



POLICY 2-25

VERSION 3

Information Management Systems

Approved: Brad Fish
Chief Executive Officer

Date: 14 / 06 / 2006

Considered by the Board at the May 2006 Board meeting.

PURPOSE:

To ensure that PCQ gains the greatest value from corporate information by maintaining its consistency, accessibility and integrity.

POLICY FRAMEWORK:

Information Management Systems are to support the efficient operation of the whole of PCQ. They are to be corporate in nature and not dependent on any particular individual to operate.

Data only becomes an asset to PCQ when it is ordered and stored in such a way that it can be systematically retrieved. This process turns data into information. PCQ recognises that information is its second greatest resource. In order to gain the greatest benefit from that resource, it has to be treated with respect by all users.

Good information management practices also require PCQ to identify information that no longer needs to be retained and dispose of it. This must be done in accordance with PCQ's obligations under the *Libraries and Archives Act 1988* and the *Financial Administration and Audit Act 1977*. This legislation requires PCQ to retain information for prescribed periods and in prescribed forms.

APPLICATION:

This policy applies to all PCQ employees.

POLICY:

PCQ has established and will maintain an Information Management System (the System) for corporate information. The System includes processes for archiving and destruction of information in accordance with operational and legislative requirements. The System's detail is documented in the Information Management System Manual, a copy of which will be retained on the Intranet.

All users are to comply with the procedures when filing information.

1. Roles & Responsibilities

The Information Management Officer (IMO) has overall responsibility for the functioning of PCQ's Information Management System and its integrity. The creation and naming of files, where information is filed and advising users on the correct use of the System are dealt with in the procedures.

It is the responsibility of the individual user to decide whether information should be included in the Information Management System. If the information records an action or decision, or is created in the operation of the organisation, then it must form part of the Information Management System. Any form of information that is not a result of, or does not affect the operation of the business, such as periodicals, drafts, working papers, notes and newsletters, need not be retained.

All users are required to put accurate file references on all incoming and outgoing correspondence. The reference can either be in the form of a number or the name of the relevant file (at least first three levels).

All users of the system will use their best endeavours to comply with the System, including selecting the most appropriate file. Where the user is uncertain which file to select, they will approach the IMO for assistance.

The IT Support Officer will be responsible for providing backup service when the IMO is not available, and will remain capable of performing all the tasks and have the same responsibilities as the IMO.

2. Audit

The IMO will publish an audit plan, identifying areas to be audited and the sampling schedule. This will include random audits of files to ensure all information is accurate and on the correct file. The IMO will continuously monitor correspondence being placed on file. If a new file is deemed necessary the IMO will discuss with the relevant user and a new file title will be agreed.

3. Other PCQ Information Storage Systems

All corporate systems that store information should be consistent with the corporate classification system.

4. Information Security

4.1 Physical Records

The Information Management Officer is responsible for advising on and implementing measures to ensure the security of physical records to a level commensurate with their importance. Important records shall be protected from loss, destruction and falsification. For example, originals of major contracts will be retained in the fire resistant storage. The IMO will develop and maintain a register which identifies physical information which requires more secure storage than the broader records system.

4.2 Information Technology

4.2.1 Systems Administrator Responsibilities

The Systems Administrator will be responsible for developing and documenting access controls to ensure:

- control of access to information
- prevention of unauthorised access to information systems
- protection of networked services
- prevention of unauthorised computer access
- prevention of unauthorised access to information held in information systems
- detection of unauthorised activities
- information security when using mobile computing and teleworking facilities

4.2.2 User Responsibilities

Users will comply with systems administrator requirements developed to ensure the security of information systems, and follow good security practices in use of IT systems (eg in the selection and use of passwords). Users shall also ensure that unattended equipment has appropriate protection.

PROCEDURAL IMPLICATIONS:

This policy should be considered with AS/NZS 4444.2:2000 *Information Security Management*.

Related policies:

- Retention of Board Minutes and Papers
- Archiving
- Publications
- Information Technology Developments

REVIEW DATE:

This policy should be reviewed by December 2011.