

New Zealand Government Data Management Policies

version 1.1, July 2000

New Zealand Government Data Management Policies

Version Notes	4
INTRODUCTION	5
Preface	6
Contributing Agencies	8
THE BIG PICTURE	10
Interrelationships of Principles, Policies & Standards	11
GUIDING PRINCIPLES	12
POLICIES SUMMARISED	13
CONTROL POLICIES	16
Ownership	17
Stewardship	19
Custodianship	21
Treaty of Waitangi Obligations and Cultural Awareness	23
Charging/Cost Recovery	24
Access Rules	25
DEFINITION POLICIES	28
Data Identification	29
Document Identification and Capture	30
Context	31
Source	32
INTEGRITY POLICIES	33
Authenticity Integrity and Retrievability	34
Auditability	35
Interchange, Replication and Interfaces	37
Retention	38
STANDARDS	39
GLOSSARY	40
BIBLIOGRAPHY	46

APPENDIX 1 – RELATIONSHIP TO PREVIOUS PAN-GOVERNMENT INFORMATION POLICY	50
APPENDIX 2 – POLICIES AND STANDARDS WITH POSSIBLE PRIVACY ISSUES	53

Version Notes

Version Number	1.0a
Summary of changes affecting meaning	Nil
Other changes	Correct name in 'External Contributors' Correct titles used in internal cross-references
Version Number	1.1
Summary of changes affecting meaning	Changes resulting from input from Privacy Commission: <ol style="list-style-type: none"> 1. Removed references to "private information" and replaced them with 2. Changed several policy rationale statements to indicate Privacy Act implications, rather than stating 'complies with the Privacy Act'; 3. Preface: Added warning not to regard use of the Policies & Standards as a substitute for familiarity with the Privacy Act; 4. Policies Summarised: Updated to reflect change to policy statement wording in Policy: Charging/Cost Recovery; 5. Policy: Stewardship: Added task for Crown Data Steward to consult with Privacy Commissioner; 6. Policy: Charging/Cost Recovery: Notes governance of Privacy Act over certain charges; 7. Addition of appendix showing policies/standards with potential privacy issues.
Other changes	Added number to first appendix title.

Introduction

Preface

The need for a government-wide set of policies and standards on data management is evident from a number of key observations about the nature of current practice, and how this has evolved since the 1980s. It is also based on the assumption that Crown data and document stores are of great value and need to be preserved for both operational and policy development purposes.

Before the widespread use of computer workstations, the bulk of Crown information assets were managed through paper document filing systems and a few large central databases. Filing systems had developed over many years, were mostly well organised, and had to be understood by employees for them to function. Data held in the central systems was protected by tight security and the discipline required to run a big data centre.

Since the advent of the State Owned Enterprises Act 1986 and the State Sector Act 1988, responsibility for Crown information assets has been devolved within the public service and to state, public and privately owned agencies. In addition, new technologies and media for creating and managing information have led to the breakdown of paper based information management structures. Large central computer systems have been split up with every agency now using its own applications and often running its own machines and network. Most workers in most government agencies can no longer function without a personal computer workstation connected to the agency network.

Crown data and document assets are now managed under a wide variety of regimes with little central guidance or control. The day-to-day management of electronic data and document resources is often in the hands of external commercial service providers. Unless business managers have a clear understanding of where responsibilities lie, and the limitations of technology, the assets are placed at high risk. These policies and standards are intended to address this risk.

This vision for electronic government is that agencies and the public will be able to do business through a standard electronic environment, that promotes public participation and trust. Secure and reliable electronic transactions operating with reliable data are a fundamental part of that environment. Without transparent, auditable policies, standards and procedures for data management, there is little chance that agencies will trust each other's data, let alone that the public will have confidence in such systems.

There are three policy sections which aim to cover all the essential business aspects of data management and allow available technology to be applied constructively.

Control policies and standards cover ownership, security, custodianship and related aspects. A structure for government-wide policy, standards and monitoring through the function of Crown Data Steward is described.

Definition policies and standards concentrate on identifying and describing data and document assets in a consistent way across government agencies. The objective is to improve the efficiency of data and document exchange, and hence information flow, both within and between agencies, and between agencies and the public.

Integrity policies and standards are aimed at the quality and reliability of data and document assets, and hence the reliability of any information derived from them. They will enable agencies to identify their prime data sources and ensure that content can be retrieved, audited, interchanged and retained to both legislative and business requirements.

These policies and standards are intended to assist agency chief executives and anyone delegated custodial responsibilities for Crown owned data or document assets. They are mandatory for public

service departments and contracted agencies handling Crown data and document assets. They are optional but highly desirable for State Owned Enterprises and other organisations funded by the Crown, particularly where information needs to be exchanged.

The Policies and standards were developed by a working group assembled from interested government agencies. They are based on material originally developed for the Department of Social Welfare. The working group drew on its own collective experience, other electronic government projects under way at the time, the work of other government agencies, and a variety of international standards and related material.

The Policies and Standards need to be read in conjunction with the associated E-Government Information Systems Policies and Standards. They should not be used as a substitute for familiarity with applicable legislation, such as the Privacy Act, but for data management issues where cross-sectoral legislation will be relevant, they endeavour to act as pointer to the legislation.

The approach taken can be summed up as follows:

- Keep it simple, but don't oversimplify
- Do what is relevant to your position and responsibility
- Do equivalent tasks the same way
- Know who's got what
- Track information flows effectively
- Give someone responsibility to ensure it all happens.

The Policies and Standards should be regarded as living documents, to be improved by regular reviews based on feedback from the Public Service, legislative changes, developments in international standards etc. It is unlikely that any government agency will be fully compliant from day one, however every agency will be required to demonstrate reasonable progress towards compliance.

Contributing Agencies

The table below lists the people and government agencies that directly contributed to the Policies and Standards. The input included initial comments on the terms of reference and the DSW standards, membership of the Working Group, specialist advice on particular topics, and periodic reviews of documents.

Additionally, we acknowledge the assistance of the States Services Commission in selecting the Working Group, facilitating liaison between the various E-Government projects and with the Chief Executives' IM/IT group, and keeping project managers informed of E-Government developments in other countries.

We also acknowledge the support and vision of the Chief Executives who championed the E-Government projects which these Policies and Standards form a part of. They were bold enough to seek and embrace the short-term discomfort of change for the ultimate benefit of the New Zealand Public Service.

Working Group

Project Manager	Wayne Pincott	Ministry of Social Policy
Project Consultants	Derek Rayner Trish O'Kane	Ministry of Social Policy SWIM Ltd
Group Members	Keitha Booth Edwin Bruce Elizabeth Buckley Barn McDavitt Ellen Moss Cheryl Remington John Roberts Laura Simpson Greg Sloane Stephen Walsh	Ministry of Economic Development Ministry of Fisheries Ministry of Justice Statistics New Zealand Work and Income New Zealand Ministry of Education National Archives Department of Inland Revenue Ministry of Agriculture and Forestry Land Information New Zealand

External Contributors

Bala Benjamin	Law Commission
Rob Brown	Ministry of Social Policy
Jean Cavaney	Department of Internal Affairs
Mike Clark	Ministry of Social Policy
Ros Coote	The Treasury
Tony Dawbin	NZ Qualifications Authority
Chelsea Grootveld	Te Puni Kokiri
Philippa Fogarty	Independent
Chris Fripp	Federal President RMAA, Australia
Brent Fry	Ministry of Agriculture and Forestry
Kevin Godwin	Foundation for Research, Science

Chris Hurley	and Technology
Joanne Koreman	National Archives
Dr Phillip Lindsay	Independent
Rob McNie	Agresearch Ltd
Dean Martin	Ministry of Transport
Brooke Martin	Ministry of Justice
	Ministry of Economic Development
Miles Middlemass	ERO
Richard Murcott	LINZ
Jenny McDonald	LINZ
Brett Mudgway	Department of Labour
Mike Pearson	Ministry of Fisheries
Dan Phelon	IRD
Steve Pyatt	NZ Defence Force
Brian Reeve	Housing NZ
John Ryan	Independent
Rinke Schonoveld	NRIMS Secretariat, Australia
Gerrard Smith	Land Information New Zealand
Inspector John Spence	Department of Prime Minister & Cabinet
Michael J Steemson	The Caldeson Consultancy
Robin Turner	Crown Law Office
Dallas Welch	Statistics New Zealand

THE BIG PICTURE

The diagram on the following page provides a one-page overview of the interrelationships between the Principles, Policies and Standards.

Interrelationships of Principles, Policies & Standards

Please view:

http://www.govt.nz/egovt/infopack/map_principles_policies_stds.xls

or

http://www.govt.nz/egovt/infopack/map_principles_policies_stds.pdf

GUIDING PRINCIPLES

Founding Principle:

Collaboration between and within agencies for the common good is fundamental to delivering E-Government benefits, especially those of open government, streamlined services and reduced cost.

1. Standardisation of policies within an agency and across agencies is beneficial to both the agency and to government as a whole.
2. Agencies must manage data and business documents in ways that are both deliberate and explicit, based on the adoption of relevant international and industry standards and guidelines.
3. Policies and standards should be straightforward and beneficial, applicable to any size of organisation and formulated to encourage good practice.
4. Data and business documents owned by the Crown are strategic assets.
5. Government agencies will be good corporate citizens, behaving responsibly with the data and business documents held by them.
6. Treaty obligations and cultural awareness issues pertain to data and document management.
7. Data and business documents will be publicly and equitably available and accessible unless explicit reasons preclude this.
8. Privacy and confidentiality of individuals and commercial interests will be protected.
9. Collection, use, retention and disposal of data and documents must be subject to legal and defined business requirements.
10. Data and business documents must be controlled, defined, and have integrity so that they are fit for the purpose of their collection.
11. Data and business documents should be collected or created once into a prime authoritative data source, then used many times.
12. Data and document management policies apply irrespective of storage medium.

Policies Summarised

Policy title and key statement

Ownership

Data collected by or for a government agency under statutory provisions, or by contract, or through an information-matching agreement under the Privacy Act, is owned by the Crown, not the individual agency. Other data may be supplied for use by agreement with an external owner. Business documents created or collected by or for a government agency are owned by the Crown.

Stewardship

The Crown through a responsible minister will appoint a Crown Data Steward with a government-wide mandate to manage and develop the Crown's data and document assets in accordance with established policies and standards.

Custodianship

Every item of data and every business document held by, or maintained for a government agency on behalf of the Crown, will have a Business Custodian and a Physical Custodian.

The role of Business Custodian is assumed by the agency's Chief Executive, who may delegate day-to-day responsibility to an appropriate employee. The role of Physical Custodian will be assigned to the service provider holding the data under an explicit directive or agreement.

Treaty of Waitangi Obligations and Cultural Awareness

Each agency will recognise and meet Treaty of Waitangi obligations and, where Maori are affected, consult with Maori in all issues relating to access, capture, usage, storage, transfer and retention of data and business documents. Each agency will also attempt to accommodate identified cultural, ethnic and religious issues related to data and document management, where they do not conflict with statutory and explicit business requirements.

Charging/Cost Recovery

Agencies may need to recover costs in some cases where information is disseminated from government data or document stores.

Agencies must apply the PFGHI (Policy for Government Held Information) pricing principle where information is disseminated from government data or document stores.

Agencies should refer to *Cabinet Committee Minute CGA(97)M10/1, 16 July 1997, "Government Information Supply Activities"* to determine an appropriate charging regime for the service.

The *Ministry of Justice Charging Services Guidelines* will set the actual price for the service, to ensure consistent pricing across Government.

Charges relating to an information privacy request where an individual requests access to, or correction of personal information, are governed by the Privacy Act.

Agencies will work in consultation with Treasury when establishing charging or cost recovery schemes.

Access Rules

The Business Custodian will establish and maintain access rules for the categories of data and business documents under his/her control. Access rules must be based on the principle of public and equitable access to information unless explicit reasons preclude this.

Data Identification

Government agencies will identify data elements for which they hold custodial responsibility by defining and maintaining their metadata in a data catalogue.

Document Identification and Capture

Agencies will create and implement policies and standards to identify and capture all business documents created or received in their processes.

Context

Contextual information about logical business data stores or complex datasets will be captured and stored in the agency's data catalogue.

Contextual information about business documents will be captured and associated with the documents and managed according to organisational policies and standards.

Source

Agencies will be able to identify and locate the prime authoritative source of their data elements and business documents. Where it is cost effective, prime authoritative sources should be held electronically.

Authenticity Integrity and Retrievability

Data and business documents will be managed to preserve and demonstrate their authenticity, integrity, and retrievability to meet business and statutory requirements.

Auditability

Data elements and business documents must be defined in a consistent manner and stored in a consistent format across all stores and, where required by the Business Custodian, changes to form or content must be recorded in an audit trail.

Interchange, Replication and Interfaces

Within legislative provisions and access protocols, information may be interchanged between agencies. The preferred method is via a defined electronic system interface to the appropriate data or document stores.

Retention

Data and business documents will be managed within a defined retention process.

Control Policies

Policy

Ownership

Data collected by or for a government agency under statutory provisions, or by contract, or through an information-matching agreement under the Privacy Act, is owned by the Crown, not the individual agency. Other data may be supplied for use by agreement with an external owner. Business documents created or collected by or for a government agency are owned by the Crown.

Scope & Interpretation

In the context of these policies and standards, the meaning of ownership is defined within the following statements.

When ownership is vested in the Crown it means that all relevant data and document stores must be treated as Crown assets, and must be managed by government agencies accordingly. In addition, agencies must act as good corporate citizens and apply appropriate care to data acquired from an external owner, or documents copyright to non-government organisations or individuals. Ownership of data refers to control of the Crown's copy of that data for statutory purposes and does not necessarily imply the exclusive transfer of intellectual property rights.

While the Crown asserts ownership of its copy of collected data, any data supplied by groups or individuals remains the property of those groups and individuals, except where statute or explicit agreement transfers exclusive intellectual property ownership to the Crown. See [Standards: Transfer of Intellectual Property](#).

Ownership confers the right of the Crown to instruct agencies and monitor that all relevant statutes and regulations are followed in collecting and managing the asset, and that these policies and standards are being applied.

In some cases data is collected and managed by external organisations under legislation for government purposes. This data is a Crown asset and must be managed accordingly. For a definition of government agency, see [Glossary: Government Agency](#).

Business documents are distinguished from non-business documents (see *GLOSSARY: DATA OBJECTS*) because non-business documents do not require the same level of active management.

Good management of Crown data and business document assets includes:

- Adherence to these policies and standards
- Adherence to statutory provisions of the *Archives Act*, the *Official Information Act*, the *Privacy Act*, *Copyright Act* and any specific empowering legislation for the agency
- The capacity to restrict data or documents or make them available to government or non-government agencies as required by government and allowed by law.
- Keeping abreast of the *Mataatua Declaration on Cultural and Intellectual Property Rights of Indigenous Peoples* and subsequent developments arising from it.

Supporting Standards:

Transfer of intellectual property
Reasons for collection/creation

Rationale

For data and business documents owned by the Crown, the Crown has a duty of care for their management, on behalf of the people of New Zealand.

Data is a key Crown asset without which business would be impossible. Clearly defined accountability and control over that asset is required to ensure that it is managed satisfactorily.

Documents, in many forms, deliver much of the value added to raw data by government employees. Clearly defined accountability and control over these assets is required to ensure that the value is not lost to the Crown.

Policy

Stewardship

The Crown through a responsible minister will appoint a Crown Data Steward with a government-wide mandate to manage and develop the Crown's data and document assets in accordance with established policies and standards.

Scope and Interpretation

Integrity of data is a key requirement to develop effective policy advice, deliver resulting services, and measure the results. Common data management policies and standards applied across government agencies promote integrity and consistent quality. When reliable data is easily available, the costs of delivering information are reduced and quality improves.

The objective of the Crown Data Steward is to ensure integrity and consistency of data as the raw material for the derivation of information and policy. The main responsibilities of the Crown Data Steward are:

- Develop and maintain the Data Management Policies and Standards on behalf of the Crown
- Exercise the ownership rights of the Crown to monitor that all relevant statutes and regulations are followed in managing Crown data and document assets, that the specified policies and standards are being applied, and report on the results
- Approve and ratify data and document management policies, standards and practices developed within government agencies to meet specific requirements
- Promote rationalisation of overlapping data stores and cost-effective use of data and document assets within legislative boundaries
- Develop the government high level data catalogue and publish in a workspace accessible to all government agencies
- Facilitate data and document sharing where appropriate by:
 - Assisting, and arbitrating if necessary, in the development of new sharing arrangements
 - Consulting with the Privacy Commissioner when personal data is included that may involve information matching or other provisions of the Privacy Act
 - Approving and monitoring both existing and new sharing arrangements, ensuring that business objectives and quality requirements are met.
- Ensure valuable data stores orphaned by agency re-organisation or other changes are transferred to an appropriate business custodian. (see also [Standards: Retention requirements](#), [Standards: Transfer between agencies](#), [Standards: Destruction protocols](#))

Rationale

All parties are in agreement that data collected through the activities of government agencies belongs to the Crown. However, concepts of stewardship, and how the Crown's ownership interests in data should be delivered are relatively recent and still evolving. Significant practical problems are beginning to become apparent with current stewardship arrangements. Problems include:

- Stewardship responsibilities are broken up among a huge range of departments
- Departmental stewards are likely to give priority to immediate departmental or narrower sector interests
- Departmental stewards have limited capacity to see the 'big picture'
- No central oversight of how departments are delivering their stewardship responsibilities

- Lack of government-wide strategic oversight of data developments to ensure that the Crown's data assets deliver consistent future returns to the Crown
- Data developments appear to be moving at too slow a pace to achieve government targets for e-government.

Together these issues demonstrate the need for a Crown Data Stewardship role with government-wide responsibility to manage and develop the Crown's data and document assets in accordance with established policies and standards.

Policy

Custodianship

Every item of data and every business document held by, or maintained for a government agency on behalf of the Crown, will have a Business Custodian and a Physical Custodian.

The role of Business Custodian is assumed by the agency's Chief Executive, who may delegate day-to-day responsibility to an appropriate employee. The role of Physical Custodian will be assigned to the service provider holding the data under an explicit directive or agreement.

Scope & Interpretation

The Business Custodian is accountable for maintaining the quality, integrity, availability, and security of data and documents at the levels expressed in these policies and any derived standards or better.

The Business Custodian normally has the exclusive right to control the updating or alteration of data, although this may be initiated by others e.g. under provisions of the Privacy Act. In some cases external organisations collect and maintain data on behalf of, or in partnership with, the Crown. The Business Custodian will agree a data management regime based on these policies and any derived standards with the external organisation.

In some cases the business and physical custodian may be the same person or group. The agreement will then take the form of a detailed definition of each role. Even though day-to-day duties may be delegated, there will always be one business and one physical custodian responsible for every data element and business document.

In particular, the Business Custodian will ensure:

- Maintenance of an explicit directive or agreement with a Physical Custodian and monitoring of performance for all data and document stores under his/her control
- Inclusion of these policies and standards in all relevant service, purchase or development contracts
- Application of the policies and any derived standards within the agency
- Participation in relevant shared management arrangements or other inter-agency initiatives
- Transfer of data stores orphaned by agency restructuring or other causes to an appropriate custodian.

Over time, the prime authoritative source may move to different Business and Physical Custodians. In some cases the same logical data element could have different custodians based on length of retention, particularly if it loses operational value over time but retains analytical or historical value.

The Physical Custodian is responsible for the continued physical existence, availability, integrity and security of data or documents for as long as is required by the Business Custodian and defined in an explicit directive or agreement.

Supporting Standards

Physical Custodian Agreement

The position, not the person

Rationale

The concept of custodianship of data and documents allows agencies the day-to-day control they need over the assets for which they are held accountable. It does not confer ownership, which is vested at a higher level.

The Physical Custodian performs a key role in maintaining the agency data and document resources on behalf of the Crown. It is essential that clear lines of accountability be maintained between the Business Custodian and both internal and external service providers.

Policy

Treaty of Waitangi Obligations and Cultural Awareness

Each agency will recognise and meet Treaty of Waitangi obligations and, where Maori are affected, consult with Maori in all issues relating to access, capture, usage, storage, transfer and retention of data and business documents. Each agency will also attempt to accommodate identified cultural, ethnic and religious issues related to data and document management, where they do not conflict with statutory and explicit business requirements.

Scope and Interpretation

The Crown acknowledges the potential cultural sensitivity of some data and business documents, and has the intent to be a good corporate citizen. However, a cultural perspective may be in conflict with statutory or business requirements and different cultural perspectives may be in conflict with each other. Agencies should therefore manage data and business documents so that both Treaty obligations and cultural issues are considered and managed in a transparent and sensitive manner, even if each agency decides it cannot satisfy the wishes of all groups on some issues.

When determining explicit business requirements for data and document management, agencies should identify obvious key points where Treaty of Waitangi obligations or cultural issues may arise. Examples are requesting, supplying, or disposing of data or documents:

- About individuals
- About cultural practices
- For Maori, also about land and places.

In addition, where Treaty of Waitangi or cultural issues are brought to their attention, agencies must be able to demonstrate how they have responded.

Treaty obligations and cultural awareness can encompass a broad range of issues including information capture, intellectual property rights, availability/security, contextual/metadata, usage, storage and retention.

Examples:

- Some cultures define family relationships very broadly e.g. who is an “aunt” or “brother”, and have various family naming conventions. Individuals can have different names to be used in defined contexts. Agency systems are typically set up to handle data and documents within a narrow set of conventions. This can lead to confusion in descriptions of relationships, and the handling of family and individual names, titles etc. Agencies could respond by clarifying what family relationships are being described and by allowing for a broader range of naming conventions.
- Naming geographic features with significance to several different groups.

Agencies may also seek to have statutory requirements reviewed where it is judged that they conflict unnecessarily with Treaty obligations and cultural issues.

Rationale

- Responds to the Crown’s Treaty obligations to know the effects of its policies on Maori
- Demonstrates the agency’s commitment to the Treaty of Waitangi
- Improves the ability of agencies to meet the needs of their customers, and to demonstrate awareness of their cultural differences
- Aligns agencies with Te Puni Kokiri, Ministry for Pacific Island Affairs and SSC guidelines, and assists agencies to demonstrate a commitment to the Treaty of Waitangi
- Allows agencies flexibility in managing cultural, statutory and business requirements.

Policy

Charging/Cost Recovery

Agencies may need to recover costs in some cases where information is disseminated from government data or document stores.

Agencies must apply the PFGHI (Policy for Government Held Information) pricing principle where information is disseminated from government data or document stores.

Agencies should refer to *Cabinet Committee Minute CGA(97)M10/1, 16 July 1997, "Government Information Supply Activities"* to determine an appropriate charging regime for the service.

The *Ministry of Justice Charging Services Guidelines* will set the actual price for the service, to ensure consistent pricing across Government.

Charges relating to an information privacy request where an individual requests access to, or correction of personal information, are governed by the Privacy Act.

Agencies will work in consultation with Treasury when establishing charging or cost recovery schemes.

Scope and Interpretation

In many cases charges are either set by legislation, or can be agreed between the parties involved in a data sharing arrangement.

Where there is disagreement, or where charges to individuals or private organisations are not mandated in legislation, the policy papers above must be adhered to, along with any subsequent guidelines issued or endorsed by Treasury. In all cases, Treasury rules take precedence.

Where there is doubt about existing guidelines produced by other government agencies, Treasury must be consulted.

Each agency should develop its own guidelines, based on those of the policies described above, where more detailed rules are required.

Rationale

Dissemination of information derived from Crown data or document stores extracts value from a government funded asset. Treasury must set or endorse the policy for any charging to ensure that individual agencies follow the same regime.

Policy

Access Rules

The Business Custodian will establish and maintain access rules for the categories of data and business documents under his/her control. Access rules must be based on the principle of public and equitable access to information unless explicit reasons preclude this.

Scope and Interpretation

The intention of this policy is to ensure that rules are in place to govern access to documents and data. Sensitive material needs to be secure; access to other data and document assets should not be unnecessarily restricted. Each agency must preserve the security of material with a government security classification. In order to complete this task it will be necessary to define the prime authoritative source for all data elements and document categories (see *SOURCE*).

Complex datasets e.g. geospatial databases, may contain several categories of data that need to be viewed together in context to provide meaningful information. In these cases it is necessary to apply a security classification to the dataset at the level of the most sensitive data it contains.

Where data is extracted from multiple datasets or data stores and combined, the resulting dataset or report may require greater security than its constituent parts.

A document may also contain several categories of data with different security requirements that cannot be separated without editing. Documents must be assigned a security classification according to the most sensitive data they contain.

Rules will be consistent with relevant legislation and government requirements for inter-agency data and document sharing, and access by external organisations or individuals. The main acts governing this area, apart from those governing individual agencies, are: the *Privacy Act*, the *Official Information Act*, the *Statistics Act*, the *Copyright Act* and the *Archives Act*. Rules will also be consistent with Department of Prime Minister and Cabinet security guidelines.

Security systems implemented around data and document stores must follow the access protocols established under this policy. This will achieve a consistent approach to security across agencies that can work both internally and for external interfaces.

The table 'Indicative Categories of Data and Access Protocols' shows an indicative rule set and may be used to assist preparation of data access rules for a particular agency. Once data is categorised for access and security, document access rules may be based on their data content.

Supporting Standards

Publishing

Security

The position, not the person

Secure electronic exchange

Individual privacy and confidentiality

Commercial sensitivity

Equity of access

Rationale

Clear and well-known access rules allow government agencies to get maximum use out of the Crown investment in data and document assets. This can improve performance through:

- Retention of “Corporate memory”
- Improved quality and consistency of outputs
- Quality decision making at strategic and operational levels
- Reduced duplication
- Improved ability to respond to customers’ needs
- Improved ability to respond to requests for information
- Increased confidence in the availability of data and documents.

Indicative Categories of Data and Access Protocols

Data Pertaining to:	A Private Individual	An Employee	The Agency	External Organisation	The Physical Environment	Data views, Summary Data & Statistics	Data Matching Interchange
Provided by	The individual Crown Agencies Other third parties	The employer Former employees Employment agencies Other third parties	Agency Business units	External organisations Credit agencies Other third parties	Internal collection or external source, observation equipment	Data Warehouse, Research bureaux, Other third parties	Other agency matching agreement
In custody of	Agency CEO	Agency CEO	Agency CEO	Agency CEO	Agency CEO	Agency CEO	Agency CEO
Authority to maintain	Business Custodian	Business Custodian	Business Custodian	Business Custodian	Business Custodian	Business Custodian	Business Custodian
Use in data matching programme?	Only with legal authority (<i>Privacy Act</i>)	Only with legal authority (<i>Privacy Act</i>)	N/A	Only with legal authority (<i>Privacy Act</i>)	N/A	N/A	Only with legal authority (<i>Privacy Act</i>)
Must inform provider of purpose formally?	YES	YES	N/A	NO	N/A	N/A	NO
Use for other purposes?	NO	NO	N/A	YES	N/A	N/A	NO
OK to release to third parties without consent?	Crown Agencies for data matching & subject to legal authority	NO	Subject to OIA request	Subject to legal authority, copyright, or prior expression of confidentiality	Subject to copyright and commercial sensitivity	Subject to confidentiality & copyright + Official Information Act	NO
Subject has the right of access, update, and review and to have dissenting view recorded?	YES	YES	YES	YES	N/A	N/A	YES

Definition Policies

Policy

Data Identification

Government agencies will identify data elements for which they hold custodial responsibility by defining and maintaining their metadata in a data catalogue.

Scope and Interpretation

The purpose of the data catalogue is twofold: first to allow each agency to identify and better use its own data resources, and second to publish the definitions to a wider audience across the whole of government. Government agencies should not hold data that is not identified and labelled.

The content of the catalogue is metadata describing the properties of data elements and their context in databases or datasets. It does not contain actual values or allow the direct retrieval of actual values. For example, while the catalogue might show that Name and Address are data elements in a database, it would not show the name and address of any particular person.

A data catalogue must be in an electronic form suitable for the size and complexity of the data stores being described. It will have a functional rather than an organisational focus. For small agencies with limited quantities of data this may be a simple document, while for larger agencies more elaborate data or system modelling tools may be preferred.

Since the catalogue is in effect an asset register, it must contain enough information for an enquirer to understand the purpose, meaning, and most important properties of the agency's data elements and the context in which they exist. Properties will include a business definition and physical characteristics e.g. size or data type, which may be required to retrieve and use the data.

The form of the catalogue will be consistent with NZ Government core metadata standards to ensure interoperability between databases and datasets. In some cases specialised standards will apply to complex datasets e.g. geospatial data. See also [Context](#)

Individual agency catalogues will contribute to a government-wide high level catalogue to be made available through NZGO.

Any regular exchange of data between agencies, regardless of technology, including extracts directed to a data warehouse, will be accompanied by an exchange of catalogue definitions.

Over time, agencies will be expected to harmonise definitions of data elements held in common or used for matching purposes.

Supporting Standards

Individual responsibilities

Discovery implications

Data Catalogue

Process maps

Rationale

The Crown makes huge investments in collecting and storing data. An effective catalogue is essential to get best use of data assets both within agencies and across government.

Policy

Document Identification and Capture

Agencies will create and implement policies and standards to identify and capture all business documents created or received in their processes.

Scope and Interpretation

The need is to capture and manage documents of business and statutory significance to an agency, but not to capture and manage every document. See [Glossary: Data Object](#) for definitions of document, business document, and non-business document. In this context 'capture' means to get documents into a controlling system, whether paper based or electronic.

Analysis supporting the creation of agency policies and standards is necessary to identify:

- What processes take place in the conduct of the agency's business
- What business documents are gathered or created by those processes
- How business documents must be managed to meet the agency's business needs.

The agency's own policies and standards will be consistent with these policies and standards, and will permit the agency to implement sound practices for paper/electronic document handling. They also have significant implications for workplace procedures and training.

Supporting Standards

Discovery implication

Individual responsibilities

Data Catalogue

Process maps

Skills and training

Rationale

Identification and subsequent management of all business documents reduces the risk of poorly informed or inconsistent decision-making, increases business reliability, reduces duplication of effort, and prevents ad-hoc management by individuals. It helps agencies to demonstrate and maintain the credibility of business processes and to contribute to e-govt objectives, while it also reduces time spent servicing Official Information Act enquiries.

Policy

Context

Contextual information about logical business data stores or complex datasets will be captured and stored in the agency's data catalogue.

Contextual information about business documents will be captured and associated with the documents and managed according to organisational policies and standards.

Scope and Interpretation

Agencies must use a defined standard set of contextual information or metadata (see *GLOSSARY: METADATA*), that has been derived from New Zealand government metadata standards. These standards will exist at four levels:

1. international
2. community of interest
3. agency
4. interoperability between databases and datasets.

Each agency will have to develop a detailed set of standards to meet its own requirements, or ratify an existing set.

Standardisation facilitates the effective sharing of information, both within and between agencies. Agencies can add metadata requirements specific to certain categories of data or documents, e.g. metadata on a policy report might include the related business output. Advancing technology may enable changes in core and optional metadata fields, for example the agency may wish to include electronic signatures.

Core metadata must be sufficient to describe the document, dataset, or data store, and to establish its validity and relevance for business or evidential purposes. Capture of most metadata for business documents is best undertaken at the time they are created or received, usually by the individual involved. It will normally be a specialist task to define complex datasets or data stores.

Supporting Standards

See New Zealand Government metadata standards

Classification of documents

Core metadata

Rationale

Quality contextual information is a valuable resource for management. Accurate and adequate metadata assist agencies to comply with legislative requirements by demonstrating which documents are associated with a process at every stage. In addition, complex datasets and data stores can be defined in the data catalogue both as physical entities and logical groupings if required. Metadata can also be used to implement business rules, e.g. if the document is "final" then its status is "read only".

Policy

Source

Agencies will be able to identify and locate the prime authoritative source of their data elements and business documents. Where it is cost effective, prime authoritative sources should be held electronically.

Scope and Interpretation

Where data is held in multiple physical databases e.g. for analysis purposes or technical performance reasons, the Business Custodian will designate the master source of the data which will always take precedence should conflict in data values occur.

This implies that update procedures should be concentrated on the main data source, with the subsidiary data store(s) being fed electronically from the main data store. It also implies that the physical formats adopted in different databases for the same logical data element should be consistent.

Defining a prime source falls naturally into the process of defining access and security arrangements (see [Access Rules](#)).

It is relatively easy to describe the location of physical items such as paper documents, disks, tapes etc. For material held within a storage area network it may not be possible to establish a physical location lower than a managed unit as recognised by the system.

Supporting Standards

Prime authoritative data source location

Synchronise data and document stores and publishing systems

Rationale

The prime authoritative source is defined to ensure that only one version of any given data element or business document is recognised as the correct one. This prevents confusion and promotes consistency. The source must be locatable to prove that adequate management provisions are being applied to data and document assets.

Electronic storage, when managed and organised according to these policies and standards, provides superior retention and retrievability options over paper based systems.

Integrity Policies

Policy

Authenticity Integrity and Retrievability

Data and business documents will be managed to preserve and demonstrate their authenticity, integrity, and retrievability to meet business and statutory requirements.

Scope and Interpretation

This policy covers both the logical and physical integrity of data and document stores and their contents.

In order to present consistent information both internally and externally, document and data stores must be managed within agencies as a coherent whole. This means:

- All stores are known
- Duplication of content between stores is minimised and controlled
- Content is presented whole even if parts are stored on different physical media
- The original content, context, and structure of documents is preserved
- Authorised activities are permitted
- Unauthorised activities are prevented
- Relevant events are logged
- Content is retrievable in a usable format

Demonstrating the logical integrity of data at a single item level means ensuring that the content in a physical database or file matches the business (logical) definitions for those data elements.

Demonstrating the logical integrity of a business document means proving that the technology for managing the content of a document store performs to specifications.

Demonstrating authenticity means showing that systems for collection and storage were used in the manner intended, by reference to standard procedures.

Physical integrity must be guaranteed by the service provider acting as Physical Custodian. This will involve all aspects of managing the physical systems to maintain, store and deliver content from data and document stores.

Supporting Standards

Referential Integrity

Integrity of application software

Integrity of configuration

Integrity of content

Integrity of process

Skills and training

Version control

Document templates

Retrievability

Rationale

Agency data and business document resources lose their value in proportion to any loss in their perceived and actual integrity, authenticity and reliability. Any degradation in the value of Crown data and business document resource must be avoided wherever possible.

Policy

Auditability

Data elements and business documents must be defined in a consistent manner and stored in a consistent format across all stores and, where required by the Business Custodian, changes to form or content must be recorded in an audit trail.

Scope and Interpretation

The general requirement that data be defined consistently within each agency and between agencies is necessarily a long-term goal. The aim is to make sure that users can always compare "apples with apples", regardless of where the data came from.

The most obvious examples are classification schemes, which should follow international standards or generally accepted guidelines e.g. country codes or job types. Increasing importance will also need to be given to person identification details which may be used for access to government services through a common portal based on the internet.

Consistency in the metadata elements used to describe business documents is also an important goal for every government agency. This includes attributes of individual documents e.g. title, version etc. as well as agency-wide metadata, e.g. a directory tree structure or document classification scheme. Consistent storage allows consistent retrieval and the ability to follow an audit trail.

Change control over data structures, document templates, and systems that maintain content is essential to ensure that neither current nor historical material is corrupted or made invalid.

Comparison of the physical content of database fields with the logical definition is an audit task that should be included, where required, as part of a system data audit. It should also be checked as part of the internal audit procedures used by service providers.

The intention of a system audit trail is to track and report system access and data changes. It helps protect against the possibility of unauthorised change to critical or sensitive data elements by logging details of who made the change.

Data collected by machine e.g. scientific observations, or data with no person-related content might not need special audit provisions, depending on usage requirements.

With personal data, systems must not only track changes but must also allow the recording of any changes requested by the individual concerned which were not implemented. This is required under the Privacy Act.

Supporting Standards

Change control

Version control

Audit trail

Rationale

Auditing is the means whereby the integrity of Crown data and document assets is checked and verified. A clear audit report is easiest to achieve when data and document stores are well organised.

Consistent definition and storage is also important for the eventual harmonisation of definitions for key data elements throughout government, where these are held in common. This also aids in the compilation of statistics across government, which in turn assists operational and policy development.

Policy

Interchange, Replication and Interfaces

Within legislative provisions and access protocols, information may be interchanged between agencies. The preferred method is via a defined electronic system interface to the appropriate data or document stores.

Scope and Interpretation

At its most sophisticated a system interface may involve direct automatic database links, or hyperlinks to documents and data records with authentication via digital certificate. At its most humble, it may be a letter requesting a document as part of a formal manual procedure.

Interchange may involve a physical transfer one record at a time or in bulk, or establishing a temporary or permanent link between records on different systems. In general, interfaces should be designed to move the minimum amount of data to achieve the result required.

Interfaces for data matching purposes are controlled via the Privacy Act and must meet stringent criteria. All such arrangements must be subject to approval by the Privacy Commissioner unless specified in separate legislation.

Replication should normally be reserved for development of a data warehouse, high availability (hot) back-up sites, or where technological limitations require data to be duplicated at multiple sites. Where replication is undertaken the following principles will apply:

- One system for each data element or document will be identified as containing the master copy
- An audit trail will be retained to prove that the target matched the source at each transfer
- Data transformation between systems will be kept to a minimum and fully documented where required

Supporting Standards

Interchange

Replication

Interfaces

Migration

Rationale

To facilitate the delivery of government services, on-line government data and document stores need defined electronic interfaces to allow appropriate access. These can be used both externally by the public and internally between agencies to increase efficiency and improve service delivery.

Policy

Retention

Data and business documents will be managed within a defined retention process.

Scope and Interpretation

Parameters of the process such as retention time will be governed by legislation applying to particular agencies, business needs, or by provisions of the Archives Act, the Official Information Act or the Privacy Act.

Storage and back-up systems must ensure that data and documents are available in time to meet business requirements.

Supporting Standards

Media-independent classification of documents

Back-up, recovery and restore

Storage media

Disaster recovery

Retention requirements

Transfer between agencies

Destruction protocols

Rationale

Retention plans will allow agencies to retain stores of valuable business documents and data and dispose of unwanted material at the right time.

STANDARDS

This Policies document is complemented by a companion document, the “New Zealand Government

The standards emphasise best practice and minimum quality levels for implementation of these policies, rather than prescribing technological solutions which could be beyond the reach of smaller agencies. Government agencies who provided early input to the development advised that the policies and standards should avoid going beyond generic best practice into business, legal and technology specific areas (these are typically low-level, operational policies and standards).

GLOSSARY

The purpose of this Glossary is to define and explain terms used in the Data Management Policies and Standards

AGENCIES AFFECTED BY THESE POLICIES AND STANDARDS

These policies apply where any agency creates, collects or has custody of data elements and/or business documents owned by the Crown. Responsibilities attributed to an agency in these policies and standards fall ultimately to the Chief Executive Officer. see also [Copyright](#).

APPROVED DATA/DOCUMENT STORE

See [Data or Document Store](#)

ATTRIBUTE

A characteristic of an object or entity

ARCHIVES/PUBLIC ARCHIVES/ARCHIVED RECORDS

The terms archives and archived are largely avoided in the policies and standards, with a preference for reference to the retention of data or documents, some of which may have continuing value. This avoidance is because the terms are used in a range of ways in different contexts.

BACK-UP

The process by which electronic data and document stores are regularly copied to a medium that can be used to restore data and systems at the same or at an independent location.

BUSINESS REQUIREMENTS

Business requirements are those identified by an agency as essential or useful for its operation.

CLASSIFICATION

“Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification scheme.” (*ISO 15489-1 Draft standard on records management*). See also [Security-Classification](#) for the particular use of classification for security purposes.

CLASSIFICATION SCHEME

An arrangement or division of objects into groups based on characteristics that the objects have in common e.g. origin, composition, structure, application, function etc. (*ISO/IEC 11179-1:1999(E)*)

COLLECTION/CREATION

The process of acquiring or creating data elements or business documents, describing them, and including them in a primary authoritative data source.

COPYRIGHT

A property right primarily concerned with publication of original material. See the *Copyright Act 1994*: sections 14-16 for a full definition.

Copyright does not affect Crown ownership of data or documents held in databases or stores which is governed by other legislation including the Privacy Act. If material from these stores is published then intellectual property agreements including copyright may apply.

The Crown may own and may also have copyright over a document without necessarily owning data contained in it.

The Copyright Act 1994 states that the Crown holds copyright over works produced by “a person employed or engaged by the Crown”. The Crown does not hold copyright over works produced by Crown entities or State Owned Enterprises. The list of these bodies is legislated and they are as a consequence not bound to these policies and standards unless they are specifically engaged by the Crown to produce or collect data. (see also [Agencies affected by these policies and standards](#))

CUSTODIAN - BUSINESS CUSTODIAN

The agency with the prime statutory responsibility for the creation/collection, use, improvement, retention and disposal of primary authoritative data source(s). This agency will normally be the government agency with the greatest operational interest, even if the resource is managed externally on behalf of the Crown. The Business Custodian sets standards and responsibilities for the Physical Custodian, whether or not both roles exist in the same organisation.

CUSTODIAN – PHYSICAL CUSTODIAN

The organisation, group or individual responsible (through an explicit directive or agreement) to the Business Custodian for the physical preservation of data elements or documents and for making them available for use. This will normally be the service provider controlling the physical data or document store environments. The Physical Custodian could be in the same organisation to the Business Custodian or a separate one.

DATA

A representation of facts, concepts or instructions in a formalized manner, suitable for communication, interpretation or processing by humans or by automated means (*ISO 2382-4* also quoted in *ISO/IEC 11179-1:1999(E)*). See also [Data Objects](#).

DATA CATALOGUE

See [Standards: Data catalogue and function map](#).

DATABASE

A collection of related structures containing data and definitions of database objects.

DATA ELEMENT

See [Data Objects](#).

DATA ITEM

One occurrence of a [Data Element](#).

DATA OBJECTS

- ***Data element/Simple data object***

A unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes. (*ISO/IEC 11179-1:1999(E)*) . Elements of data can be defined by their meaning, their context and their physical properties. Includes metadata about documents and text fields in databases

- ***Document/Complex data object***

Contains multiple data elements, and is a self-contained grouping of complex data objects formatted to convey information.

Includes:

- Static Documents – electronic, paper, microfilm, large text fields including presentation information (e.g. HTML or XML pages), database BLOBs, maps, photos, digital images;

- Material with a time-based aspect. Visual items, including films/video footage; photos; digital images. Audio items, including voice-mail messages, audio-tapes e.g. recorded speeches.

Excludes:

Physical items that are not themselves formatted to convey information, but that can be described by data elements or documents. Examples are biological material and geological samples.

- **Business document**

Business documents are those documents with specified statutory and/or public purposes that support the business of the agency. They are self-contained records of business transactions, intended for person-to-person communication. They are primarily documents received or created as part of the agency's business, e.g. correspondence, reports, e-mail, and e-mail attachments.

- **Non-business document**

Non-business documents are typically not business-driven but, if created using Crown equipment on Crown time, they are still owned by the Crown. They do not require the same level of control, definition or integrity assurance as business documents. Agencies benefit from managing them to ensure that they are distinguished from business documents and have appropriate (short) retention periods. They include:

- Non-work material, i.e. literally 'personal'
- Trivial work-related material such as the time and place for meetings, administrative details
- Material seen by no-one except the creator and not communicated to anyone else or to file
- Copies of material sent from elsewhere *and* not meant to result in an action on the part of the recipient, e.g. advertising, material from the Internet
- Dynamic linked documents. These do not meet the criteria of being self-contained, and pose issues about maintaining integrity over time. A static version of a dynamic linked document could be a business document.

DATA OR DOCUMENT STORE

The physical storage space for data elements or documents. Includes electronic file systems or databases, paper based storage systems, etc.

- **APPROVED DATA OR DOCUMENT STORE**

A store that meets the explicit requirements of the business custodian for control, definition and integrity assurance of data or documents in the store.

Includes:

Database management systems, document management systems, records management systems.

Excludes:

Personal databases or electronic documents held in personal drives and physical records, where these are known only to individuals and not to the agency. Excludes systems that only provide finding aids, but includes tools for control, definition and integrity assurance

DATA WAREHOUSE

One or more data stores originating from prime authoritative data sources by an auditable replication process.

GOVERNMENT AGENCY

See [Agencies affected by these policies and Standards.](#)

DATA TYPE

“The format used for the collection of letters, digits, and/or symbols, to depict values of a data element, determined by the operations that may be performed on the data element.” (*ISO/IEC 11179-1:1999(E)*)

FUNCTION MAP

The correlation between the functions performed by an agency and data and document stores which support them.

INFORMATION

A collection of data objects presented with definitions in a form suitable for the intended audience. Effectively then:

Information = Data Object + Definition + Presentation.

INFORMATION INTERCHANGE

“The process of sending and receiving data in such a manner that information content or meaning assigned to the data is not altered during transmission.” (*ISO/IEC 11179-1:1999(E)*).

LEGISLATION

Government laws, including Acts, Regulations, Rules, Orders in Council

METADATA

“Metadata is data describing stored data: that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records.” (*DOD 5015.2-STD*)

“Metadata is the information and documentation which makes data understandable and shareable for
ISO/IEC 11179-1:1999(E), p.30)

1. For data elements held in a data store, their properties are also called metadata. These typically include size, data type, textual definition, etc. plus context properties e.g. whether the data element is mandatory or optional within its data set.
2. For a business document this includes the name of the author and/or the creator, the date it was created and/or edited, the name of the document, access rights, classification, etc.
3. For data and document stores, metadata describes the properties of the store or dataset.

OWNERSHIP

See [Policies: Ownership.](#)

POLICY

A course or principle of action. Policies are high level, focused, and specific actions can be derived from them.

PRIME AUTHORITATIVE DATA SOURCE

The data or document store that is authorised by the Business Custodian as the prime source for a defined set of data. This source will be the master record for any other copies, and holds the “correct” and up-to-date data for that data set.

PRINCIPLE

A fundamental truth or law as the *basis* for reasoning or action. In particular here, principles are an agreed set of assumptions, as the basis for the derivation of policies.

PUBLISH

Make publicly known (*Concise Oxford Dictionary*). Make widely available by one or more active delivery mechanisms, either within a specific group or agency or to a group of agencies or to the public in general.

A document management system alone is not a publishing system because it has a passive delivery mechanism – i.e. you search for what you want in a mixed set of unrestricted and restricted material. Production and distribution of printed material is publishing, as is electronic delivery via a structured website. Electronic publishing may be a replication of existing material or a link to material in a database or DMS.

RECORDS

“Recorded information, in any form, including data in computer systems, created or received and maintained by an organization or person in the transaction of business or the conduct of affairs and kept as evidence of such activity”. (*AS4390*).

RECOVERY

The process of recovering electronic data or documents, without loss, from a corrupted state caused by system or other errors.

REPRESENTATION (OF DATA)

The combination of a value domain, data type, and, if necessary, a unit of measure or a character set.

RESTORE

The process of restoring an electronic data or document store from back-up media at the same or an alternate location. Normally only required in the event of a general disaster and may involve some data loss from work done after the last viable back-up.

RETENTION AND DISPOSAL SCHEDULES

In order to manage records effectively, an agency should develop a **retention and disposal schedule**. A schedule allows the agency to describe classes or groups of records that are of archival value, while they are still current, and to ensure their appropriate management. It also permits the identification of other records for timely destruction. This applies to records in any medium.

If a Retention Schedule is agreed with National Archives, then disposal and archiving can be undertaken as normal business processes. The two parties also negotiate:

- Whether the records will be transferred to National Archives or retained in the agency to agreed standards
- What access the public will have to those archived records

SECURITY-CLASSIFICATION

(Adapted from papers written by the Interdepartmental Committee on Security)

A system of graded levels of security, where each grade has a prescription based on the damage that is likely to result from the unauthorised disclosure of information or material. These security-classifications “shall be applied” for material relating to “the security, defence or international relations of New Zealand” and “may also be applied” to “information or material of special sensitivity relating to ... the maintenance of the law or the economy of New Zealand”. (*Cabinet Directive [CO (82) 14]*). See also [Classification](#), used for the categorisation of information.

STANDARD

“A standard is a published document that sets out the minimum requirements necessary to ensure that a material, structure, product, method or system will do the job it is intended to do.” (Standards New Zealand)

Standards can demonstrably be met or not met through observable and testable evidence. They set limits and are more detailed and explicit than policies. They differ from procedures in that a procedure is a way of proceeding, especially a *mode* of conducting business or a description of how to do something.

STATUTORY REQUIREMENTS

Statutory requirements are those imposed on the agency by legislation (Acts and Regulations) or by court rules

STEWARDSHIP

SEE STEWARDSHIP POLICY

TEXT

Text is the combination of alpha and numeric characters to denote words, terms, numbers, identifiers, etc. Text can occur in a data element, or can be part or all of the content of a document.

VERSION

A document *version* or (*revision*) is the form of a document that is saved as a version subsequent to the original or to another version. The form may be a draft or a final.” (*Sutton*).

VITAL RECORDS

“Vital Records are those records without which the organization could not function. In identifying vital records, consideration should be given to those records which are needed to:

- Operate the organization’s functions after an emergency or disaster
- Re-establish the organization’s functions after an emergency or disaster
- Establish and protect the rights and interests of the organization and its clients”
- (Australian Records Management Standard *AS4390*)

“Records identified as essential for the continuing conduct of an organization’s business, including the recreation of its legal status and determining the rights and obligations of its stakeholders.” (*ISO/CD 15489-1*)

BIBLIOGRAPHY

This bibliography is a combination of references, and of links to websites that were current at the time the policies and standards were developed. It is not an exhaustive list, but contains all the key documents referenced by the development project. Some of the web addresses may have altered since this table was compiled.

Organisations	Address
Archives of Australia, Local Government, University and other Archives	http://www.aa.gov.au/
Centre for Technology in Government, United States	http://www.ctg.albany.edu
Ministry of Justice, New Zealand	http://www.justice.govt.nz
NARA (National Archives and Records Administration), United States	http://www.nara.gov
National Archives of Canada	http://www.archives.ca/index.html
National Archives, New Zealand	http://www.archives.govt.nz
School of Information Management and Systems, Monash University, Australia	http://www.sims.monash.edu.au
State Records NSW, Australia	http://www.records.nsw.gov.au
State Services Commission, New Zealand	http://www.ssc.govt.nz
University of New South Wales Archives, Australia	http://www.library.unsw.edu.au/~archives/archives.htm 1

Issue

Article Title

Address/Reference

Custodianship and Stewardship

New South Wales Custodianship Guidelines for Natural Resources Information. Draft.	http://www.nrim.nsw.gov.au/custod/guide.html
--	---

Data interchange/consolidation

Final Report on the Feasibility Study into the Costs and Benefits of Integrating Cross-sectoral Administrative Data to produce social statistics.	Statistics New Zealand, Wellington New Zealand, 1998.
Information retrieval application service definition and protocol specification for open systems interconnect, ANSI/NISO Z39.50-1995.	ANSI/NISO
Information technology – Data management – Part3: IRDS export/import facility, ISO/IEC 13238-3:1998 – International Standard	ISO/IEC
Information technology – Guidelines for the organization and representation of data elements for data interchange – Coding methods and principles, ISO/IEC TR 9789:1994 – Technical Report.	ISO/IEC
Information technology – Information resource dictionary system (IRDS) services interface, ISO/IEC 10728:1993 – International Standard	ISO/IEC

Email and Record Keeping

E-mail and other flood control problems	http://www.chips.navy.mil/chips/archives/99_jan/erm104.htm (United States)
---	---

Evidence

Legal admissibility of information stored on Electronic Document Management Systems	http://www.caldeson.com/admit.html (New Zealand)
Report 50, Electronic Commerce. Part One. A Guide for the Legal and Business Community. Chapter 5, Evidence	Law Commission, 1998 (New Zealand)

Glossary of Terms

Glossary of Common Records Management Terms	http://www.epa.gov/nrmp/gloss/ (United States Environmental Protection Agency)
---	--

Information management policy

Guiding principles for the Justice Sector Information Strategy	http://www.justice.govt.nz/pubs/reports/1997/infopolicy/principles.html (New Zealand)
Managing your information: Justice Sector Information Management Policy Guidebook	http://www.justice.govt.nz/pubs/reports/1997/infopolicy/Default.htm (New Zealand)
Policy framework for government held information	http://www.justice.govt.nz/pubs/reports/1997/infopolicy/framework.html (New Zealand)

Metadata

AGLS (Australian Government Locator Service)	http://www.naa.gov.au/recordkeeping/gov_online/agls/summary.html (Australia)
Dublin Core Metadata Initiative	http://purl.oclc.org/metadata/dublin_core (United States)
Information technology – Information resource dictionary system (IRDS) framework, ISO/IEC 10027:1990 – International Standard	ISO/IEC
Information technology – Notation of format for data element values, ISO/IEC 14957:1996 – International Standard	ISO/IEC
Information Technology – Specification and standardization of data elements: <ul style="list-style-type: none">• Part 1: Framework for the specification and standardization of data elements, ISO/IEC 11179-1:1999 – International Standard• Part 2: Classification of data elements, ISO/IEC 11179-2:1999 – International Standard• Part 3: Basic attributes of data elements, ISO/IEC 11179-3:1994 – International Standard• Part 4: Rules and guidelines for the formation of data definitions, ISO/IEC 11179-4:1995 – International Standard• Part 5: Naming and identification principles for data elements, ISO/IEC 11179-5:1995 – International Standard• Part 6: Registration of data elements, ISO/IEC 11179-6:1997 – International Standard	ISO/IEC
Pittsburgh: Functional requirements for Evidence in Recordkeeping	http://www.lis.pitt.edu/~nhprc/prog1.html

Metadata, continued

Pittsburgh: Metadata Specification Derived from the Functional Requirements	http://www.lis.pitt.edu/~nhprc/meta96.html (United States)
SPIRT (Strategic Partnership with Industry - Research and Training), Monash University	http://www.sims.monash.edu.au/rcrg/research/spirt/ (Australia)
The MetaWeb Project	http://www.dstc.edu.au/RDU/MetaWeb/ (Australia)

Record Keeping Guidelines/Handbooks

The Disposal and Retention of Documents	Chartered Institute of Corporate Management (New Zealand) Inc, 1994
---	---

Security

Generic business security policy, version 0.1 (draft)	State Services Commission, June 1999
Security in Government Departments and Organisations. A handbook for staff.	Interdepartmental Committee on Security

Standards Development Framework

Information technology – Reference model for data management, ISO/IEC 10032:1995 – International Standard	http://isotc.iso.ch/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards/s017995e.pdf
---	---

Standards for Electronic Records Management

Australian Standard © Records Management, AS4390.1 1996, Records Management.	http://www.naa.gov.au/recordkeeping/rkpubs/advices/advice25.html (describes AS4390) http://www.standards.com.au/ (Australia) Standards Australia, Homebush, New South Wales, 1996.
Bibliography on electronic records 1995-1999	http://www.records.nsw.gov.au/publicsector/erk/websites/websiteguide.htm (Australia)
DOD 5015.2-STD: US Department of Defence Design Criteria Standard for Electronic Records Management Software Applications, 1997	US Department of Defence
Functional Requirements to Ensure the Creation, Maintenance and Preservation of Electronic Records	http://www.ctg.albany.edu/projects/er/fulfspcs.html (United States)
International Standard ISO/CD 15489-1. Records Management (draft).	Secretariat SAA., Internal Organization for Standardization, 1999
Models for action: Developing Practical Approaches to Electronic Records Management and Preservation	http://www.ctg.albany.edu/ (United States). Notes: navigate from this URL to the project page
National Archives Electronic Records Policy	http://www.archives.govt.nz/statutory_regulatory/er_policy/introduction_frame.html (New Zealand)
Standard for the Storage of Public Records and Archives. Draft Storage Standard, NAS 9901.	National Archives, Wellington New Zealand, 1999
Standards and Recordkeeping in the New Zealand Public Sector	http://www.archives.govt.nz/statutory_regulatory/standards/record_keeping/contents_frame.html (New Zealand)

Standards for software

Design Criteria Standard for Electronic Records Management Software Applications DOD 5015.2 STD	http://jitc.fhu.disa.mil/recmgt/ (United States)
OGO (Office for Government Online)	http://www.govonline.gov.au/ (United States)

Strategies for implementing electronic records management

Information Society Ireland Strategy for Action, Report of Ireland's Information Society Steering Committee.	Forfás, Dublin Ireland, 1996.
Modernising government.	Prime Minister and Minister for Cabinet Office, London, England, 1999
The Value Added Information Chain	Susan L Cisco and Karen Strong, <i>The Information Management Journal</i> , Vol 33,1 January 1999 (United States)
VERS (Victorian Electronic Records Strategy). Final report.	http://home.vicnet.net.au/~provic/vers/ Public Record Office, Melbourne Victoria Australia., 1998.

Treaty and Cultural Issues

Mataatua Declaration on Cultural and Intellectual Property Rights of Indigenous People.	
Maori and Records Management. Draft paper for the New Zealand Guide to Australian Standard AS4390 Records Management.	Wellington New Zealand, 1999

APPENDIX 1 – RELATIONSHIP TO PREVIOUS PAN-GOVERNMENT INFORMATION POLICY

The table below is intended to re-assure data and information managers that these Policies and Standards have been developed with an emphasis on building on existing public service best practice resources. Agencies that have sought to follow NZ public service best practice in developing their internal policies should have few difficulties with these Policies and Standards.

The table demonstrates the tight correlation between the Guiding Principles of these Data Management Policies, and two information policy documents with significant profiles across the public service - “Guiding principles for the Justice Sector Information Strategy” (JS) and “Policy Framework for New

These Data Management Policies and Standards are seen as a merging and evolutionary progression of the Justice work on information management policy and Ministry of Social Policy’s (MSP) data management policies. They also represent a ‘fleshing out’ of PFNZ.

Additional columns demonstrate relationships to other key sources, and show that the Policies are a genuine corollary of the Principles.

	JS	PFNZ	Relationships to other work	Relationships to Policies
1. Standardisation of policies within an agency and across agencies is beneficial to both the agency and to government as a whole.	1.	2.	Adapted from Delphi: “Standardisation of business rules across the enterprise, across agencies”	General
2. Agencies must manage data and business documents in ways that are both deliberate and explicit, based on the adoption of relevant international and industry standards and guidelines.				General
3. Policies and standards should be straightforward and beneficial, applicable to any size of organisation and formulated to encourage good practice.	6	9 10		General
4. Data and business documents owned by the Crown are strategic assets.	1	4 7	<i>Cabinet Paper CAB (98) M 22/28 29 June 1998</i>	CONTROL: Ownership
5. Government agencies will be good corporate citizens, behaving responsibly with the data and business documents held by them.			Chief Executives agreement with SSC <i>Cabinet Paper(EXG) (98) 65 On criteria for stewardship</i>	CONTROL: Stewardship Custodianship
6. Treaty obligations and cultural awareness issues pertain to data and document management.		3		CONTROL: Treaty of Waitangi Obligations and Cultural Awareness
7. Data and business documents will be publicly and equitably available and accessible unless explicit reasons preclude this.	9 3	1 2 11	<i>Official Information Act Statistics Act “Security in Government Departments and Organisations. A</i>	CONTROL: Charging/Cost recovery Access Rules

			<i>handbook for staff</i> ⁷ , published by the Department of the Prime Minister and Cabinet	
8. Privacy and confidentiality of individuals and commercial interests will be protected.			<i>Official Information Act</i> <i>Statistics Act</i> <i>Privacy Act</i> <i>"Security in Government Departments and Organisations. A handbook for staff"</i>	CONTROL: Access Rules
9. Collection, use, retention and disposal of data and documents must be subject to legal and defined business requirements.	7	6 8	Adapted from OGO (Aus) "Collection, use and disposal of information must be subject to legal requirements" <i>Archives Act</i> <i>Statistics Act</i>	CONTROL: Access Rules DEFINITION: Data Identification Document Identification and Capture Source INTEGRITY: Interchange, Replication and Interfaces Retention
10. Data and business documents must be controlled, defined, and have integrity so that they are fit for the purpose of their collection.	6	9 10		DEFINITION: Data Identification Document Identification and Capture Context Identification of Data Sources INTEGRITY Auditability
11. Data and business documents should be collected or created once into a prime authoritative data source, then used many times.	4	5		DEFINITION Source INTEGRITY Authenticity, Integrity and Retrievability Interchange, replication and interfaces
12. Data and document management policies apply irrespective of storage medium.			<i>Archives Act</i>	DEFINITION Source INTEGRITY Authenticity, Integrity and Retrievability Interchange, Replication and Interfaces

Key to Table:

JS = Justice Sector Guiding Principles

PFNZ = Policy Framework for NZ Government-held information

APPENDIX 2 – POLICIES AND STANDARDS WITH POSSIBLE PRIVACY ISSUES

Table Relating Policy Statements and Standard Statements

Note: Bold and Italic entries indicate possible privacy issue

Policy Statement Title	Standard Title
Ownership	
	Reasons for collection/creation
	Transfer of Intellectual property
Custodianship	
	Physical Custodian agreement
Access Rules	
	Publishing
	Security
	The position, not the person
	Secure Electronic Exchange
	Individual privacy and confidentiality
	Commercial sensitivity
	Equity of access
<i>Identification</i>	
	<i>Individual responsibilities</i>
	Discovery Implications
	Data catalogue and function map
	Process maps
Context	
	Core metadata
	Media-independent classification of documents
Source	
	Prime authoritative data source location
	Synchronise data and document stores and publishing systems
	Authenticity, Integrity, Retrievability
	Referential Integrity
	Integrity of Application Software
	Integrity of configuration
	Integrity of content
	Integrity of process
	Skills & Training
	Version Control
	Document Templates
	Retrievability
<i>Auditability</i>	
	Change Control
	Audit Trail

Interchange, Replication, Interfaces	
	Interchange Agreement
	<i>Replication</i>
	<i>Interfaces</i>
	<i>Migration</i>
Retention	
	Backup, Recovery & Restore
	<i>Storage Media</i>
	<i>Disaster Recovery</i>
	<i>Retention Requirements</i>
	Transfer between agencies
	Destruction Protocols