16 May 2022

[redacted]

Kia ora [redacted]

Your Official Information Act request, reference: GOV-018052

Thank you for your request to [redacted] on 13 April 2022, asking for the following information under the Official Information Act 1982 (the Act):

- *a copy of ACC client information record keeping policy/document*

ACC is guided by several pieces of legislation when determining how client information is kept
This legislation includes the Privacy Act 1993, the Health Act 1956 and related Health Information Privacy Code 1994, the Public Records Act 2005, and the Accident Compensation Act 2001 (the AC Act). These Acts and the Code can be viewed online via www.legislation.govt.nz.

ACC complies with Archives New Zealand's 'Authority to retain public records in electronic form only', which grants approval for public offices to retain public records in an electronic form only. ACC's full disposal authority relevant to the claims process (DA442) is available publicly online, and can be viewed on the New Zealand Archives website at https://collections.archives.govt.nz/web/arena/search#/item/aims-archive/DA442/da442

ACC policy documents
ACC has created a number of policy and standards documents relevant to your request. We have provided with this letter the following:

- Information management policy
- Information management standards

As this response may be of interest to other members of the public
ACC may proactively release a copy of this response on ACC's website in future. All requester data, including your name and contact details, will be removed prior to release if so. The released response will be made available www.acc.co.nz/resources/#/category/12.

If you're concerned about this response, please get in touch
You can email me at GovernmentServices@acc.co.nz. You can also complain the Ombudsman via info@ombudsman.parliament.nz or by phoning 0800 802 602. Information about how to make a complaint is available at www.ombudsman.parliament.nz

Ngā mihi,

Sara Freitag
Acting Manager Official Information Act Services
Government Engagement & Support

Information Management Policy

POLICY NUMBER	5.0.0
TOPIC	Information Management
OWNER	Chief Technology and Innovation Officer
BUSINESS GROUP	Technology and Innovation
AUTHOR	[redacted] Manager Information Frameworks and Assurance
DATE APPROVED	25th March 2021
APPROVER	ACC Board
NEXT REVIEW DATE	25th March 2023

1 Policy Statement

As a Crown entity, ACC holds information on behalf of the peoples of New Zealand. The information held is related to the duties ACC is responsible for in accordance with the Accident Compensation Act 2001. These duties relate to ACC's major functions: injury prevention, rehabilitation, setting and collection of levies; assessing and paying claims and investment management. This constitutes the primary use of this information.

ACC holds a unique set of information that has significant value, not only for NZ but internationally.

Information is the only enduring asset that ACC holds and should be treated as such. This aligns with the Māori data sovereignty principle of viewing this as a treasure (Māori: taonga). In recognition of the obligations under the Treaty of Waitangi (Māori: Te Tiriti o Waitangi).

To extract the maximum value of this resource, the secondary use of information must be actively promoted and supported for secondary use which includes:

1. Identifying opportunities for injury prevention initiatives
2. Improving customer service by improving outcomes, efficiencies and effectiveness
3. Sharing information for external use in support of insights and research related to accidents, injuries, treatments
4. Ensuring information is available and representative of the peoples of NZ, including Māori, minorities and marginalised groups to facilitate and support these communities
5. Partnering with representative groups to promote, support and advise on the appropriate use of ACC information

To ensure that information is fit for purpose, ACC is committed to establishing, maintaining and monitoring modern information management practices to ensure they meet both primary and secondary needs. This includes meeting legal compliance, accountability requirements and stakeholder expectations.

2 Alignment with Government

As a crown entity, ACC is expected to conform and adhere to government policies and practices related to information management as specified by appointed officials. In addition, as ACC is viewed as part of the health and disability sector, we also need to conform to specific sector requirements.

These are described in more detail in Appendix 3.3.

3 Policy Objective

We are committed to establishing modern information governance and management practices that meet our customer expectations, ongoing business needs, security, privacy and legal requirements including:

- Capturing only relevant, and applicable, information
- Securing and storing our information appropriately, recognising that we are a customer-centric organisation
- Documenting actions and decisions as required for legislative, governance and legal reasons
- Managing information as a strategic corporate asset

All our information management practices are delivered in accordance with the principles set out in this policy, and its supporting standards and procedures. ACC is committed to continuous improvement in our corporate information policies, processes and standards.

4 Policy Scope

This policy is intended for all our people, including our board members, consultants, contractors and organisations (including vendors and other third parties) engaged to undertake work on behalf of ACC.

This policy covers all information that we create, ingest, receive, manage, store and share as part of conducting our business.

5 Policy Principles

Our Information Management principles are the foundations for the way that we use information within ACC.

Our information must be managed, secured, and maintained as per our Information Management principles. We must also comply with all relevant legislation and government standards.

Personal and health information makes up a significant part of our information.

The ACC Privacy Policy sets out additional requirements for storage and use of this information and must be read in conjunction with this policy when dealing with personal and health information.

4.1 Our Information is a strategic asset and we actively manage it

Our Information Governance Group (IGG) must ensure that our information assets are professionally managed. This supports our objectives, principles, and the obligations set out in the IGG Terms of Reference.

Active management means:

- We have senior leaders setting strategy, and making sure we are sufficiently resourced to manage our information assets in a consistent, integrated way
- We use our information assets to deliver insights and enable smarter business decisions
- Our change management processes consider, and actively manage, information management risks at both design and implementation stages
- All staff must ensure the information they use is accurate and fit for purpose.

4.2 Our information has clear ownership

All our business-critical information assets must be assigned a Steward (business owner) by subject area, and at least one Custodian (information caretaker) as per our Information Stewards and Custodians Standard.

Stewards and Custodians must ensure that our information is cared for (actively managed) throughout its lifetime. They must also ensure that information access is only granted where needed for the particular role and is disposed of (destroyed or archived) at the end of its lifetime in accordance with our approved disposal authorities.

Clear ownership means:

- We must ensure all staff understand and are able to manage our information within their role
- We must ensure our information is fit for purpose and aligned with the strategic direction set by the Information Governance Group (IGG)
- All our key information assets have defined business owners (Stewards) with agreed delegation of authority
- Stewards are responsible for making decisions related to their assigned information assets
- Custodians support Stewards by ensuring the information they are responsible for is fit for purpose, meets primary and secondary needs, is readily accessible by those that need it and is trustworthy.

4.3 We make our Information fit for purpose

We must manage information to ensure it is fit for purpose, consistently described, trustworthy and meets all needs. We all have a responsibility to conform with required quality requirements by, taking ownership of the information in our care.

Fit for purpose means:

- We protect the value of information against misuse, misinterpretation, unnecessary access restrictions or failure to maintain its quality

- Active stewardship of our information ensures that it remains fit for purpose. To do so it must be accessible and complete, well described so that it is understood, and can be used with confidence in support of both internal and external:
    - Evidence-based decision making
    - Research
    - Reporting
    - Analytics, and
    - Data Mining
- Information must be periodically reviewed to ensure compliance with all relevant legislation and standards as shown Appendix 1
- Good archiving and disposal practices ensure our information is compliant with the requirements of the Public Records Act 2005.

4.4 We make our information Accessible, yet Secure

We enable the sharing of our information to make best use of the information assets we hold and promote public and government confidence in our information.

We protect the ethical use, confidentiality, integrity and accessibility of information, through active management and adherence to the principles of our Privacy Policy, Information Security Policy and Standards.

Accessible, yet Secure means:

- We comply with our obligations under the New Zealand Open Data Charter
- We enable appropriate, and prevent inappropriate, access and reuse of our data assets
- We improve the effectiveness and efficiency of work by allowing people to discover, use, and share information
- We enable better, evidence based, decision making
- When we share information externally, we ensure appropriate approvals and/or formal agreements are in place, and where relevant will seek advice from the ACC Ethics Panel.
- We minimise the risk of uncontrolled release of our information, and the resulting harm arising to our clients, business and personnel
- The privacy and confidentiality expectations of all stakeholders are met.

4.5 Our Information is simplified by design, and we standardise it for reuse

Our information architecture and Enterprise Information Management (EIM) Strategy provides the big picture of how our information hangs together. It is designed to provide visibility, promote reuse, integration and efficiency.

Simplified and standardised information means:

- A well-managed information architecture that allows people to discover, use and share information
- It provides a lean, agile information environment that results in more efficient use of information assets, and promotes cost effective business outcomes
- The concept of ‘create once, use many times’ meaning duplication and reinvention is minimised, which allows us to significantly reduce the cost and effort in creating and managing duplicate information

4.6 We all share a common understanding of how we work

All our people and contractors understand their responsibilities as set out in this policy and its supporting policies, standards, procedures and guidelines.

We all work to deliver our information management goals and best practice outcomes for all our customers.

6 Accountabilities

The ACC Board is responsible for ensuring ACC's compliance with the directions to support an all of government approach including the current direction on Information and Communication Technologies (ICT).

To support the Board, each Executive member is accountable for understanding and compliance with this policy and its supporting policies and standards within their business area.

This includes effective implementation of information management practices across our work activities to ensure the principles of this policy are understood and that the relevant legislation and standards are complied with.

The Chief Technology and Innovation Officer (CTIO) is accountable for the operational implementation and monitoring of this policy.

7 Responsibilities

All employees are collectively responsible for Information Management.

Role	Responsibilities
Employees including contractors, consultants and temporary staff engaged by ACC	Must read and understand the principles of this policy. Adhere to any reasonable instruction that is given to comply with legislation and best practice. Complete information management training as required so that they: • Comply with our documented information management policies and procedures • Can create full and accurate records of activities, transactions, and decisions carried out during daily business activity • Ensure that such records are maintained by being captured into the appropriate information management system • All Information assets are classified in accordance with our Information Security Policy • When creating or amending information, they are responsible for its quality • Maintain best privacy practices in line with the Privacy Policy, including managing information safely and reporting breaches.
People Managers	• Ensuring these principles are understood • Creating an environment where appropriate information management

	practices are present in team thinking, discussion, and decision-making • Develop skills and knowledge to support and facilitate staff in information management best practices • They communicate expectations with staff, monitor compliance, and ensure accurate reporting.
The Information Governance Group (IGG)	• Operates with appropriate delegation of responsibility to oversee and govern the information management function and is accountable for Enterprise Information Management Strategy • IGG's focus is to ensure that our information is actively managed throughout each stage of its lifecycle as a strategic business asset • IGG's roles and responsibilities are set out in by the IGG Terms of Reference Document • Appoints required roles and delegates appropriate authority to ensure they can operate effectively in their information role and duties in conjunction with their manager.
Security and Privacy advisory group (SPAG)	• Responsible for advising the IGG on the outcomes of the Information security roadmap and the Privacy maturity roadmap.
Content and Records Advisory group (CRAG)	• Responsible for the advising the IGG on the outcomes of the content and records (C&R) roadmap and ongoing maintenance of the Information Management Policy.
Chief Technology and Innovation Officer (CTIO)	• Directs and leads our information management initiatives • Holds the positions of Chief Data Officer (CDO) and Chief Information Officer (CIO) as defined in relevant NZ legislation and policy • Ensures that our Information is managed and updated, disposed of, or archived in a timely fashion in accordance with our approved disposal authorities • Responsible for ensuring Information Stewards and Custodians are trained in the skills needed for their role in our information management • Provides Senior leadership representation as chair of the IGG.
Ethics Panel	• Advises on any research requests for personally identifiable or potentially personally identifiable ACC data
The Head of Enterprise Data, Information and Security (EDIS) on behalf of the CTIO.	• Responsible for developing and implementing information systems and governance processes to ensure operational measures and monitoring is in place to support this policy • Ensures all staff are aware of the policy and that the appropriate structures and roles are put in place with the right level of training and guidance to operate at the required level • Support IM governance groups and roles to enable them to fulfil their obligations and responsibilities.
Information Stewards	• Accountable and responsible for implementing operational policy, business value, scope, definitions, rules, standards, structure, content, use and disposal for information and data under their responsibility • Make decisions on strategic needs as well as the collaborative needs and external partners and providers • Ensure that Custodians are supported by management • Ensure that all our information assets for which they are responsible are defined and maintained in the Information Asset Register.

Information Custodians	• An inclusive role that accepts one or more delegated information and data custodianship activities on behalf of the Information Steward • Manage and support the day to day operation and use of information • Custodians use our processes and information management standards to make day to day decisions about information governance.
Executive	• Empower and direct our information management maturity and roadmap goals with appropriate delegation of authority • Provide executive support and oversight of all our information management activity.
Board	• Board is responsible for ensuring the organisation is aware of the need to look after our information through high-quality monitoring and information management practices.

8 Monitoring and oversight

The monitoring and oversight of privacy follows the five lines of assurance model (5LOA).

LOA:	Role	Monitoring & Oversight
1st Line	Employees and People Managers	• All people managers monitor the completion of information management modules and training • All employees remain alert to potential breaches of the Policy and report potential and actual breaches to their manager • All people managers ensure that (i) breaches brought to their attention are documented, (ii) notification of the breach is provided to the owner of the Policy within five days of the breach occurring • From time to time we deliberately take actions contrary to a policy's provisions (corporate policy exceptions). When people managers are responsible for a corporate policy exception, the people managers ensure that the exceptions are agreed either using the process in the Policy or by agreement in writing from the Policy owner.
	Group Risk and Compliance Manager and/or Advisor	• Supports employees/groups to determine whether events constitute actual breaches of the Policy • Escalates breaches to the Group's Leadership Team and Chief when appropriate. • Updates risk registers as required.
	Policy Owner	• The Policy Owner ensures that the Group (and other parts of ACC if applicable) respond appropriately to Policy breaches and requests for exceptions.
2nd Line	Enterprise Risk Team	• Performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches • Reports to the Executive and the Board on the outcomes of such activities.
	Enterprise Data Information and Security (EDIS) team	• Provide oversight of all information management aspects in this policy and subject matter expertise to staff and management when required • Regularly review and report to ensure the intention of the policy is being honoured • Carry out periodic audit and assurance activities on information

LOA:	Role	Monitoring & Oversight
		management practices along with the Enterprise Risk and the Privacy team • Supports employees to determine whether events constitute actual breaches of the Policy • Escalates breaches to the Group's Leadership Team and Chief when appropriate • Supports the oversight of our information management practices and decision making via the Information Governance Group and sub governance groups.
3rd Line	Internal Audit (and external providers)	• Performs periodic audit activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches • Reports to the Executive and the Board on the outcomes of such activities.
4th Line	Executive	• Ensures each Group has sufficient emphasis on risk management and meeting compliance obligations • Ensures effective processes and monitoring are in place to meet compliance obligations for the Policy • Acts in an appropriate and timely manner in response to reports received that alert the Executive to opportunities to improve Policy compliance activities.
5th Line	Board	• Responsible for approving any material changes to the level 1 Policies, including text related to monitoring and oversight of compliance with the Policy • Acts in an appropriate and timely manner in response to reports received that alert the Board to opportunities to improve Policy compliance activities.

This policy will be formally reviewed every 2 years. We acknowledge the changing information management landscape may require policy changes and updates more regularly where technology or best practice changes.

Where practicable these changes will be managed through standards and best practice guidelines.

9 Breaches of Policy

Complying with all policies and procedures is a requirement outlined in the Code of Conduct. Behaviour or actions that are investigated and found to be in breach of the Code of Conduct may result in disciplinary action. Refer to Code of Conduct for further information.

10 Contacts

The Information Management team can be contacted in relation to any queries regarding this policy.

11 Definitions

Our Information	All data and information produced by ACC, and all information under our care regardless of to whom it belongs, or where it originated.
Custodian and Steward	As defined in the Information Stewards and Custodians Standard.
Information	All recorded forms of data, knowledge, facts, intentions, opinions, or analysis, irrespective of the content, or the medium through which it is communicated or stored. Information may be contained in a variety of media, for example: printed documents, handwritten notes, diaries, maps, spatial data, photographic data, images, videos, electronic databases, electronic documents, emails, web pages, voice mail and audio records.
Information Architecture	The structured organisation of information and its relationship to business processes and systems. This excludes technical system design.
Information management	The creation and maintenance of complete, accurate and reliable evidence of business transactions in the form of recorded information.
Information Repository	An environment (either electronic or physical) where information is registered, stored, and managed.
Records	A record is any documentation or evidence of business activity and decisions, regardless of format.
Retention and Disposal Schedule	A systematic listing of the records created by an organisation, which informs their lifecycle management from creation to disposal.

12 References

This Information Management Policy is supported by the Information Management Governance structure in Appendix 2. Supporting sub policies, standards, procedures and guidelines are outlined in Appendix 1.

The legislative requirements that our information assets must meet are listed under Appendix 2.

13 Version Control

Version	Date	Material change reason	Who
0.1	13/07/20	Initial Draft	[Out of Scope]
0.2	26/7/20	EDIS review completed	[redacted]
0.3	21/9/20	Feedback from reviews added	[redacted]
0.4	12/10/20	Final preparation for GG's	[redacted]
0.5	16/04/21	Amendments for Board (minor)	[redacted]

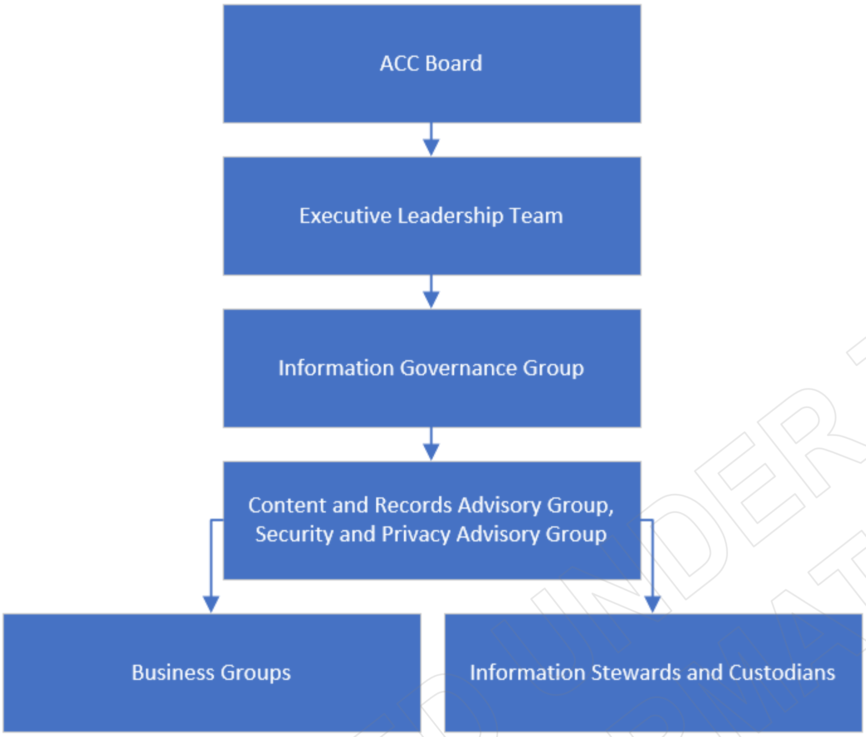
14 Appendices

Please note the following appendices are informative only they are accurate as of the time of publication and should not be considered an authoritative list or source given the changing policy and legislative landscape.

13.1 Appendix 1: Supporting Documentation

Subordinate Policies and Standards
Information Security Policy (Tier 2) Privacy Policy (Tier 2) Cloud Computing Policy (Tier 2) Use of the Internet Policy (Tier 3) Email and Instant Messaging Policy (Tier 3) Information Management Standards (omnibus document) Information Security Standards (omnibus document) Stewards and Custodians Standard Cloud Collaboration Standard
Associated Technology Policy and Standards
Telephony Policy (Tier 3) BYOD Policy (Tier 3) Modern Device Standards Vendor Device Standard
Related Acts, Standards and Codes
Accident Compensation Act 2001 Privacy Act 2020 Public Service Act 2020 Health Information Privacy Code 1994 Public Records Act 2005 Health Act 1956 New Zealand Public Health & Disability Act 2000 Tax Administration Act 1994 Copyright Act 1994 Official Information Act 1982 Contract and Commercial Law Act 2017 Evidence Act 2006 Financial Reporting Act 1993 Public Finance Act 1989 and Public Finance Amendment Act 2004 Resource Management Act 1991 and Resource Management Amendment Act 2005 State-Owned Enterprises Act 1986 Health and Safety in Employment Act 1992 New Zealand Public Health & Disability Act 2000 Data Content Standards (data.govt.nz)

3.2 Appendix 2 – Information Governance Boards


ACC Board
Executive Leadership Team
Information Governance Group
Content and Records Advisory Group, Security and Privacy Advisory Group
Business Groups
Information Stewards and Custodians

3.3 Appendix 3 – Alignment with Government

As a crown entity, ACC is expected to conform and adhere to government policies and practices related to information management as specified by appointed officials. In addition, as ACC is viewed as part of the health & disability sector, we also need to conform to specific sector requirements.

All-of-Government Official Functions (www.digital.govt.nz)

The NZ Government has established functional leads who are charged with developing and improving designated areas across government. The roles are delegated to specific chief executives by the Public Service Commissioner.

The roles are:

1. Government Chief Digital Officer (GCDO) oversees the development and management of digital for the state sector. The GCDO is responsible for:

   - setting digital policy and standards
   - improving investments
   - establishing and managing services
   - developing capability
   - system assurance (assuring digital government outcomes)

2. Government Chief Data Steward (GCDS) supports the use of data as a resource across government to help deliver better services to New Zealanders. The GCDS is the government functional lead for data and ensures that government agencies have the capability and right skills to maximise the value of data. This is achieved through setting data standards and establishing common capabilities, developing data policy and strategy, and planning across the state sector. Focus has been on:

   - Co-developing a Data Stewardship Framework to enable agencies to manage data as a strategic asset and benchmark their data maturity
   - Leading the government's commitment to accelerate the release of open data, including the implementation of the International Open Data Charter
   - Developing data governance across the system through evolving approaches to data ethics and Māori data governance.

3. Government Chief Information Security Officer (GCISO) role strengthens Government decision making around Information Security and supports a system-wide uplift in security practice. The GCISO is the government functional lead for information security. The GCISO's work includes:

   - coordinating the government's approach to information security
   - identifying systemic risks and vulnerabilities

- improving coordination between ICT operations and security roles, particularly around the digital government agenda

- establishing minimum information security standards and expectations

- improving support to agencies managing complex information security challenges.

4. Government Chief Privacy Officer (GCPO) leads an all-of-government approach to privacy to raise public sector privacy maturity and capability. The role sits within the Digital Public Service branch of the Department of Internal Affairs, reporting to the Government Chief Digital Officer. The GCPO is the practice lead for privacy and supports government agencies to meet their privacy responsibilities and improve their privacy practices. The GCPO is responsible for:

   - providing leadership by setting the vision for privacy across government

   - building capability by supporting agencies to lift their capability to meet their privacy responsibilities

   - providing assurance on public sector privacy performance

   - engaging with the Office of the Privacy Commissioner and New Zealanders about privacy.

Statistics NZ (data.govt.nz)

Statistics NZ (as GCDO) is responsible for overseeing official government statistics. Tier 1 statistics are New Zealand's most important statistics, and are essential to help the Government, business, and members of the public to make informed decisions and monitor the state and progress of New Zealand. Tier 1 statistics describe New Zealand's economy, environment, population, society, culture, international relations, and civil and political rights. Tier 1 statistics are also used by a range of organisations to develop new services and products.

One of the 162 Tier 1 statistics is the incidence of injuries annually produced by Statistics NZ using ACC and MoH data.

As ACC supplies data to produce a Tier 1 statistic, ACC must ensure that the Tier 1 statistic is of good quality and has integrity. Producers of Tier 1 statistics must adhere to the Principles and protocols for producers of Tier 1 statistics. Tier 1 statistics must be presented impartially and clearly without judgement and must be managed in such a way to ensure that the statistics are free from undue influence.

Ministry of Health

The Health Information Standards Organisation (HISO) with the Ministry of Health supports and promotes the development and adoption of fit-for-purpose health information standards for the New Zealand health system. HISO works with health providers and shared services organisations, clinical and consumer groups, software vendors and industry bodies, the academic community, the wider government sector and other standards development organisations. It also supports *He Korowai Oranga: Māori Health Strategy* for the effective delivery of health and disability services to Māori and represent the interests of all New Zealanders as consumers of health services and stakeholders in the health system.

HISO links with the international standards community through Standards NZ, SNOMED International for SNOMED CT, and through HL7 New Zealand for HL7 standards.

As a participant in the Health & Disability Sector, ACC is expected to adhere and support the standards produced by HISO.

ACC

PREVENTION. CARE. RECOVERY.

Te Kaporeihana Āwhina Hunga Whara

Information Management

STANDARDS

Business Group	Technology & Transformation
Author	[Out of Scope]
Date	May 2019
Version	0.91

Table of Contents

Contents

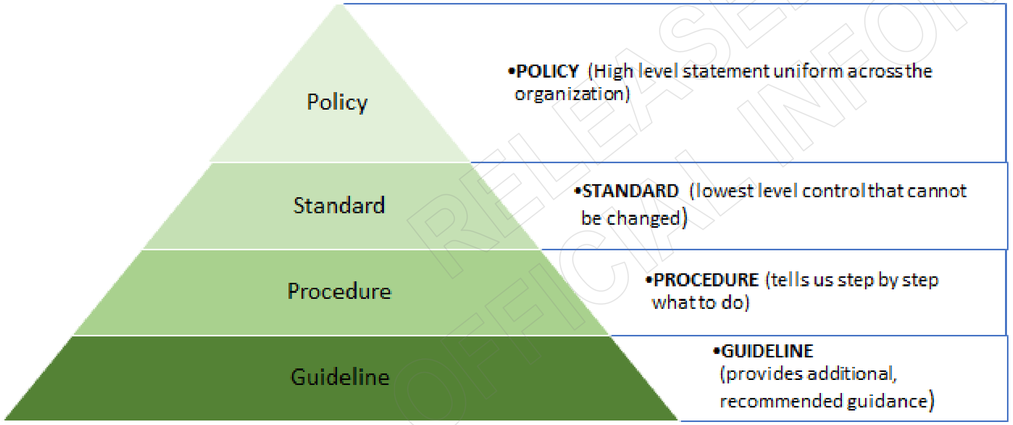
1 Introduction

1.1 Purpose

The purpose of this document is to collate the set of minimum standards that must be applied in relation to information management at ACC.

1.2 How to apply standards

This standard has been developed in line with the Corporate Policy Governance Model's definition of Policies, Standards, Procedures and Guidelines as reflected in the diagram below.



- **POLICY** (High level statement uniform across the organization)
- **STANDARD** (lowest level control that cannot be changed)
- **PROCEDURE** (tells us step by step what to do)
- **GUIDELINE** (provides additional, recommended guidance)

1.3 Key relevant documents

Include the following: *(in hierarchical order)*

- Legislation
- Policies
- Procedures and standards
- Guidelines
- Forms
- Other useful resources

Where the same type of document appears, they are listed alphabetically.

1.4 Definitions

Term	Definition
Record	ISO 30300:2011 defines a record as "Physical or digital evidence of a business transaction, activity or decision which fulfils or supports a core function of business".
Authoritative source	A trusted record viewed as a reliable source of information because it can be proved that it has not been tampered with.
Core business system	An authoritative source (a location, technical system, or repository) of data or information within ACC.
Dissemination	To disperse, spread, or share information internally or externally.
Immutable record	A record which is neither capable of nor susceptible to change; unchangeable; unalterable.

Information and records system/ information repository	A system which captures, manages and provides access to records over time e.g. Oracle Financials, Payroll System, Contract Management System, Corporate Shared Drives, etc.
Information lifecycle	When properly managed, every piece of information that is created progresses through a life cycle. The life cycle is divided into five stages: 1. Create/Collect 2. Organise 3. Use and Share 4. Maintain and Protect 5. Retain and Dispose
Metadata	Information about a piece of information or data which describes the characteristics and attributes of that piece of information or data.
Retention and disposal schedules/ Disposal Authority for ACC records	Retention and disposal schedules set the length of time that ACC keeps certain types of records and the processes for disposing of records at the end of the retention period. The schedules are available on The Sauce at http://thesauce/how-to/knowledge-management/recordkeeping/applying-our-disposal-authorities/index.htm.
Shared Drive	At ACC, the phrase 'Shared Drive' refers to the I:\ Drive, J:\ Drive or any ACC Cloud solution where information is created, stored, searched and shared e.g. OneDrive for Business or Document Store/SharePoint
Taxonomy	A system of organising information into logical groupings or classes and sub-classes e.g. Folder Structure.

1.5 Roles and responsibilities

ACC has adopted the 5 Lines of Assurance (5LoA) model for enterprise risk management and assurance. This model defines the high-level expectations for the Board, Executive, managers, specialist functions and independent assurance providers in identifying, assessing, deciding and assuring about risk in ACC.

The following table demonstrates how the 5LoA model maps to ACC's roles and responsibilities to establish accountability.

Role	Responsibilities

1st Line
All Staff
	• ACC has a legal obligation to comply with the Information Management requirements of the following acts:
	  ◦ Public Records Act 2005
	  ◦ Accident Compensation Act 2001
	  ◦ Privacy Act 1993
	  ◦ Copyright Act 1994
	• Staff wilfully and knowingly acting in a manner that breaches these obligations are in breach of the ACC Code of Conduct and may be subject to disciplinary actions

	• All ACC Staff must create full and accurate records of their daily business activity. This includes recording activities, transactions and decisions made when dealing with clients, providers and staff
	• People managers will ensure their staff: ◦ are aware of ACC's Information Management Policies and associated procedures ◦ follow the above policies and procedures
2nd Line	• The Information Frameworks and Assurance Team will support ACC staff by providing a framework to systematically manage ACC information and records

Specialist functions including RCO	- The Information and Digital Tools Team will support ACC staff by providing operational support for information systems access requests
	- People managers and project managers will ensure their staff and teams comply with the requirements of the Copyright Act 1994.
3rd Line **Assurance Services**	- Enterprise Data, Information and Security teams will conduct periodic audits and support investigations as required in collaboration with RCO and Assurance.
	- Enterprise Data, Information and Security teams, in collaboration with RCO and Assurance, will conduct periodic audits and support investigations into misuse as required.
4th Line **CEO and Chiefs**	- The Chief Technology and Transformation Officer will place organisational controls in support of these standards
5th line **ACC Board**	- The ACC Board has overall responsibility for implementing effective risk management. They will review and assesses CEO's and Chiefs' reporting and management of objectives

2 Standards subject specific content

2.1 Records management Standard

Many ACC documents are also records. A 'record' is defined by the ISO[1] as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business". This can include:

[1] **Source:** ISO 30300:2011 *Information and documentation — Management systems for records — Fundamentals and vocabulary*. Found online 4 February 2019 at https://shop.standards.govt.nz/catalog/30300%3A2011%28ISO%29/view?client=html5

- Documents
- Letters
- Emails
- Text messages
- Digital images
- Audio recordings
- Databases and web pages
- Records in both physical formats (e.g. paper, or X-ray prints) and digital formats (e.g. CDs, USB keys, Office 365 documents).

ACC staff members, **must,** as part of their daily work:

- Create, and maintain, full and accurate records of your work to provide evidence of your activities or decisions
- Capture all your work records into ACC's core systems, not your personal H:\ drive, email/calendar, or OneDrive/OneNote
- Name your records so that they can be found and reused in the future (see 2.7 below)
- Ensure that, while working at ACC all your work records are:
  - Accessible to authorised ACC staff, now and after you depart
  - Usable, i.e. not corrupted or incomplete
  - Retrievable, i.e. appropriately named and stored in a standard location, e.g. on the shared drive or the Document Store
  - Preserved for future use.

People managers must ensure their staff are aware of, and follow, ACC's Information management policies and procedures.

2.1.1 Projects

Project managers are responsible for maintaining the formal records of their project and **must**:

- Ensure that project files (electronic and/or physical) are created at the beginning of a project
- Ensure all historical information is captured and filed as appropriate

- Ensure that all members of the project team save their work to the project file

  When deciding which project records to retain, project managers should consider:

  - The significance of the project's contribution to the functions performed by ACC
  - The importance of the project to the development of ACC within the New Zealand government infrastructure
  - Any residual value to the creators

2.2 Disposal of ACC records Standard

ACC formally contracts record retention and disposal with Archives New Zealand. This contract sets out:

- The many classes (types) of records ACC creates
- How long we must retain records of each class when they become non-current/are no longer active (this varies from months to decades)
- Our disposal action when the retention period ends (destruction, retention or transfer to Archives NZ for their collection).

Only members of the Information and Digital Tools team are permitted to authorise a disposal action.

For help with managing ACC record disposal (including personal work records), email [Out of Scope]

2.3 Clear desk Standard

ACC employees must secure all information in their workspace. This includes securing both electronic and physical information:

- At the end of the work day
- When they expect to be away from their workspace for an extended period.

Computer workstations/laptops must be locked (logged out or shut down) when unattended and secured at the end of the work day.

Mass storage devices such as CD, DVD, USB drives, or external hard drives must be locked away when not in use.

Printed materials must be immediately removed from printers or fax machines.

Avoid printing physical copies - documents should be viewed, shared and managed electronically whenever possible.

All documents that:

a) are no longer required, **and**

b) can be destroyed because they do not need to be kept as records of ACC decisions or actions

must be placed in the designated blue shredder bins for destruction.

Store rooms, filing cabinets and drawers must be kept closed and locked when unattended and not in use.

Keys and physical access cards must not be left unattended anywhere in the office.

Each team manager is responsible for enforcing the above standards. Repeated or serious violations of the clear desk standard can result in disciplinary actions in accordance with ACC's Code of Conduct.

If devices or documents go missing, or a workspace may have been tampered with, staff **must** notify [Out of Scope] immediately.

2.4 Classification and labelling Standard

The New Zealand Protective Security Requirements (PSR) require ACC to protectively mark information to help keep official information secure. They are a visual reminder of the security measures that apply to information or equipment.

Document classification or markings can be applied to a document manually, or automatically using the Microsoft AIP (Azure Information Protection) tool where available.

Documents with a protective marking or classification **must** be reviewed regularly and declassified when appropriate.

ACC staff who wish to classify or declassify a document but don't know how to do so must contact the Information and Digital Tools team for advice.

Documents stored on ACC servers may be scanned for sensitive content and where found, may have appropriate security classifications applied automatically.

ACC uses the following security classifications:

UNCLASSIFIED

- Official information that doesn't need a security classification is called 'unclassified' information. Most official information fits this category. **UNCLASSIFIED** isn't a formal security classification; is used as a protective marking. It shows a document has been reviewed and the impact from unauthorised disclosure or misuse has been assessed.
- Within ACC, **UNCLASSIFIED** is used to show a document has been assessed, or where an endorsement marking (q.v. 2.4.1 below) may be required on an otherwise unclassified document.
- **UNCLASSIFIED** may also be applied as the default classification for documents subject to software-applied automatic classification.

IN CONFIDENCE

Used when compromising the information is likely to:

- Prejudice the maintenance of law and order
- Impede the effective conduct of government
- Adversely affect the privacy of New Zealand citizens.

For instance, when the compromise of information could prejudice:

- Citizens' commercial information
- Obligations of confidence
- Measures for protecting the health and safety of the public
- The substantial economic interest of New Zealand
- Measures that prevent or mitigate material loss to members of the public.

Or when a compromise of information could:

- Breach constitutional conventions
- Impede the effective conduct of public affairs
- Breach legal professional privilege
- Impede the government's commercial activities
- Result in the disclosure or use of official information for improper gain or advantage.

When ACC receives documents with a higher security classification, for example from NZ Police, we must ensure they are appropriately declassified before being stored in ACC systems.

ACC **IS NOT** certified to receive, or store documents classified above **IN CONFIDENCE**.

ACC **must** take reasonable care to ensure we do not accept, or store, these documents unless they have been correctly declassified.

Where a document is received that has classification above **IN CONFIDENCE** staff **MUST** contact the Information Security and Privacy teams before dealing with the document.

If staff receive a document with a protective marking and don't know what to do with it, they should contact the Information Security Team at [Out of Scope]

2.4.1 Endorsement markings

Endorsement markings warn people that information has special requirements.
They may indicate:

- the specific nature of information
- temporary sensitivities
- limitations on availability
- how recipients should handle or disclose information.

ACC acknowledges some business areas may need endorsement markings.

Endorsement markings **must** only be implemented where a clear business case exists. The Chief Information Security Officer (CISO) must approve a process for classification, handling and declassification of documents before endorsement markings can be used.

Business units that require endorsement markings should first consult the Information Security Team and read the following:
https://www.protectivesecurity.govt.nz/information-security/security-classification-system-and-handling-requirements/new-zealand-government-security-classification-system/endorsement-and-compartmented-markings/

2.5 Copyright Standard

2.5.1 Key relevant documents

Include the following: *(in hierarchical order)*

- Copyright Act 1994
- ACC Information Management Policy

2.5.2 Definitions

Term	Definition
Intellectual Property	Intellectual property is an intangible asset and refers to creations of the mind: inventions, literary and artistic works, symbols, names, images, and designs used in commerce

2.5.3 Copying materials at ACC

ACC staff must only copy materials within the provisions of the Copyright Act 1994. Just because an item, image or file is found on the internet does not mean it is legal to download/copy or use it.

ACC staff are responsible for determining if copyright law applies. This is often the case even if the copyright symbol © isn't present.

'Copying' includes:

- Photocopying
- Duplicating an e-book, or sharing an e-book that is licensed for single-use only
- Copy-and-pasting text, images, or other files from the internet
- Right-mouse click Save As, or "snagging" or "snipping" an image online
- Scanning a document
- Copying the content of a document word-for-word, either by hand or typed.

2.5.4 What qualifies for copyright protection?

Copyright doesn't depend on the physical format of an item. For example, copyright may exist in:

- Paintings
- Written works such as novels, poems, articles, notes and song lyrics.
- Works of dance or mime and scenarios or scripts for films and plays.
- Paintings, drawings, plans and maps.
- Musical scores or arrangements.
- Sound recordings.
- Films, which includes DVDs, Blu-Rays and digital downloads.
- Communications including broadcasts or cable programmes.

2.5.5 What doesn't qualify for copyright protection?

Copyright protection does not apply to some government works, such as:

- Parliamentary bills
- Acts of Parliament
- Regulations
- Bylaws
- Parliamentary debates
- Select Committee reports
- Court and tribunal judgements
- Reports of royal commissions, commissions of inquiry, ministerial inquiries or statutory inquiries.

Be aware that reprints or publications of this material by non-governmental parties may have copyright.

2.5.6 Creating a reference or citation for an item

When using a copyrighted piece of work, reference its title, author, date and other distinguishing information so that the work can be identified and re-acquired in the future. Use a recognised referencing style, such as:

- Harvard System of Referencing Guide
- APA (American Psychological Association) Referencing Guide
- MLA Referencing Guide.

2.5.7 Client files and Copyright materials

Staff working with copyrighted material included in ACC client files must be fully informed and trained on their responsibilities:

- Copyright material must only stay on client files while it is actively used for research purposes. Once the research is complete, the copyright material must be cited appropriately and then removed from the file and destroyed.
- If copyright material is required for a review, hearing or appeal, this is permitted by section 59 if the Copyright Act as a "Parliamentary and judicial proceeding". ACC reviews and appeals meet this definition, but ADR (facilitation / mediation / conciliation) does not.
- When archiving a file, cite any research material it contains. If the research material is required in the future, the IDT team can retrieve a new copy for ACC staff.
- Copyright material on a client file must not be reproduced nor distributed with the file. If the copyright material is intended for research, or private study by the client and/or their advocate(s), then release is allowed.
- Section 43 of the Copyright Act ("research or private study") sets out the amount of material that can be copied.
- Only material required for research may be scanned into a Virtual Client Folder (VCF). Scanned copies must be replaced by citations when the client file is archived.

2.5.8 Information taken from library research databases

ACC purchases access to external internet-accessible databases, such as Medline and ProQuest. Information from these databases must not be shared with third parties.

2.5.9 Technology systems and software

Technology system specifications must include copyright compliance as part of their business requirements. The Service Assurance team (a part of Technology & Transformation) is responsible for ensuring software licensing agreements comply with the provisions of the Copyright Act.

2.5.10 Copyright infringements

The Manager Information & Digital Tools is responsible for responding to notifications of suspected copyright infringements. As per the requirements of the Act, a response is required within fourteen working days of receipt.

2.5.11 Contact for information

Email copyright policy queries to the Information & Digital Tools team at [Out of Scope]

2.6 Physical document storage Standard

Before deciding to archive a physical document, it **must** first be considered for digitisation

Staff sending a physical document for offsite storage must clearly and accurately name the document so it can be readily found and/or re-used when required in the future.

When staff send cartons of physical documents to offsite storage, they must compile and include a *transmittal list* in each carton. This list must describe all the contents in enough detail for the physical documents in each carton to be identified and re-used as required.

Physical files can be archived at ACC as corporate records, open claim files and archived claim files.

2.6.1 Corporate records

Corporate records include all records created within the corporate office such as Finance, HR and office administration.

Where possible, these must be digitised and stored in an appropriate digital system of record.

2.6.2 Open claim files

Open files are active client files, stored temporarily, with our offsite storage provider. They are file managed with individual barcodes.

Lodging and retrieving open claim files off-site is done through the ReQuest online web tool.

2.6.3 Archived physical claim files

In Eos, the “archived” status indicates the physical record has been sent to offsite storage.

Claim files are closed in Eos in preparation to be sent to offsite storage.

2.6.4 Onsite physical records

Any business-related records, for example personnel files, should be stored in digital form only.

Where the physical file is required, it must be listed and stored in secured filing cabinets or with ACC’s offsite storage provider.

This listing must be stored within a corporate shared drive and updated as required.

For queries about the offsite storage of physical documents, email the Information & Digital Tools team at [Out of Scope] or refer to the Sauce page http://thesauce/how-to/knowledge-management/recordkeeping/index.htm

2.7 Digitization and Digital document storage Standard

Staff uploading a digital document to an ACC core system (e.g. Eos, Hyperion, Promapp, Oracle Financials or the Document Store) must comply with the applicable system’s uploading standards. This includes complying with all relevant document naming conventions or practices.

Physical documents digitised for archiving/storage **must** comply with the Archives NZ recommended standards for the digitisation of text and photographic prints.

- **Bit depth**: 8 bit. Greyscale or bi-tonal. **Resolution**: 300 ppi. **File Format**: PDF/A, TIFF, JPEG 2000. **Compression**: Lossless compression
- **Bit depth**: 24 bit. Colour. **Resolution**: 300 ppi. **File Format**: PDF/A, TIFF, JPEG 2000. **Compression**: Lossless compression.

If in doubt, read the system documentation or ask the Information and Digital tools team for guidance.

Additional information about post-digitisation information disposal can be found here: Archives NZ advice

2.8 Document naming Standards

Naming documents consistently and accurately will allow ACC staff to find documents when they need it. This means documents can be found no matter where in ACC the document was created, or how long ago.

Inconsistent document naming leads to future problems, including:

- Lowering the chances of finding all relevant documents when searching. This means we risk making decisions based on incomplete knowledge
- Confusion over which version of a document is authoritative, which reduces staff confidence and trust in the systems
- Introducing compliance risk under the Accident Compensation, Privacy, Public Records, and Official Information Acts.

2.8.1 Document file names

File names should describe the document's content while being as brief as practical. The file name should let users find the document using search functions even when it is stored in an unexpected location.

2.8.2 Guiding principles

When naming documents, ask:

- does your file name clearly identify the document's content or purpose?
- did you use words that will still make sense to you when in six months' time you are searching for the document?
- that your file name is meaningful enough so that others using search to look for the document will easily locate it.

Aim to strike the right balance between:

- **Brevity**; keeping titles short. Thirty characters is a sensible maximum name length
- **Usability**; usefully describing the document's content

Personal names

Personal names should not be used as part of file names.

Where it is appropriate to use a personal name in a file name (e.g. staff management documents), use the following format:

> **First name Last name**, for example **Josephine Bloggs**. Avoid **Bloggs, Josephine** or **J Bloggs**

Corporate names

When using a corporate name in a file name, use the full form of the name unless its acronym is commonly accepted.

Do not use initial articles in corporate names, e.g. use Treasury, not ***The*** Treasury

Date Format

When identifying an event that occurred on a specific date, use the format **dd month yyyy** (e.g. Debrief – Security alert Shamrock House - 20 July 2018)

Note: a document's creation date is captured automatically as metadata in many systems. As such, the creation date may not be needed as part of the file name.

Dates should only be used in file names to:

- identify a specific event (e.g. an incident, report, meeting, etc.), or
- distinguish between similar documents (e.g. recurring meetings, weekly/monthly/quarterly/ reports)

Acronyms

Acronyms should not be used as part of a file name unless widely recognised e.g. ACC for Accident Compensation Corporation, or MOH for Ministry of Health.

Do not use punctuation such as full stops within the acronym (use NATO not N.A.T.O).

Write all acronyms in uppercase.

Abbreviations

Abbreviations (e.g. rpt, mtg, proc) **must not** be used in file names.

2.8.3 System Specific Guidance

A short-form desktop guide to naming documents for the ACC Document Store is available at https://accnz.sharepoint.com/:b:/s/Infodatamgmt/Recordsdocumentmgmt/ESWqnw_fSzREodqEoA2Ig3YBuAAf6cjBhUjiBKXqkLuOJQ?e=F9fl9P.

More lengthy guidance on naming Document Store documents is available at: https://accnz.sharepoint.com/:w:/s/Infodatamgmt/Recordsdocumentmgmt/EctUu2nyx51LhcI3aArZY9QBVEobsZ6GP78eouPO423Isw?e=dClAjW.

Email queries regarding ACC Document Store naming standards to the Information & Digital Tools team at IDT@acc.co.nz.

2.9 Metadata Standard

Where supported, all ACC documents **must** be saved with appropriate Metadata so the documents are searchable and discoverable.

At a minimum, this Metadata should include enough information for a user to find a document using a search engine.

Many ACC systems will automatically label documents with appropriate Metadata.

Contact the Information and Digital Tools team with any concerns or requests for further information.