**Australian Government**

**The Treasury**

| AUDIENCE | CATEGORY |
|----------|----------|
| All Staff | Information Management Policy |

THE TREASURY – POLICIES AND PROCEDURES

# Information Governance Framework

This document was endorsed by the Information Strategy Committee on 27 June 2019

For further information or questions, phone Josh Pearse x4015

recordsservicesteam@treasury.gov.au

# Contents

| Date | Version | Description of change | Name | Position |
|------|---------|----------------------|------|----------|
| 29/10/2014 | 1.0 | All | Simon Kovacs | Approved version |
| 11/01/2017 | 1.1 | Rewriting of sections 1,2,3,4 & 7 | Josh Pearse | Draft |
| 17/10/2018 | 1.2 | Rewriting of sections 4, 5 and 9, general re-formatting | Josh Pearse | Draft |
| 2/07/2019 | 1.3 | Noting of authorisation, removal of watermark | Josh Pearse | ENDORSED |

# 1. PURPOSE

The purpose of this document is to outline the framework for the creation, security and management of records and business information within Treasury.

Treasury's information is a major component of its corporate memory and is a vital asset that supports business operations. Treasury records provide valuable evidence of Treasury's corporate and core business activities.

Treasury is committed to establishing and maintaining secure and efficient information management and recordkeeping practices that enable its business outcomes, comply with accountability and legislative requirements, and address stakeholder needs.

The *Information Governance Framework* is a key governance tool for enabling the *Information Governance* theme of the *ICT Strategic Plan*.

# 2. FUNCTION

The Information Governance Framework (Framework) enhances Treasury's business performance by providing a business context for information governance and recordkeeping practices, processes and systems that treat information as an asset. This will provide for the ongoing security, integrity and accessibility of records, in turn guaranteeing the continued contribution of records to the efficient, effective and ethical delivery of quality outcomes.

Within the Commonwealth Government, good information governance:

- Provides evidence of government decisions and activities;

- Demonstrates that the accountability requirements of an organization have been met;

- Supports business activities through the creation of usable and reliable records, contributing to business efficiency and efficacy; and

- Minimises business risk by ensuring that the right records are created to sustain business performance and continuity.

# 3. SCOPE

This Framework applies to the management, security, access and disposal of all physical and electronic information created or captured in the course of Treasury business activities, and all business applications used to create or capture Treasury records including email, business information systems and databases (including those hosted by other government agencies and cloud providers). This also includes Treasury business information captured in business diaries and in laptop computers, as well as Treasury devices such as Notebooks, iPads, smartphones, iPhones, cameras and hard drives.

This Framework applies to all permanent, contract and non-ongoing staff engaged by Treasury.

# 4. INFORMATION LIFECYCLE

## 4.1 Creation of 'Official Records'

**Any information or data created, collected, generated or stored by Treasury as a result of business processes, decisions and outcomes is considered a Commonwealth record.** Commonwealth records must be managed in accordance with applicable National Archives'-endorsed Records Authorities.

Treasury's Records Authorities dictate the correct management and retention periods of particular types of business information. Records Authorities also empower Treasury to dispose of Commonwealth records in accordance with Section 24 of the *Archives Act 1983*, once the minimum retention period has expired.

Official Records can only be disposed of after obtaining approval from the Agency Records Manager, and only once the minimum retention period has elapsed.

## 4.2 Information Security Classifications

All information generated or collected by Treasury is subject to Treasury's *Agency Security Framework*[1] which is compliant with the Australian Government's *Protective Security Policy Framework*.

Information must be classified and stored in accordance with its content, and sometimes context, to ensure that only parties with a requisite need-to-know and security clearance have access to the information or are in a position to receive the information.

This requirement also applies to information that is collected and stored on Treasury assets for reference only and not necessarily considered to be part of an official Treasury record.

## 4.3 Access to Treasury Information

**Sharing information within the Treasury:**

Information is an asset which should be available to the appropriate staff in Treasury and used to improve the service Treasury delivers to the Australian public. Information access should not be restricted unnecessarily, but should always protect:

• Sensitive material that is **security classified** or material with an information management security marking such as OFFICIAL: Sensitive or material that has information management access restrictions such as Privacy, Legal privilege or Legislative secrecy provision; and

• individual staff or client privacy.

When handling information, staff are reminded of their obligations under the APS Values, APS Code of Conduct, APS Commissioner's Directions and Public Service Regulations.

---

[1] Specifically, Section 10 – 'Information Security'

**Release of publicly available information:**

In accordance with Treasury's obligations under the Information Publication Scheme, access to information subsequently released to the public is provided (where practical) on the Treasury website. This is the responsibility of the Communications and Parliamentary Division.

The public have legislative rights to apply for access to information held by Treasury under the *Freedom of Information Act 1982* and the *Archives Act 1983*. These rights apply to all information held by the Treasury, whether in officially endorsed records management systems or in personal stores such as email folders or shared and personal drives. Responses to applications for access under Freedom of Information legislation are the responsibility of the Law Design Office. Responses to applications for access under the *Archives Act 1983* during the open access period are the responsibility of the National Archives of Australia.

## 4.4 Normal Administrative Practice (NAP) Disposal

Section 24 of the *Archives Act 1983* allows Commonwealth agencies to destroy certain types of records in the normal course of their work. This disposal tool is known as Normal Administrative Practice (NAP). NAP may be applied to records of short-term, facilitative or transitory value; often referred to as ROT (redundant, obsolete or trivial information). Treasury has NAP guidelines that assist staff in identifying ROT and using NAP.

Staff should be familiar with these guidelines and be aware that unauthorised destruction not only risks **criminal penalties** under the *Archives Act 1983* but may expose the Treasury to a range of other risks including:

- inability to comply with regulatory and legislative responsibilities such as the Freedom of Information Act and the Privacy Act;

- inability to provide access to information during legal discovery action; or

- damage to organisational reputation.

Staff must not destroy information, other than in accordance with the Treasury's NAP guidelines, without the approval of the Agency Records Manager.

# 5.  MANAGING RECORDS

## 5.1 Recordkeeping Policy Statement

Treasury information must be created, stored and managed in **an endorsed Treasury business system**, and be kept for as long is required, and no longer, to guard the continuity of reliable and accessible digital information stores against technical obsolescence. Only information classified SECRET or higher can be stored in a paper file.

The following systems and software applications are currently endorsed for the capture and storage of digital information in line with approved Treasury record classes and the *Minimum Metadata Standard*. These include:

• SharePoint
• HP Content Manager (formerly *TRIM*)
• Foreign Investment Management System (FIMS3)
• Parliamentary Document Management System (PDMS) and CABNET+
• Aurion
• TechnologyOne

**Outlook** and **Shared Drives** are not approved information management systems. Information that constitutes an official record must be transferred to one of the **endorsed** systems in a timely manner.

## 5.2 Digital Continuity Statement

In line with the National Archives' *Digital Continuity 2020 Policy*[2], the Treasury supports a **digital approach** to all information management and recordkeeping.

The *Digital Continuity 2020 Policy* is a principles-based whole-of-government information management compliance model which aims to ensure that:

1. Information is Valued
2. Information is Managed Digitally
3. Information, Systems and Process are Interoperable

By practicing digital recordkeeping, the Treasury will ensure information is complete, available and useable for as long as the information is required by legislation or is required to fulfil a business activity.

Information must be able to be:

• found when needed;
• accessed when needed;
• worked with in the required manner; and
• identified and contextualized reliably by metadata.

---

[2] Australian Government *Digital Continuity 2020 Policy* is available here: http://www.naa.gov.au/records-management/digital-transition-and-digital-continuity/index.aspx

# 6. INFORMATION MANAGEMENT LEGISLATION AND STANDARDS

There are several legal and procedural requirements that govern the way Treasury must manage information. Relevant legislation, standards, policy, advice and guidance that have recordkeeping implications for the Treasury include:

- *Archives Act 1983* and other relevant legislation[3];

- Australian Standard *Records Management AS ISO 15489*;

- International Standards *Principles and Functional Requirements for Records in Electronic Office Environments ISO 16175* and *Information and Documentation – Management Systems for Records ISO30300*.

- The *Australian Government Recordkeeping Metadata Standard 2.2*

- Attorney-General's Department, *Commonwealth Protective Security Policy Framework*

- The Australian Signals Directorate (ASD), *Information Security Manual* (ISM);

- Department of Prime Minister and Cabinet, *Cabinet Handbook (10th Edition)*

The above material comprises a combination of:

- Australian government policy requirements and minimum standards and associated guidelines for certain information management activities;

- Australian government legislative and mandatory requirements, primarily relating to controlling the destruction of records and disclosure of government information; and

- Australian government best practice standards, checklists and guidelines covering a wide range of recordkeeping and information management activities.


## 6.1 Minimum Metadata Standard

In accordance with the National Archives' *Digital Continuity 2020 Policy*, Treasury business systems must progressively implement the *Minimum Metadata Standard*[4]. This standard ensures that information stored on all business systems has a consistent minimum amount of auditable metadata that can contextualize business transactions in a defensible and transparent manner.

The Metadata Standard is also designed to ensure that all information has a base-level of consistent metadata tagging which allows for homogenous searching and management across systems and platforms. The initial requirement for basic metadata compliance came into effect on **31 December 2016**, and will enable compliance with Principle 3 (Information is Interoperable) of the *Digital Continuity 2020 Policy*.

The Minimum Metadata Standard also applies to **Cloud hosting** of business systems engaged by Treasury to store business information and should be consulted before engaging Cloud services.

---

[3] These include *National Security Information Act 2004, Privacy Act 1988, Electronic Transactions Act 1999, Evidence Act 1995, Crimes Act 1914, Public Service Act 1999, Public Governance, Performance and Accountability Act 2013*

[4] The National Archives of Australia's *Minimum Metadata Set* can be found here: http://www.naa.gov.au/records-management/agency/minimum-metadata/index.aspx

### 6.2 Treasury Companion Policies

This Framework <u>replaces</u> *Treasury's Recordkeeping Policy*.

This Framework is <u>informed by</u>:

- National Archives of Australia's *Government Information Management Standard*

- Treasury's *Records Authority*

- The *Archives Act 1983*

- Treasury's *Agency Security Framework*

This Framework <u>informs</u>:

- Normal Administrative Practice (NAP) Guidelines

## 7. INFORMATION MANAGEMENT RESPONSIBILITIES

| | |
|---|---|
| **All Treasury staff including secondees, contractors, and consultants engaged by the Treasury** shall: | • understand information management obligations and responsibilities that relate to their position;<br><br>• ensure that key decisions and events are accurately recorded and can be easily retrieved when needed;<br><br>• capture records into designated information and records management systems that provide evidence of the actions, decisions and communications made in carrying out Treasury business activities; and<br><br>• destroy records only in accordance with an authorised disposal authority or through the application of normal administrative practice (NAP). |
| **The Information Strategy Committee** shall: | • endorse the Information Governance Framework; |
| **The Deputy Secretary, CSBSG** shall: | • provide sufficient support and resources for sustaining a successful information governance program; and<br><br>• promote compliance with Treasury's information and records management policies and guidelines and the Australian Government's *Digital Continuity 2020 Policy*. |
| **The Chief Information Officer** shall ensure that: | • strategies are developed and implemented to support the information and records management policies;<br><br>• Treasury's information management practices comply with its obligations and responsibilities as a Commonwealth agency; and<br><br>• all staff are advised of the Treasury's information management requirements. |

| | |
|---|---|
| **All managers and supervisors of the Treasury's staff** shall: | • ensure that information and records are properly maintained for the operations for which they are responsible. This includes governance of the creation, maintenance and lawful disposal of Treasury's records;<br><br>• ensure staff:<br><br>- receive training and ongoing support to manage the Treasury's information and records appropriately;<br><br>- have time and resources available to comply with records management obligations; and<br><br>- monitor and evaluate records management practices relating to operational matters for which they are responsible. |
| **Information Services Division** shall: | • provide training, advice and general support to all staff regarding responsible and efficient information management;<br><br>• develop, implement and maintain records management products and tools, including systems, to assist in the creation of complete and accurate records;<br><br>• promulgate the Treasury's information and records management policies and guidelines to all staff;<br><br>• monitor staff and system compliance; and<br><br>• ensure that records are retained for as long as they are required. |
| **ICT Staff** shall: | • maintain technology for the Treasury's information and recordkeeping systems, including maintaining appropriate system accessibility, security and business continuity measures; and<br><br>• ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with the 'Disposal' requirements in this Framework. |

## 8. FRAMEWORK MONITORING AND REVIEW

This Framework will be updated every two years or earlier if there are changes in the Treasury's work or regulatory environments.

# 9. RELATED DOCUMENTS

- Agency Security Framework

- Normal Administrative Practice (NAP) Guidelines

- Social Media Policy

# 10. TERMINOLOGY

The following table lists definitions of terms used or associated with this Framework.

| Term | Description |
|---|---|
| Capture | The process of lodging a document or digital object into a recordkeeping system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time. For certain business activities, this functionality may be built into business information systems so that the capture of records is concurrent with the creation of records.<br>*Glossary of Records Management Terminology – National Archives of Australia.*<br>*http://www.naa.gov.au/records-management/publications/glossary.aspx* |
| Creation | To make a record (evidence) of business transactions<br>*Glossary of Records Management Terminology – National Archives of Australia.*<br>*http://www.naa.gov.au/records-management/publications/glossary.aspx* |
| Cloud computing | Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. |
| Record | 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.<br>*(AS/ISO15489 Part 1: 3.15)* |
| Recordkeeping | The making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes the creation of records in the course of business activity, the means to ensure the creation of adequate records, the design, establishment and operation of recordkeeping systems and the management of records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration).<br>*Glossary of Records Management Terminology – National Archives of Australia.*<br>*http://www.naa.gov.au/records-management/publications/glossary.aspx* |
| Recordkeeping metadata | Information about records and the context in which they are captured and used. This is information that the National Archives recommends be captured in business systems used by Australian Government agencies to create and |

| | capture records. |
|---|---|
| | *Australian Government Recordkeeping Metadata Standard Version 2.2 (AGRkMS)*<br>*National Archives of Australia's Minimum metadata set* |
| Recordkeeping System | A framework to capture, maintain and provide access to evidence of transactions over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include:<br><br>• both records practitioners and records users;<br><br>• a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices;<br><br>• policy statements, procedures manuals, user guidelines and other documents that are used to authorise and promulgate the policies, procedures and practices;<br><br>• the records themselves;<br><br>• specialised information and records systems used to control the records; and<br><br>• software, hardware, other equipment and stationery.<br><br>*Glossary of Records Management Terminology – National Archives of Australia.*<br>*http://www.naa.gov.au/records-management/publications/glossary.aspx* |
| Records Authority | A records authority is an instrument issued by the National Archives of Australia to give its approval to Australian Government agencies or other organisations or persons to dispose of Commonwealth records. Records authorities may also state which classes of records are to be retained as part of the archival resources of the Commonwealth. Records authorities that permit destruction generally specify the minimum length of time that Commonwealth records must be retained. Some authorities may include other conditions. Records authorities are issued under the Archives Act and Regulations for the purposes of sections 24, 26 and 3C. Section 6 of the Archives Act empowers the Archives to authorise the disposal or destruction of Commonwealth records. Records authorities (RAs) usually apply to the records of a single agency. General records authorities (GRAs), such as the Administrative Functions Disposal Authority (AFDA), normally apply to all Commonwealth institutions. Records authorities were previously referred to as records disposal authorities (RDAs), while general records authorities were previously referred to as general disposal authorities (GDAs).<br>*Glossary of Records Management Terminology – National Archives of Australia.*<br>*http://www.naa.gov.au/records-management/publications/glossary.aspx* |
| Records Management | The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.<br>*Glossary of Records Management Terminology – National Archives of Australia.*<br>*http://www.naa.gov.au/records-management/publications/glossary.aspx* |

# 11.   RESOURCES

- National Archives of Australia *Australian Government Recordkeeping Metadata Standard* (AGRkMS) Version 2.2 National Archives of Australia (2018) *http://www.naa.gov.au/information-management/managing-information-and-records/describing/metadata/AGRKMS/index.aspx*

- National Archives' *A-Z for Information and Records Management*: http://www.naa.gov.au/information-management/support/a-z/index.aspx

- National Archives of Australia (2018). Special access arrangements under sub-section 56(5) of the Archives Act 1983. Special access – Fact sheet 219  *http://www.naa.gov.au/collection/fact-sheets/fs219.aspx*

- National Archives of Australia (2018) Digital Continuity Policy 2020 *http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/index.aspx*

- Australian National Audit Office (2012). Performance Audit Report No. 53 2011-12 – Records Management in the Australian Public Service.

- International Organization for Standardisation (2010). Information and documentation – Principles and functional requirements for records in electronic office environments – ISO 16175, Geneva Dec 2010.

- Standards Australia (2008). Australian Standard for Records Management – AS ISO 15489, Sydney March 2002.

- ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles

# 12.   CONTACTS

For advice, please contact the Agency Records Manager- Information Strategy Unit, Information Services Division, who is also responsible for updating and maintaining this policy/procedure.

To provide feedback on this Framework, please contact the Information Strategy Unit.

Search... | SEARCH | People s

Home | About ⌄ | Services | Knowledge library ⌄ | TSY News ⌄ | Social ⌄ | Emergency | First aid ⌄

## Quick guide to recordkeeping

The Treasury's records are its corporate memory, and as such are a key strategic asset for ongoing operations, providing essential evidence of business activities and transactions. The Treasury recognises its regulatory requirements as a Commonwealth agency, and is committed to the recordkeeping principles and practices set out in the National Archives' *Information Management Standard* and Australian Standard for Records Management (AS ISO 15489).

## What is a record?

Records are defined in the *Archives Act 1983* as a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of:

(a) any information or matter that it contains or that can be obtained from it; or

(b) its connection with any event, person, circumstance or thing.

Records include papers and documents, emails, spreadsheets, notebooks and diaries, social media posts and information in business systems including case management systems and CRMs. Essentially, if you can read it or obtain information from it, it is a potential record.

Commonwealth records are records created or received in the course of APS employment. Those records can be:

- Useful or important records that need to be kept indefinitely by the National Archives. These are known as retain national archives (RNA).
- Useful or important records which should be retained as long as there is a business or legislative need
- Low-value records which should be disposed of when those records are no longer current or useful

Every APS employee has an obligation to ensure that their records are kept appropriately and that useful or important information is available to other staff in their agency.

## Recordkeeping obligations

The creation, maintenance and accessibility of Commonwealth records are key elements of sound public administration and accountability.Creation of records to account for business activity and decisions is specifically prescribed in the *Public Governance, Performance and Accountability Act 2013*.

- Records are an essential part of the Treasury's corporate memory and risk management strategies. Records are important (and sometimes vital) assets that support the Treasury's operational business needs, comply with legislative and other regulatory requirements and meet community expectations.
- The *Public Service Act 1999*, the APS Commissioner's Directives and the APS Values and Code of Conduct consistently carry the message that public servants are accountable for their actions and should be able to account for those actions.
- Effective recordkeeping is key to meeting these obligations, as well as assisting APS employees to quickly and accurately respond to requests from Minsters and the Parliament.

## Archiving in SharePoint

Information created at Treasury is generally archived in SharePoint, with the retention period linked to the record class applied to the library, site or document type, depending on the most appropriate aggregation level of the information.

- The Records Authority class applied to a record defines the minimum retention period for that record. Retention periods can vary i.e. 7 years for some types of records, or up to 10 years, 30 years , 50 years or 'Retain as National Archives' (RNA) for others. RNA records are eventually transferred to the National Archives permanently.
- Retention periods are activated only if the information aggregation (or 'file') is dormant – i.e. no modifications are made to documents, or no new documents added.
- Once the contents of a SharePoint 'file' are archived, the records are retained until the retention period passes. At this time, the appropriate disposal actions are undertaken by the Treasury Records Manager.
- Permanent disposal of expired records is only carried out with the approval of the business area that owns the records. Keeping information for longer is acceptable as long as that action is based on a legitimate business need. Records must not be destroyed earlier than the minimum retention period.

## What do I need to do?

Treasury information must be created, stored and managed in an endorsed Treasury business system, and be kept for as long is required, and no longer, to guard the continuity of reliable and accessible digital information stores against technical obsolescence. Only information classified SECRET or higher will be stored in a paper file.

The following systems and software applications are currently endorsed for the capture and storage of digital information in line with approved Treasury record classes and the Minimum Metadata Standard. These include:

- SharePoint (via RecordPoint)
- HP Content Manager (formerly TRIM)
- Foreign Investment Management System (FIMS3)
- Parliamentary Document Management System (PDMS)
- Aurion
- TechOne (OneGov)

Outlook, network shared drives and apps such as GovTEAMS are not Treasury-endorsed information management systems. Information that constitutes an official record must be transferred to one of the endorsed systems in a timely manner.

## eLearning Module for Recordkeeping

A Recordkeeping Awareness (RKA) eLearning module (taking around 25 minutes) is available on Treasury Learning. The module explains why recordkeeping is important and the responsibilities of Treasury staff. The Recordkeeping Awareness eLearning module is now located under the Onboarding>eLearning folder.
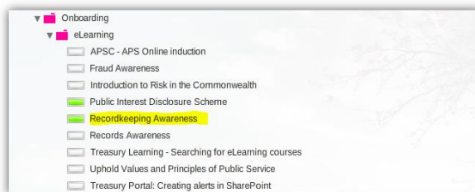


## HPE Content Manager

### Background

HP Content Manager (HPCM) is the latest iteration of the HP Records Manager, or 'TRIM', system. It is a fully-compliant information and records management system, able to store nearly any type of digital file.

HPCM manages all Treasury's legacy paper records, and some electronic records from the period of approximately 2001-2012. Though SharePoint is ostensibly Treasury's primary 'recordkeeping system', HPCM is still actively used by several areas of Treasury for storage of digital information.

HPCM is available to staff who require access to records previously saved in HP TRIM or because of their business processes, require access to HPCM to save official records.

HPCM is only accessible through the desktop client, as the web client is no longer actively supported by HPE.

If you require HPCM, please lodge a New Software Request through the Delphi self-service portal via My Applications>Delphi>Popular Requests>Software Request

**Contact:** Information Strategy Team (x3811).
**Last updated:** 14/11/2018

# Guide to records removal

## Normal Administrative Practice (NAP) Guidelines

The Archives Act includes a 'Normal Administrative Practice' provision which allows for the destruction of a number of categories of records without formal authorisation.

Many low-value records should be destroyed when no longer useful, in accordance with normal administrative practice.

Records may be divided into two broad categories;

- useful or important; and
- low-value.

Useful or important records are to be saved into Treasury's recordkeeping systems.

Low-value records should not be saved into Treasury's recordkeeping systems and may be destroyed by Treasury staff in accordance with normal administrative practice.

NAP allows staff to routinely destroy (by deletion) records that are not needed as evidence of Treasury's day-to-day business and that do not need to form part of Treasury's corporate records.