Policy

Information Management Policy

About this document

Note that printed document copies may not provide the most up to date information. Please refer to docCM for the current version.

Disclaimer	This document has been written for Department of Conservation (DOC) staff and contractors. As a result, it includes DOC-specific terms and refers to internal documents that are only accessible to DOC staff and contractors. It is being made available to external groups and organisations to demonstrate departmental best practice. As these procedures have been prepared for the use of DOC staff and contractors, other users may require authorisation or caveats may apply. Any use by members of the public is at their own risk and DOC disclaims all liability for any risk.
Document Coordinator	Mark Ingram, Enterprise Systems and Services Manager
Document Owner	Mike Edgington, Chief Information Officer
Approved for use by	Rachel Bruce, DD-G Corporate Services Date: 22/07/2020 DOCDM-1353574
Effective date	01/10/2014
Last reviewed	26/08/2019
Classification	UNCLASSIFIED
docCM ID	docDM-1353574

Department of Conservation
Te Papa Atawbai

New Zealand Government

Contents

1. Background

1.1 Purpose

The purpose of this policy is to clearly state the principles that guide our information management actions and shared responsibilities. DOC is committed to developing and maintaining information management practices that support our daily operations and enable DOC to meet its business needs, accountability requirements and partner expectations.

This policy shall also be read as being DOC's records management policy.

1.2 Scope

This policy covers all information created or received by DOC. It covers all media and formats, i.e. structured (e.g. data) and unstructured (e.g. text-based information, images, sound and video recordings).

1.3 Audience

This Information Management Policy applies to all DOC staff, contractors, volunteers and any other person working with our information.

1.4 Introduction/Context

Information is one of DOC's key assets. It informs our work and every one of us creates and/or uses information in some form every day. It is therefore important that we have a common understanding of what it means to 'manage our information', the principles that guide us in that process and the mandates that direct government agencies in this activity.

The information management policy covers policy statements, objectives, guiding principles, mandate, and roles and responsibilities.

For information on how to use the information management policy statements see the Related Documents section for current related SOPs and guidelines.

1.5 Objectives

Applying this policy will ensure:

- DOC operates most effectively by following good information management practice.
- A consistent approach to information management practices across the Department.
- We treat information with care and use it only for its proper purposes.
- We understand our specific roles and responsibilities as users and custodians of information.
- DOC demonstrates its commitment to, and compliance with, government mandates for managing and sharing information, in particular 'information is managed as an asset'.

1.6 Guiding principles

1. We value our information and look for ways to use and reuse it to grow conservation.
2. We build information management awareness, capability, and governance into our daily work.
3. We manage our information digitally by default.
4. We store information in DOC-approved repositories.
5. We champion an open and collaborative information culture both with our people and our partners.
6. We protect personal information to ensure compliance with the provisions of the Privacy Act 2020.
7. We protect commercial and sensitive information from unauthorised or inappropriate access or release.
8. We retain all rights in intellectual property created by DOC employees and independent contractors/suppliers generated in the course of their employment or engagement with DOC. Intellectual property is only assignable with the express written agreement of DOC.
9. We comply with the information management policy, and related standard operating procedures and guidelines when carrying out DOC activities.

1.7 Mandate

The mandate for this policy originates from the standards and legislative requirements governing the management of information in the public sector. These include:

Public Service Standards of Integrity and Conduct – we must treat information with care and use it only for proper purposes. We must not access information that is not relevant to our roles.

The **Public Records Act 2005** - as a government agency we must keep full and accurate records of our activities and must manage our information carefully on behalf of the public. We must adhere to all current Standards issued by Archives New Zealand (Department of Internal Affairs).

The **Copyright Act 1994** exists to protect copyright owners from unauthorised use of their work, while also setting out conditions for use by persons other than copyright owners.

The guiding principle of the **Official Information Act 1982** is that information held by the Department must be made available unless good reason exists under the Act for withholding it.

The **Privacy Act 2020** controls how agencies collect, use, disclose, store and give access to 'personal information'.

The **Contract and Commercial Law Act section 229(1)** provides that so long as certain requirements are met, an electronic record will be considered just as valid as a written record and if the electronic version of the record is a reliable means of assuring that the integrity of the information is maintained and that the information is readily accessible so as to be usable for subsequent reference then only that form of the record need be kept.

The Declaration on Open and Transparent Government says we must be proactive in sharing our information.

NZGOAL framework (NZ Government Open Access and Licensing framework) 'seeks to standardise the licensing of government copyright works for re-use using Creative Commons New Zealand law licences and recommends the use of 'no-known rights' statements for non-copyright material. It is widely recognised that re-use of this material by both individuals and organisations may have significant creative and economic benefit for New Zealand'.

The Government Chief Digital Officer directs government agencies to manage information as an asset (https://www.digital.govt.nz/digital-government/strategy/progress-towards-a-digital-government-strategy/).

New Zealand Information Security Manual (NZISM) mandates government agencies to ensure 'information important to its functions, its official resources and its classified equipment is adequately safeguarded to protect the public and national interests and to preserve personal privacy. This policy addresses the protection of the Confidentiality, Integrity and Availability of all official information'.

1.8 Terms and definitions

Refer to Appendix I for terms and definitions used in this document.

2. Roles and responsibilities

All staff members, including contractors, volunteers (where relevant) and any other person working with information must:

- Be familiar with the information management guiding principles set out in this document and apply them to their day-to-day activities; and
- Use the approved repositories for storing their information.

Managers and team leaders

In addition to their responsibilities as staff members, managers, and team leaders:

- Are responsible for championing the information management principles and practices within their business units.
- Must ensure their staff and contractors are aware of and are following the policy in their daily activities, and
- Provide support and guidance to assist staff to follow the policy.

Deputy Director-General Corporate Services

- Is accountable for the co-ordination and strategy of information management.
- Promotes compliance with information management policies and SOPs; and
- Finally approves and signs off policies covering information management topics.

Business owner – Chief Information Officer

- Is responsible for the implementation of information management practices including the oversight of appropriate documentation, training, testing, monitoring and reviewing of information management.
- Authorisation of approved DOC repositories; and
- Monitors compliance with information management policies and reporting to external parties on DOC's level of information management maturity.

Information Services and Systems Group

- Develops and delivers information management services, advice, and training.
- Supports integration of information management requirements into business and information technology strategies and plans.
- Collaborates with information resource and system owners to address information life cycle requirements in the development and operation of processes, systems, standards and tools.
- Analyses new or amended legislation, government policies and standards for information management impact; and
- Implements government-wide policies, directives, and standards.

- Develops information management standard operating procedures, guidelines, tools and best practices, as well as developing and supporting DOC information management initiatives.

3. Policy statements for Information Management Guiding Principles

1. **We value information as an asset.**

DOC values information and manages it as a public asset. This means that as individuals and as an agency we embed good information management practises to reduce work and to make good use of our organisational experience.

We create and hold information on the understanding that it has value beyond its immediate use and can be repurposed in many ways. We ensure our information is reliable and trustworthy.

Our information has a lifecycle from creation to disposal. Information will be held only as long as required and disposed of in accordance with the DOC records disposal authorities. As a public agency, DOC is obliged by law to manage its records effectively and to retain them only to meet business needs and statutory requirements. To comply with this requirement, we allocate retention periods to records to ensure that they are retained for the appropriate length of time but no longer. These retention periods are listed in DOC disposal authority and the Government General Disposal Authority. Contact Information Services for more information.

2. **We build information management awareness, capability, and governance into our daily work.**

DOC maintains a culture which values information management. We will define and assign information management accountabilities across all levels of the Department.

We will regularly communicate with staff, contractors, volunteers, and partners to inform and promote information management principles, policy and practice.

All staff will understand their responsibilities as information creators and users and, where appropriate, as information system owners/custodians/maintainers.

Information management requirements are an integral activity when developing new or revised business initiatives. All data and information systems will have identified owners, custodians, and maintainers to promote accountability, interoperability and improvement.

DOC will update and/or develop comprehensive standard operating procedures, guidelines and systems for information management.

3. **We manage our information digitally by default.**

DOC's approach is to create, receive and manage information in digital form wherever possible.

Digital information has considerable advantages over physical information. Digital information is readily available and able to be accessed quickly. It is searchable and able to be shared when maintained in a DOC-approved system. Digital information is easier to audit than physical information, because each interaction is captured in a dedicated metadata field.

Digital information is a considerable asset that can be used and re-used across government and in collaboration with our partners.

Records received in paper format are scanned and saved into the document management system or other business system for ease of future management, access and auditing.

4. **We store information in DOC-approved repositories.**

All work-related information must be stored in a DOC-approved system, not in personal systems accessible only to the individual concerned, such as U: drives. The document management system will be used for all official unstructured information unless an approved business information system is used instead.

Information stored in DOC-approved systems must be available for future use by those who need it. Information in these trusted systems can be more readily packaged and/or released to partners and stakeholders for re-use.

5. **We champion an open and collaborative information culture both with our people and our partners.**

DOC's operating model supports open collaboration with other government agencies, private enterprise and the public. This includes shifting existing internal information to more open, external facing systems where appropriate.

The information we manage is of significant interest and value to the public. Our commitment is to share non-sensitive information and to be responsive to public requests. We achieve this by implementing two key rules:

1. Non-personal information (including data) is open by default to DOC people unless valid business reasons apply for restriction.
2. Non-personal information (including data) is released proactively for public access and unrestricted use as per NZGOAL and Creative Commons licensing unless there are identified grounds for refusal or limitation. It is discoverable and accessible and released online via recognised channels.

6. **We protect personal information to ensure compliance with the provisions of the Privacy Act 2020.**

DOC collects and uses personal information from people for employment purposes and as part of its day-to-day operations. The Department protects personal information relating to staff, contractors, volunteers and/or members of the public to ensure compliance with the provisions of the Privacy Act 2020.

Personal information is a subset of official information. Personal information means information about an identifiable, living person. Information in its ordinary dictionary meaning is that which informs, instructs, tells or makes aware. Accordingly, personal information is anything which instructs, tells or makes (another person) aware about an identifiable individual.

In the context of information management, privacy is concerned with how personal information is collected and handled by government. This extends to an individual's right to privacy and to access and amend their personal information.

All personal information, e.g., for staff, volunteers and the public, will have the same privacy protections, and must be appropriately protected and classified. Business systems will conform to privacy and identity standards.

For more information see the Privacy Policy (doc-5568567) and Managing Personal File (HR) and Payroll Processing Document Digitally SOP (doc-3196921). A list of documents related to this policy can be found in Section 4.

7. We protect commercial and sensitive information from unauthorised or inappropriate access or release

DOC creates, collects and uses commercial and other sensitive information and must ensure compliance with government standards for information security.

We comply with the following security principles:

- Confidentiality – ensuring that information is only accessed by authorised persons
- Availability – ensuring that information and services are accessible when required by authorised users, and
- Integrity – ensuring that information is not altered without authorisation.

Commercial and other classified data, information and metadata must be appropriately protected and classified.

Information received should be stored in accordance with the security classification assigned to it by the third party. The security obligations set by the third party should be considered when assessing information for release, for example Official Information requests.

All business systems must be developed in accordance with government security requirements, including security and accreditation certification and risk assessment requirements.

For more information see the Guide to Information Security Classifications (docdm-1417587) and/or contact Information Systems and Services.

8. **We retain all rights in intellectual property created by DOC employees and independent contractors/suppliers generated in the course of their employment or engagement with DOC. Intellectual property is only assignable with the express written agreement of DOC.**

All intellectual property produced by DOC staff in the course of their employment is owned by the Crown, with DOC the custodian, following the terms of their employment or otherwise created under the direction or control of DOC.

DOC often hires external parties to supply goods and services. Whenever DOC pays for work, DOC should own the intellectual property that is generated and should not sign away its rights in the contract. Contracts should, however, make clear what right the contractor has to use DOC's intellectual property. In cases where a third party owns the intellectual property DOC will respect the limitations on the use of that information (subject to its legal obligations including those under the Official Information Act).

When making decisions in relation to the commercialisation of intellectual property, for example in a partnership agreement, staff must seek appropriate legal advice.

DOC shall consider intellectual property and copyright ownership when buying or creating information and information systems, and in using or storing information created by others.

DOC information is generally covered by Crown Copyright unless the contributor or creator agrees to an alternative arrangement. Information covered by Crown Copyright is eligible to be released under Creative Commons licence for unlimited use (CC-BY) unless there are valid grounds for restriction.

9. **We comply with legislation, this information management policy, standard operating procedures and guidelines when carrying out DOC activities**

DOC will ensure that the collection, use, preservation, and disposal of information meet statutory, legal and administrative requirements. This includes compliance with the Public Records Act 2005, the Privacy Act 1993, the Official Information Act 1982, whole-of-government guidelines on the management of government-held information, data management standards and exchange protocols, and the standards issued by Archives New Zealand.

We handle and use information, whether created or received, in line with all relevant policies and procedures.

We monitor and report on compliance as part of standard business assurance and risk practices.

4. Related documents

For more information and related documents see the DOC Intranet Procedures and Guides. Key related documents are listed below. These documents will be amended, updated and consolidated over time. For that reason, it is important to refer to the latest version of this policy for the most recent list of Related Documents:

Framework

Security and Privacy Framework (Draft) (doc-5577365)

Policies

1. Information Security Policy (docDM-1494047)
2. Draft Intranet Policy (docDM-532638)
3. Web Policy (docDM-1101903)
4. Spatial Metadata Policy (docDM-809521)
5. Spatial Data Stewardship Policy (docDM-809514)
6. Risk Management Policy (doc-2224884)
7. Official Information and Proactive Release Policy (doc-3189349)
8. Privacy Policy (doc-5568567)
9. Information Gathering for Compliance, Law Enforcement and Security Policy (doc-5960847)

SOPs

1. Information Management SOP (doc-2527619)
2. Storage of Records SOP (docdm-640994)
3. Use of DOC Technology SOP (doc-2182996)
4. Official Information Act and Proactive Release One Page SOP (doc-3190309)
5. DOC Images Database SOP (docDM-217950)
6. Spatial Data Management SOP (docDM-833004)
7. Managing Personal File (HR) and Payroll Processing Document Digitally SOP (doc-3196921)
8. Security, Identification, Prevention and Response SOP (Draft) (doc-5990613)

Guidelines and other related material

- Guide to Information Security Classifications (docdm-1417587)
- Access Control Model for DOC Information Assets (docdm-1478190)
- DOC disposal schedule DA538 (docdm-723436)
- Copyright Issues Guideline (doc-5602589)
- Using Low Risk Cloud Application or Services Guidelines (DOC-5403603)

5. Document Information

5.1 Version history

Version	Date	Author	Summary of Changes
0.1	04/02/2014	Andrea Grover	First draft
0.2	05/05/2014	Andrea Grover	Feedback from Louise Mercer; elaborating policy statements
0.3	23/05/14	Andrea Grover	Incorporating feedback from ISS, Legal, and adding IP policy statements
1.0	01/09/2014	Andrea Grover	Feedback from Allan Ross and Ashley Mudford
1.1	14/10/2014	Andrea Grover	Feedback from Jan Hayes; endorsement by Security Committee
1.2	26/07/2019	William Brockelsby	Review conducted pending feedback.
1.3	06/08/2019	William Brockelsby	Feedback incorporated from Info Security, Government Services and Security team.

5.2 Approval history

Previously approved:

Policy - Information Management SIGNED October 2014 (docDM-1507582)
Information Management Policy Memo to Security Committee (docDM-1485653)
Information Management Policy Memo to DDG (docDM-1484270)

5.3 Distribution and Consultation

Name	Title	Date of Issue	Version
Louise Mercer, Claire Ashcroft, Keri Ford, Shane Jackson, William Brockelsby	Information Services Team	12/3/14	0.1
Gavin Walker	ICT Strategy and Architecture Services Manager	8/5/14	0.2

Name	Title	Date of Issue	Version
Sharon Alderson	Shared Services System Manager	15/5/14, 25/8/14	0.2 0.3
Jonathan Dreadon	Database Administrator	23/5/14	0.3
Jonathan Berry	Security Consultant, Aura Security	25/5/14	0.3
Lucy Hoffman, Tina Weir, Dylan Nyika, Haisley Simpson, Rachel Soppit	ECM Project team	29/5/14	0.3
Olivia Eaton, Tara Allardyce	Legal	3/6/14	0.3
Felicity Lawrence, Allan Ross, Anaru Luke, Hilary Aikman, Martin Kessick, Ashley Mudford, Sue Reed, Amy Allan, Benno Kappers, Jonty Somers, Mike Sheridan, Ann Thompson, Pamela Minnoch; Shannan Mortimer; Matiu Mataira; Dave Jane; Wendy Evans; Gary Flux; Jack Mace; Suresh Senadeera, Martyn Bayly	CIE and ECM Project Board and Steering Committee, and ECM Business Reference Group	26/8/14	1.0
Jan Hayes	Privacy Officer	5/9/14	1.0
Carl McGuinness, Christeen Mackenzie, Jan Hayes, Geoff Owen, Shagen Ganason, Peter Noble	Security Committee	13/10/14	1.0
Andrew Martin	Government Services	30/07/19	1.2
Shane Jackson, Kathryn Watson	Security Team	01/08/19	1.2
Henare Royal, Shem Watson	Information Security Team	30/07/19	1.2

6. Appendix I - Terms and Definitions

Commercialisation

Commercialisation refers to the right to grant licences to use intellectual property.

Copyright

Copyright is a set of exclusive property rights given to owners in relation to their creations, e.g., Crown copyright.

Disposal

The range of processes associated with implementing records retention, destruction or transfer decisions which are documented in a disposal authority. Section 4 of the Public Records Act 2005 outlines the possible types of disposals as: the transfer of control of a record; or the sale, alteration, destruction, or discharge of a record.

Disposal authority

The legal document that authorises the disposal of DOC's records, approved by the Chief Archivist, Department of Internal Affairs.

Information

In the broad context of this policy, the word information includes structured data and spatial information, unstructured information (such as documents, emails, spreadsheets), sound and video recordings, images, and associated metadata.

Information integrity

The accuracy, completeness, and validity of information. Integrity also means that an information asset has not been modified without authorisation and can be trusted.

Information life cycle

The life cycle of information management encompasses the following: planning; the collection, creation, and capture of information; its organisation, use and dissemination; its maintenance, protection, and preservation; and its disposal.

Information management (IM)

Information management is the activities and the organisation structure required to control an enterprise's information assets, digital and physical. These may be acquired by one or many disparate sources and should be managed in a way that optimises access and use by all who have a share in that information or a right to that information. IM creates value and assures compliance with rules and regulations.

Information resource owner/custodian/maintainer

Accountabilities for each role are defined in the Information Governance Framework (in development).

Information system owner/custodian/maintainer

Accountabilities for each role are defined in the Information Governance Framework (in development).

Information systems

Systems that create, keep, and manage information (records) and metadata (information about records), or manage metadata only while the records are held elsewhere.

Examples include finance systems, personnel systems, and core business systems, such as AMIS (Asset Management Information System).

Intellectual property

Intellectual property in the case of this policy is the output of contracts or agreements and includes copyright, trademarks, registered designs, patents, circuit layouts, data and databases, know-how and all other rights conferred under statute, common law or equity in relation to inventions. It also includes contracts or agreements fully or partly funded by DOC as well as intellectual property that arises through employment.

Official information

Official information as defined in section 2 of the Official Information Act is any information held by a department or organisation (as defined, "organisation" includes most agencies in the wider state sector) or a Minister of the Crown in his or her official capacity.

Open data and information

Open data is the idea that data and information held by government that is taxpayer funded bodies should be freely available to everyone to use and republish as they wish. This is without restrictions from copyright, patents or other mechanisms of control.

Personal information

Personal information is a subset of official information. Personal information means information about an identifiable, living person. Information in its ordinary dictionary meaning is that which informs, instructs, tells or makes aware (see Commissioner of Police v Ombudsman [1988] 1 NZLR 385). Accordingly, personal information is anything which instructs, tells or makes (another person) aware about an identifiable individual.