Te Tari Taiwhenua
Internal Affairs

UNCLASSIFIED

Information management policy

Date approved	7 March 2022
Review date	March 2023
Policy owner	General Manager Information and Safety
Cohesion link	

Policy overview

1. The Department of Internal Affairs (DIA) is committed to developing and maintaining information management practices that support our daily activities and enable us to meet our business needs, accountability requirements and the expectations of government and the public.
2. Information is one of DIA's most important assets. It is our corporate memory. Information provides evidence of the advice, actions and decisions we have made. We use and re-use information to inform our work and help us deliver high quality services.
3. Trust and confidence in DIA's information is necessary to unlock the social, cultural and economic value of the information through increased sharing, use and re-use.
4. This policy sets out the principles that guide our information management activities, clarifies our shared responsibilities, and outlines expected practices and behaviours that will help embed a common approach to how we manage, access and use our information and ensure it can be trusted.

Audience and application

5. The audience for this policy is all DIA staff.
6. It applies to:
   - All DIA staff. For the purposes of this policy all DIA staff includes permanent, temporary and events-based staff members, as well as people contracted by or in a business relationship with DIA, including volunteers and other unpaid positions;
   - All information, regardless of medium, format or where it is stored, that has been created or received in the course of business functions, processes, decision making, actions and transactions;
   - All DIA's policies, systems, practices and procedures;
   - All business activities;
   - Inter-agency initiatives where DIA is the lead agency or where it is agreed that DIA owns or is responsible for the resulting information.

Definitions

7. For the purposes of this policy ***information*** has been adopted as a term to cover both information and records.

8. **Information**:

   - Provides documentation or evidence of all business processes, advice, activities and decision-making, including information used to support these processes;
   - Includes both original sources and copies;
   - Includes documents, signatures, text, images, sound, speech or data;
   - Can come in a variety of formats such as electronic files and emails, paper, film, tape, computer disks, text messages, social media, web pages etc.

9. It is recognised that different kinds of information can require different levels of care. For instance, information that has no or only transitory value as evidence of business activity will not need to be managed with the same level of care and retained for as long as more important information which has a higher value.

10. Refer to ***Appendix A – Definitions*** for a full list of the definitions that apply to this policy.

Responsibilities

11. **All DIA staff** must:

   - Abide by DIA's Code of Conduct, which provides details on the minimum standards of behaviour required from all DIA staff;
   - Create and maintain full and accurate information about all business activities, transactions and decisions, consistent with prudent business practice;
   - Ensure information is accessible to other staff in DIA unless reasons exist to protect the information as set out in DIA's Security Classification Policy;
   - Ensure personal information is managed in accordance with DIA's Privacy Policy;
   - Ensure information protected by copyright is handled in accordance with the Copyright Act 1994;
   - Complete information management online training and be aware of who to contact for advice and support;
   - Maintain awareness of their responsibilities for managing information and applying information management practices as described in this policy as part of everyday work activities.

12. **Managers:**

   - Must ensure staff are aware of this policy and meet their information management responsibilities. This includes ensuring:
     - All new staff complete information management online training in their first week;
     - All current staff complete information management online training;
     - All DIA staff are aware of who to contact for support and advice.

- Are expected to champion the principles and practices outlined in this policy by modelling the desired behaviours.

13. **Business system owners** and **owners of DIA's information assets** must:

    - Ensure information is protected to the extent it is possible from unauthorised or unlawful access, destruction, loss, deletion or alteration. This is particularly important when information is being collected, being migrated between systems or to another agency, or when ICT systems are being upgraded or decommissioned;
    - Ensure information remains useable and accessible for as long as the information is required to be retained in accordance with General Disposal Authorities, the DIA Retention and Disposal Schedule and the Chief Archivist Retention and Disposal Schedule;
    - Ensure the accurate capture of critical metadata such as creation, receipt, transmission, alteration and deletion;
    - Ensure all new ICT systems include compliance with this policy as part of their requirements;
    - Ensure risks are identified where current systems do not comply with this policy, and that risks are managed in line with the Risk Management Framework;
    - Manage and dispose of information in accordance with the General Disposal Authorities, DIA Retention and Disposal Schedule and Chief Archivist Retention and Disposal Schedule in order to avoid unnecessary storage costs and ensure information is managed appropriately over its lifecycle.

14. The **Information and Data team** is responsible for developing, promoting, monitoring and reviewing this policy. This includes:

    - Providing expert advisory services, education and training to staff and management in support of the policy;
    - Monitoring trends and performance and providing reports to inform the business and senior management;
    - Advising the Deputy Chief Executive Organisational Capability and Services (OCS) of required improvements for the purposes of compliance and best practice.

15. The **Deputy Chief Executive OCS** owns this policy and is responsible for monitoring DIA's performance under the Public Records Act 2005 and for advising the Executive Leadership Team (ELT) of any risks to DIA's ability to meet the requirements of the Act or that could compromise the performance of the Department.

16. In addition, the **Deputy Chief Executive OCS** is the designated Executive Sponsor for DIA, as required under the Information and Records Management Standard issued by Archives New Zealand.

17. **Deputy Chief Executives** are responsible for assuring the Chief Executive that their branch complies with departmental policies and processes that support information management practices and behaviours.

18. **ELT** is responsible for ensuring that DIA has a culture which supports the promotion and adoption of information management behaviours and practices. In addition, ELT is responsible for ensuring that information management activities are appropriately resourced.

19. The **Chief Executive** is responsible for ensuring DIA meets legislative requirements under the Public Records Act 2005, Official Information Act 1982, Privacy Act 2020 and other legislation.

Guiding principles

20. The following principles underpin this policy and articulate DIA's commitment to information management:

- Everyone in DIA is responsible for managing information;
- The information we create, collect, store, maintain and use is fit for its purpose;
- Information enables us to work effectively and deliver services to New Zealanders;
- We value our information and treat it as an important departmental and public asset;
- We champion a culture of openness: information is open by default unless reasons exist to protect it;
- We ensure personal and security classified information is properly protected and that the public's information is treated with care and respect;
- We support and promote collaborative and new ways of working.

Detailed policy

21. The following statements set out the responsibilities and expectations for how information will be created in DIA.

Create and maintain

22. All DIA staff are responsible for creating and maintaining full and accurate information. Information provides credible and authoritative evidence of DIA's business activities, protects legal and other rights of clients, staff or others affected by those actions, and facilitates audit or examination.

23. All information we create, receive, store and maintain will be managed as an asset in accordance with relevant information legislation and government strategies, policies, standards and guidance.

24. All information that staff create, send or receive in the course of their work is a public record under the Public Records Act 2005.

25. Any information[1] created, received or collected by or on behalf of DIA is regarded as official information and can be requested under the Official Information Act 1982 or Privacy Act 2020.

26. All personal information collected by DIA in the course of its business will be maintained in accordance with DIA's Privacy Policy.

27. All information created by people working on behalf of DIA is owned by the Crown unless explicitly agreed otherwise. This information is expected to be managed in accordance with this policy.

[1] Some exceptions apply – refer to the Official Information Act 1982.

28. All information protected by copyright will be managed in accordance with the provisions of the Copyright Act 1994.

29. High risk systems containing high value information are identified, managed and regularly reviewed to ensure risks are identified, managed or mitigated.

Storage

30. Digital information is considered to be the authoritative source unless there is a legitimate reason for other formats to be managed as such.

31. All information must be stored in approved DIA systems only, such as Cohesion, line-of-business systems or DIA-approved cloud storage. These systems should be used in accordance with their intended purpose i.e. Email is a communication tool and is not to be used to store information over the long term. Important business emails should instead be saved into Cohesion.

32. All information must be stored appropriate to its security classification, as set out in DIA's Security Classification Policy.

33. All physical information that is required to be retained must be identified, organised and managed in accordance with guidelines for managing physical information.

34. All physical information must be kept in DIA-approved facilities which provide a safe and secure environment, protected from environmental hazards and pests.

Access and protection

35. All DIA staff are responsible for determining whether the information they create meets the threshold for a security classification to be applied.

36. All security classified information (IN-CONFIDENCE, SENSITIVE and RESTRICTED) must be handled and managed in accordance with the Security Classification Policy.

37. All national security classified information (CONFIDENTIAL, SECRET and TOP-SECRET) must be handled and managed in accordance with the Protective Security Requirements.

38. Certain security classified information may be labelled with an endorsement marking in addition to a security classification. Endorsements are warnings that the information has special requirements in addition to those indicated by the security classification and should only be used when there is a clear need for special care. E.g. STAFF-IN-CONFIDENCE, COMMERCIAL-SENSITIVE.

39. All personal information must be managed to ensure compliance with the provisions of the Privacy Act 2020, as set out in DIA's Privacy Policy.

40. Information that does not pose any risk to policy, people's privacy or national security is UNCLASSIFIED. UNCLASSIFIED information should be accessible to all DIA staff by default. By making our information open to DIA staff we have a greater ability to find information to deliver better advisory and customer services and enhance our ability to collaborate.

41. Business critical information (vital records) must be identified and readily accessible when needed.

Information sharing and matching

42. All DIA staff are required to responsibly share information within DIA and with other government agencies, in accordance with the Security Classification Policy. This includes ensuring DIA information is not inadvertently released.

43. All DIA staff are expected to share information with DIA by sending a Cohesion link which links to the original content rather than sending copies (where content is stored in Cohesion), so that it is easy for staff to find the authoritative version.

44. Personal information matching and sharing should be carried out in accordance with the Privacy Act 2020, DIA's Privacy Policy and with guidance from DIA's Chief Privacy Officer.

Use and reuse

45. All DIA staff are expected to use information to improve operational decision-making, policy development and public services.

46. DIA champions the release and re-use of non-personal government information to the public in an open format for the purposes of enabling businesses, communities and individuals to innovate to solve problems or realise new opportunities.

47. Managers are responsible for identifying and proactively releasing information and data to the public.

Integrity

48. All information produced by DIA is expected to be reliable and trustworthy.

49. All DIA staff are expected to maintain the integrity of DIA's information. This includes ensuring that adequate metadata (descriptive information about the information) is saved and associated with its related metadata so that information has appropriate context and meaning, and not altering information without authorisation.

50. Business owners and owners of DIA's information assets are responsible for ensuring the contextual and structural integrity of information is maintained over time.

Disposal

51. Information must be managed according to its business, legal and archival value.

52. Low value transitory information can be routinely disposed of in accordance with the General Disposal Authorities issued by Archives New Zealand.

53. Information relating to DIA's core business functions must be managed and disposed of in accordance with DIA's Retention and Disposal Schedule.

54. Information relating to the work of Archives New Zealand must be managed and disposed of in accordance with the Chief Archivist Retention and Disposal Schedule.

55. DIA will routinely transfer information identified as a public archive to Archives New Zealand in accordance with the relevant disposal authorities.

56. DIA must be able to account for disposal activities in accordance with legal obligations and accountability requirements.

Performance monitoring

57. The Deputy Chief Executive OCS is responsible for monitoring and reviewing DIA's compliance with the Public Records Act 2005 and other relevant legislation to ensure that it is performing to expected standards, business needs are being met and accountabilities and responsibilities are understood and adhered to.

58. In addition, the Deputy Chief Executive OCS is responsible for monitoring and reviewing DIA's information performance against the Protective Security Requirements.

Legislation

59. The following legislation is relevant to this policy:

- Public Records Act 2005
- Privacy Act 2020
- Official Information Act 1984
- Copyright Act 1994
- Evidence Act 2006
- Local Government Act 2002
- Local Government Official Information and Meetings Act 1987

Related documents

60. The following documents are relevant to this policy:

- DIA Code of Conduct
- DIA Privacy Policy
- DIA Security Classification Policy
- Risk Management Framework
- Archives New Zealand Information and Records Management Standard

APPENDIX A – Definitions

Term	Definition
Copyright	Copyright exists in original works of literary, dramatic, musical or artistic works, sound recordings and films. Copyright is an automatic right, existing when the work is created, published or performed. Copyright on agency generated works is held by the Crown
High value information	Is determined by the business context. Any information which demonstrates the performance of legislated functions, the interactions with and entitlements of customers and employees, and information about core assets, is likely to be high value. Useful sources for determining high risk and high value business include DIA's risk register, internal and external audit reports etc
Information management	Is about how DIA creates, collects, receives, organises, identifies, governs, secures, uses, controls, shares exchanges, maintains, preserves and disposes of its information and how it ensure the value of that information is identified and can be utilised to its fullest extent
Information asset	Is a body of information that can be defined and managed as a single unit so it can be identified, understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles
Information integrity	The accuracy, completeness and validity of information. Integrity also means information has not been modified without authorisation and can be trusted
Information matching	Generally involves the comparison of one set of records with another, to find records in both sets of data that relate to the same person. When it's done by a computer its known as data matching
Low value information	Information that is of short-term and/or transitory value, which is not required for business, evidential or legal purposes i.e. information created through routine administrative and business processes common to most agencies
Official information	Any information developed, received or collected by or on the behalf of DIA. Information can be requested under the Official Information Act 1982 and there is an expectation it will be made available unless there is a good reason to withhold it
Open data	Data that can be freely used, reused and redistributed by anyone – subject only, at most, to the requirement to attribute and 'share alike'
Personal information	Information about an identifiable, living person. Personal information is a subgroup of official information and is managed according to the Information Privacy Principles and Privacy Act 2020
Records management	Is an integrated framework of governance arrangements, architectures, policies, processes, systems, tools and techniques that enable organisations to create and maintain trustworthy evidence of business activity in the form of records