Australian Government
Department of Infrastructure, Transport, Regional Development and Communications

DEPARTMENT OF INFRASTRUCTURE, TRANSPORT, REGIONAL DEVELOPMENT AND COMMUNICATIONS

RECORD KEEPING POLICY

MAY 2021

Contents

1. PURPOSE OF THIS POLICY

This policy describes requirements for all staff, contractors and (where appropriate) consultants working for the department to:

- Create and manage records of the department and their responsibilities in relation to that requirement;
- Ensure records are timely, accurate and readily available when and where required;
- Manage departmental records effectively to enhance information sharing and reduce time spent finding records, and
- Improve departmental compliance with legislative recordkeeping requirements.

2. WHY WE NEED A RECORD KEEPING POLICY

The department's records are a corporate asset. They are vital for supporting ongoing operations and providing evidence of business decisions, activities and transactions. The department is required under legislation to establish and maintain recordkeeping practices that meet its business needs, accountability requirements and stakeholder expectations.

This policy provides all staff with the information they need to ensure that they:

- Understand the importance of record keeping;
- Are aware of what can happen if they do not keep appropriate records;
- Know what they are required to do, and why, and
- Know what to do, and who to ask, when they have questions about record keeping.

Key points:

- *All employees of the department are required by legislation to keep records.*
- *Any information in any format that relates to the business of the department is a record.*
- *All departmental records must be stored and maintained in an appropriate information management system.*
- *Any record in any format which carries a security classification above PROTECTED must be kept in physical (paper) format and protected in accordance with the requirements of the Protective Security Policy Framework (PSPF).*
- *Active staff participation in records management ensures information is accurate, enables improved information sharing across the department and reduces time spent searching for records.*
- *Failure to maintain reliable records can lead to excessive retrieval costs, legal action or reputational damage for the department.*

3. WHAT IS A RECORD?

For the purpose of this policy, a record is defined as any information in any format that:

- Demonstrates or is integral to the conduct of the business of the department;
- Supports the decision making process;
- Details who made a decision and when it was made;
- Is required by law (including regulations) to be kept, or
- Has significant historical interest to the community.

Records can be in any format. This includes but is not limited to:

- Hard copy or electronic documents – e.g. Word, Excel, Power Point;
- Paper or electronic files – e.g. EDRMS containers;

- Electronic messaging – e.g. Email, voicemail, instant messaging (including, Skype, Teams, WhatsApp etc.), SMS (short message service) and multimedia message service (MMS);
- Social media – e.g. Twitter, Facebook, LinkedIn, blogs, wikis, discussion boards/forums;
- Web content – e.g. public websites, intranet;
- Photographs – e.g. official photographs documenting business activities, Flickr;
- Videos – e.g. YouTube, Vimeo, video conferencing, teleconferencing, video instant messaging and podcasts;
- Data in business systems – e.g. MyWorkplace (SAP), and
- Maps, models, plans and architectural drawings.

4. MAINTAINING RECORDS

4.1. Departmental Record Management Systems

All departmental records irrespective of their format **must** be captured, classified, stored and maintained in one of the department's Endorsed Record Keeping Systems detailed at Appendix B. This should occur as soon as is practical upon creation or receipt of the record.

These systems can only be used to hold information up to and including **PROTECTED**. Information marked as **SECRET** or **TOP SECRET**, **must not** be stored in these systems.

4.2. Physical Records (paper based)

Any physical record classified **PROTECTED** or below **must** be registered and managed in one of the department's Electronic Document and Record Management Systems (EDRMS).

Any record which carries a security classification higher than **PROTECTED must** be kept in physical (paper) format in a file cover that has been appropriately registered in one of the department's EDRMS.

Paper (print to file) records **must** be protected in accordance with the requirements of the Protective Security Policy Framework (PSPF).

4.1. Digital Records

All records created or collected digitally (electronic) or converted into digital form from their original format **must** be managed as digital records within one of the department's EDRMS.

4.3. Business and administrative databases and systems

Appendix B lists all systems that are endorsed by the department for the capture and storage of specific information. These systems appropriately support information management processes, such as creation and capture, storage, protection of integrity and authenticity, security, access and retention, destruction and transfer.

4.4. Use of personal drives, shared drives and other storage

Business information (irrespective of format) stored in shared drives, personal drives, email folders, SharePoint sites, the Cloud, local applications, cabinets, workstations and on backup disks or drives is **not** compliant with the department's recordkeeping obligations. Records **must not** be stored within any of these applications or locations as they do not meet adequate access, lifecycle management, security and record integrity requirements.

5. RECORD KEEPING RESPONSIBILITIES

Everyone is responsible for managing their records in accordance with this policy. Individuals must be aware of and exercise their responsibilities.

5.1. All Departmental Staff

- Must undertake the mandatory 'Information Matters' eLearning module in LearnHub;
- Must make themselves aware of the recordkeeping obligations and responsibilities that relate to their position;
- Must adhere to this policy, and all procedures and standards in keeping / maintaining records and information;

- Must protect all records from unauthorised access, disclosure, modification, loss or damage;
- Must create and capture full and accurate records related to all business activities and ensure these are maintained in the department's recordkeeping system, and
- Should contact the Records Management team to enrol in training on recordkeeping and use of the department's EDRMS.

5.2. All Managers and Supervisors of Staff

- Will monitor staff under their supervision to ensure that they understand and comply with the department's recordkeeping policies and procedures for the creation and maintenance of records;
- Will support and foster a culture within their workgroup that promotes compliant recordkeeping practices and use of recordkeeping systems;
- Will provide agreement for the destruction of information for which they are responsible, and
- Will ensure that information in the care of their staff (including contractors and consultants) is secured in accordance with the PSPF and departmental security requirements.

5.3. The Chief Information and Security Officer (CISO)

The CISO has specific responsibilities in relation to record keeping, in particular:

- Ensuring that recordkeeping practices are reviewed regularly and that the department complies with its legislative obligations and responsibilities as a Commonwealth agency;
- Developing policies that support staff meeting their obligations;
- Providing and maintaining the department's record keeping system and ensuring that it is reliable, available and accessible to staff as required;
- Providing final departmental approval for any records management administrative matters i.e. destruction of records, etc. and
- Providing training for all staff to support awareness of their responsibilities.

5.4. The Records Management Unit (RMU)

The department has a dedicated Records Management Unit that reports to the CISO and is responsible for:

- Creating and maintaining record keeping procedures in line with this policy;
- Promulgating the department's recordkeeping policy and procedures to all employees via appropriately available communication channels;
- Supporting and fostering a culture of good record keeping within the department;
- Delivering record keeping training and advice to all staff;
- Providing support to all staff in the use of the official record management system and responding to requests for information and support;
- Monitoring the capture and creation of records into the record management system, to assist in identifying incorrectly created and/or captured records, and
- Ensuring that records are kept for only as long as the department, Government and the public require them - destroying records as established under an authorised disposal authority or through the application of normal administrative practice including associated administrative duties i.e. destruction notifications to National Archives of Australia.

6. ACCESS TO INFORMATION

Open access to information and the release of information according to relevant legislation must be balanced with the need to adhere to security classifications protecting information.

Records are a corporate asset that should be easily accessible by all staff, except where the nature of the information requires restriction due

to its security classification. Access restrictions should not be imposed unnecessarily, but must protect:

- Individual staff or client privacy;
- Sensitive material, such as security classified material or material with information management markers, for example “OFFICIAL: Sensitive NATIONAL CABINET,” and
- Release of publically available information.

In meeting obligations under the Information Publication Scheme and in the spirit of open government policies, the department provides access to publicly available information on the departmental website.

The public has legislative rights to apply for access to information the department holds under the *Freedom of Information Act 1982* and the *Archives Act 1983*. These apply to ALL information including records held by the department, whether in officially endorsed information management systems or in personal stores such as email folders or shared and personal drives.

Responses to applications for access under the Freedom of Information legislation are the responsibility of the appropriate business area.

Responses to applications for access under the *Archives Act 1983* are the responsibility of the National Archives of Australia.

7. RETENTION AND DESTRUCTION OF RECORDS

Departmental records **must** be kept up to date. The department adheres to the *Archives Act 1983* 'normal administrative practice' (NAP), and allows for some destruction without formal authorisation.

Destruction without formal authorisation only occurs when information is:

- Duplicated – for example, reference material from other agencies or information copies, extra copies of documents kept for convenience;
- Unimportant – for example, thank you emails or personal messages, or
- Of short term facilitative value – for example, insignificant drafts, or test data from business systems that provide no evidence of agency functions and activities.

These records should only be retained as long as there is a business need to do so.

Records that do not meet this criteria, and are therefore not subject to NAP as described above must not be deleted or destroyed without the application of an appropriately approved records authority issued by the National Archives of Australia. Such deletions and destructions are managed by the Records Management Unit.

8. TRANSFER OF PHYSICAL FILE CUSTODY

Inactive physical files that are not routinely required to support daily activities, **must** be returned to the Records Management Unit. Prior to the return of the files, staff **must** ensure all documents are securely attached and the security classification of the file **must** reflect the highest classification of the information it contains.

The transfer of records to a new custodian or return to the Records Management Unit **must** be registered in official record management system.

9. COMMUNICATION AND TRAINING

This Recordkeeping Policy **must** be provided to new starters and will be accessible to all staff on the intranet. Training will be provided on aspects of the policy and will be offered in formal and informal environments.

10. MONITORING AND REPORTING

This recordkeeping policy will be reviewed biannually to reflect changes in the broader Australian Government legislative and regulatory environment, best practice standards, and to ensure currency and relevancy to the business of the department.

APPENDIX A – RELEVANT RECORD KEEPING LEGISLATION, POLICIES AND STANDARDS

The following Acts relate to recordkeeping in the Australian Government:

- Archives Act 1983 – empowers the National Archives of Australia to preserve the archival resources of the Commonwealth and authorises destruction/transfer of and access to records;
- Crimes Act 1914- forbids unauthorised disclosure of information;
- Electronic Transactions Act 1999 – recognises electronic transactions as records;
- Evidence Act 1995 – clarifies the acceptance of records/copies in court;
- Freedom of Information Act 1982 – provides a public mechanism for access to records;
- Privacy Act 1988 – protects information gathered about individuals;
- Public Governance Performance and Accountability Act 2013 – includes provisions which deal with recordkeeping of Commonwealth agencies, and
- Public Service Act 1999 – employees must not disclose inappropriate information.

The department is also committed to ensuring that its recordkeeping and business systems comply with existing established standards and major reports into recordkeeping in the Commonwealth such as:

- Australian Standard AS ISO 15489 – Records Management;
- ISO 16175 – Processes and functional requirements for software for managing records;
- Australian Government Recordkeeping Metadata Standard;
- Australian Government's Digital Transition Policy;
- Australian Government's Digital Continuity Policy (including the Digital Continuity Plan);
- Policies and Guidelines published and endorsed by NAA for Commonwealth agencies, and
- Protective Security Policy Framework.

APPENDIX B – ENDORSED RECORD KEEPING SYSTEMS

The following systems are endorsed for the department's recordkeeping:

System	Endorsed for
Content Manager 9	Electronic Document and Records Management System for the Department of Infrastructure, Transport, Regional Development and Communications records and all former Department of Infrastructure, Transport, Cities and Regional Development records
Records Manager 8 via Information Management System	Electronic Document and Records Management System for the Department of Infrastructure, Transport, Regional Development and Communications records and all former Department of Communication and the Arts records
SAP	Human Resource and Financial records
PDMS+	Parliamentary documents
CabNet	Cabinet documents