority’s Computer Network must be designed and operated in a manner that assures their integrity, availability and security, while complying with computer resource procurement policies.”*

Policy: *“The Qualifications Authority’s computer network systems are to be designed to ensure their availability meets agreed Service Level Agreements.”*

19.2 Software Development

Software development is often conducted by external resources or outside of the controls of the operating environment. Because of this there is a risk that standard security considerations may be

omitted from the development brief. To counter this risk, whenever software development is commissioned, this policy must be considered as part of the design brief and thorough testing must be conducted prior to implementation.

Policy: “The Qualifications Authority’s Software development Life Cycle Standards must comply with this Computer and Information Security Policy document.”

To facilitate software development and testing, Users involved in development may require elevated privileges to development systems. However, these privileges must not be transferred to production systems. This implies an “operational system” is used for deployment.

Policy: “Software development Users must not gain elevated, or administrative privileges to production systems.”

Corporate Systems Administrators, by definition, perform their tasks addressing the overall organisational resource management needs.

20 Partners and Third Party Suppliers

20.1 Non Compliance

The Qualifications Authority’s Partners and Third Party Suppliers must comply with this policy as if they were Qualifications Authority personnel. Non-Compliance with this Computer and Information Security Policy by one of the Qualifications Authority’s Partners or Third Party Suppliers will require an examination of the relationship the Qualifications Authority holds with the partner or supplier. This includes evaluating contractual arrangements that exist between the two parties.

Policy: “All Partners of, and Third Party Suppliers to the Qualifications Authority must be supplied with, or given access to, this Computer and Information Security Policy document.”

20.2 Minimum Requirements

Because contractual commitments may be used as a means of censuring suppliers who breach this policy, the Qualifications Authority’s position will be strengthened if suppliers are provided with a copy of this policy and with the Acceptable Use Guidelines, and if supply contracts contain clauses requiring compliance with the Acceptable Use Guidelines.

Policy: “All partners or third party suppliers to the Qualifications Authority with access to the Qualifications Authority’s Computer Network are required to sign a confidentiality agreement.”

Policy: “All partner and third party administrative access to the Qualifications Authority’s Computer Network must be supervised and auditable. Administrative access should only be given if required by the person to perform partners/suppliers obligations and limited as far as possible. Any passwords associated with the administrative access given must be changed immediately on completion of the partner’s or third party business.”

If a partner or third party does not comply with this policy, the Qualifications Authority may, depending on the nature and seriousness of the incident, and on the terms of its contract with the partner or third party, do one or more of the following things (although it is not limited to these actions):

- Consult with and advise them of the Qualifications Authority’s requirements under the Acceptable Use Guidelines;
- Request them to take appropriate internal action to address the cause of the breach;

- Suspend, restrict or terminate their right to use the Qualifications Authority's Computer Network and Information;
- Seek compensation from them for damages or loss they caused or are responsible for;
- Use applicable clauses to terminate their contract;
- Report them to the police or other appropriate authority.

With the exception of consultation, any actions taken against partners and third party suppliers could have commercial ramifications. IS's responsibility is to escalate any breaches of this Computer and Information Security Policy to the appropriate business unit.

21 Recovery Action

In the event of a security violation, IS is responsible for initiating a process of recovery and prevention. The recovery process includes restoring systems and recovering Information that may have been lost or damaged and requesting the appropriate Qualifications Authority resources to assist with commercial and communications issues. The prevention process involves taking the appropriate measures to establish the cause of the violation and prevent a recurrence.

The recovery process should be adhered to in conjunction with the Qualifications Authority's Business Continuity Plan. The following common elements, however, should appear in each department's plan:

- Internal notification;
- Temporary measure to protect information, systems and customers;
- Customer notification where required;
- Permanent repairs to affected information and systems;
- Root cause analysis;
- Preventative measures to stop a recurrence of the breach.

Policy: *"All suspected information security incidents must be reported immediately to the SMG via the CIO."*

22 Software Security

Non-commercial and personal commercial software must not be installed on the Qualifications Authority's Computer Network except with the prior approval of IS.

In addition, Users must not download software from the Internet unless for the Qualifications Authority business purposes.

Policy: *"Software must be used in accordance with licensing agreements and copyright law."*

Policy: *"Software must not be installed on the Qualifications Authority's Computer Network except with the prior approval of the CIO, or the CIO's designate."*

Policy: *"Users must not download software from the Internet unless for the Qualifications Authority business purposes, and only with the prior approval of SMG."*

Appendix A

Definitions used in this Policy

“Acceptable Use Guidelines” means the “Qualifications Authority General Computer, Internet and Email Guidelines”, which set out the guidelines for the acceptable use of the Qualifications Authority’s Computer Network and Information.

“Computer Network” means the Qualifications Authority’s computer network and includes all hardware (including portable computers), software, floppy disks, CD-ROMs, other storage media, modems, and other network resources.

“Computer Security” means the protection of the Qualifications Authority’s Computer Network from unauthorised access and/or usage, whilst maintaining the reliable operation of those Computer Networks.

“download” means the transmission of a file from one computer system to another. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.

“Electronic Communications Channel” means any process, or mechanism that provides the ability to move electronic information from one point to another.

“email” means Electronic Mail. This includes corporate email systems (like GroupWise), Web mail systems (like HotMail & GroupWise's “Web Access”) and any other system that electronically transfers messages in a “store and forward” manner.

“Extranet” means an extension of an institution's intranet, especially over the World Wide Web, enabling communication between the institution and people it deals with, often by providing limited access to its intranet.

“Information” means any information held on or transmitted over the Qualifications Authority’s Computer Network, whether or not in printable format, and includes any file, document, electronic mail communication and where any information is printed onto paper, includes the paper version of that information.

“Information Security” means the preservation of the confidentiality, availability and integrity of the Qualifications Authority’s Information, where “confidentiality” is defined as ensuring that Information is accessible only to those authorised to have access, “availability” is defined as ensuring that authorised Users have access to Information and associated assets when required, and “integrity” is defined as safeguarding the accuracy and completeness of Information and processing methods.

“Internet” means an interconnected system of networks that connects computers around the world via the TCP/IP protocol.

“Intranet” means a privately maintained computer network that can be accessed only by authorized persons, especially members or employees of the organization that owns it.

“Mission Critical” means if the system, or application fails, crashes, or is otherwise unavailable to the organisation, it will have a significant negative impact upon the business.

“Partner” means any third party provider that is working in conjunction with the Qualifications Authority to provide an IS type service or product.

“SMG” means the Security Management Group. The SMG reports to the EMC.

“SOG” means Security Operations Group. The SOG is a sub-committee of the SMG and is chaired by the Technical Infrastructure manager.

“User” means any authorised user of the Qualifications Authority’s Information Systems, and includes employees of, and contractors to, the Qualifications Authority and any individual, or organisation which the Qualifications Authority permits the use of or access (including by connecting remotely) to the Qualifications Authority’s Computer Network.

Appendix B

E-Government Guiding Principles

“Common standards and policies to ensure data integrity, efficient data communication and effective return on capital investment are key to e-government. The adoption of common IS Policies and Standards is critical to providing the common ‘view’, which is a pre-requisite of cost-effective e-government.

The IS Policies and Standards are:

- *Based on Open Standards, wherever possible*
- *Supportive of contestable supply from multiple vendors*
- *Intended to deliver interconnection between products from diverse vendors*
- *Able to support a very scaleable infrastructure.*

They allow:

- *Delivery of the lowest cost of ownership while performing to negotiated Service Level Agreements*
- *Enhancement of business practices with the effective use of Information Systems*
- *Consistent access to validated management information for formulating policy and measuring operational outcomes”*

E-Government information is available from the www.e-government.govt.nz Web site.

Appendix C

Specific policies relating to Passwords

Policy: *“A User must not write down their network access details (including passwords) anywhere nor let any computer they are using save/remember their password.”*

Policy: *“Users must not divulge their personal network access details, including passwords or other network access tokens, to anyone else, including managers or systems administrators.”*

Policy: *“All User account passwords must be a minimum of 6 characters long, include both alpha and numeric characters and must not contain a User’s “User Account Name” be anything to do with the User’s real name, a relative’s name or any other easily guessed subject, or be a password that is used by the User for any other purpose.”*

Policy: *“All Intranet User account passwords will expire after 42 days (6 weeks). All other User account passwords must have an expiry period that will be determined by the SMG.”*

Policy: *“Systems will be configured to remember a User’s previous 8 passwords and prevent the User from re-using the same passwords for a period of a year.”*

Policy: *“The minimum password age will be one day to prevent Users from cycling through password changes until the User is back to the password the User was required to change.”*

Policy: *“Once a password has expired, the User will have a maximum of 6 grace logins before they have to change their password in order to access the system.”*

Policy: *“The User’s account will be locked out after 5 unsuccessful login attempts over a period of 5 days and not re-enabled until an administrator has determined the reason.”*

Policy: *“Users must either log off the Computer Network or lock their computer when leaving the office during the day, and log off the Computer Network when departing work for the day.”*

Policy: *“Computers must be configured to go into a locked state after a period of inactivity. Where the Qualifications Authority has no control over the client environment (ie: extranet & internet), a server-based inactivity timeout must be implemented (usually referred to as a session timeout).”*

Appendix D

Specific policies relating to Internet Usage

Policy: *“Users must not post to public discussion groups (“list servers”), chat rooms, or other public forums on the Internet unless their manager gives prior approval to the User making such a posting on behalf of the Qualifications Authority.”*

Policy: *“Qualifications Authority management may order the removal of any Internet posting by any the Qualifications Authority User that is deemed inappropriate or potentially damaging to the Qualifications Authority’s reputation.”*

Policy: *“Users must not download software (executable files) from the Internet except with the prior approval of SMG.”*

Users may download data files from the Internet, but must check these files for viruses before using them (decompression and decryption, when they are used, must be performed first).

Policy: *“Users must not send any sensitive parameters such as credit card numbers, telephone calling card numbers, fixed passwords, or customer account numbers through the Internet unless the connection or data is encrypted.”*

SSL in an on-line Web session is acceptable; PKI Certificate encryption is acceptable for email.

Policy: *“Users must not include SENSITIVE information in electronic mail messages sent through the Internet unless these messages are encrypted with an authorised encryption mechanism.”*

Policy: *“Subscription to real-time automatic information distribution services on the Internet (so-called “push services”) is prohibited except with the prior approval of the SMG.”*

Subscription to electronic mail distribution lists (also known as “news groups”) is permissible without this approval.

Policy: *“The establishment of any network connection with a third party (such as an “extranet”) is forbidden unless SMG has given prior approval to the controls associated with this connection.”*

Policy: *“Users must not establish any web pages, electronic bulletin boards, or other mechanism that provides public access to information about the Qualifications Authority, except with the prior approval of both their manager and the CIO.”*

Policy: *“Users must not establish an Electronic Data Interchange (EDI) or other electronic business system except with the prior approval of both their manager and the CIO.”*

Policy: *“Users must not misrepresent, spoof, obscure, suppress or replace their own or another User’s identity on the Internet or on any other the Qualifications Authority information system.”*