



ACT Health

Records Management Procedures

Document number	AHDPD-10:2022
Effective date	09 Aug 2022
Review date	09 Aug 2025
Author branch	Office of the Chief Information Officer, Digital Solutions Division
Endorsed by	Executive Board
Audience	ACT Health
Version number	1.0

Contents

Purpose	1
Scope	1
Procedure.....	3
The ACT Health Records Management Program	4
What is a record?.....	5
Benefits of good recordkeeping	6
Who manages records?	7
Records Management at ACT Health.....	7
Creation and Capture.....	8
Titling records	11
Management and Use.....	13
Stored and protected.....	16
Access.....	20
Retention and disposal	22
Preservation.....	27
Business Systems Assessment and Planning	28
Records management arrangements with outsourced service providers	29
Implementation	29
References and Related Documents.....	29
Definitions.....	31
Version Control	32
Attachment 1:	33
Business Systems and Digital Recordkeeping Functionality Assessment Tool, Territory Records Office.....	33

Purpose

All ACT Health Directorate staff are responsible for the creation and management of records. This procedure manual assists staff to meet their responsibilities and the requirements of the *Territory Records Act 2002*.

This document forms part of the records management program and supports the recordkeeping obligations set out in the Records Management Policy. Adherence with the procedures will ensure consistent and coherent recordkeeping processes and practices across ACT Health.

Good recordkeeping management practices applied throughout ACT Health support efficiency and accountability through the creation, management and retention of accurate, reliable and accessible evidence of government activities and decisions.

The retention and preservation of our corporate memory, in the form of records, ensures staff meet their functional and legislative obligations for maintaining proper and complete records. This reduces the possibility of error, fraud, manipulation or destruction of relevant information to ensure an accurate audit trail exists for all decisions, actions and operations. This also protects the rights of staff, clients, service providers and stakeholders of ACT Health.

Failure to capture all relevant records in the corporate recordkeeping system can expose ACT Health to significant risk, especially when business disputes arise, in litigation or in cases involving public accountability. Where records cannot be found to support business activities the risk becomes significantly greater.

When controlled effectively, responsible management of an organisation's business processes improves efficiency. This is supported by ensuring vital information is captured and maintained as evidence of business activities and is accessible for as long as the record is required to be retained.

Scope

Guidance for ACT Health staff, including students, volunteers, consultants, contractors and / or service providers, on the appropriate management of administrative records.

Roles and Responsibilities

This guidance excludes clinical records.

Position	Responsibility
Every employee	All staff must adhere to ACT Health's Records Management Policy and Procedures in maintaining records as required within their duties and to the Act. Staff must understand the recordkeeping requirements and responsibilities specified within these documents and how they apply to their role.

Staff are responsible for the creation and management of records in regards to the work they perform on behalf of the organisation. Staff must routinely create full and accurate records of work activities including records of all substantive decisions and actions.

Staff must ensure records are captured into the appropriate system so that they are accessible and appropriately secured as needed. Staff will be held accountable for unauthorised access to information.

Staff must not destroy records without authorisation from ACT Health's Chief Information Officer, except through the appropriate application of Normal Administrative Practices (NAP) – refer to the Procedures for further explanation.

Staff must undertake annual records management training as required.

Director-General	The Director-General is ultimately responsible for the management of records, promotes compliance with the Records Management Policy and these procedures, supports and fosters a culture of good recordkeeping in the organisation, and ensures the Records Management Program is adequately resourced.
Chief Information Officer	Develops policy, strategy, resourcing and systems to ensure the successful operation of approved records systems. Approves additions to the systems of record, compliant with standards, to be available to manage records and information. Owner of the Records Management Program, Policy and supporting Procedures. Oversees the records management program. Coordinates compliance of systems against the Territory Records Office standards for all records. Authorising the disposal of records. Reports to the Director-General on records management.
Digital Committee	Reports to ACT Health Executive Board on records management matters
Director Records Management	The Director Records Management is responsible for implementing and monitoring recordkeeping legislative and best practice requirements across ACT Health. Providing input into records management business plans. Identification of records management requirements.

The development, implementation and periodic review of the policy and procedures to ensure currency with best practice/standards.

Reporting to the CIO on records management issues.

Digital Solutions Division staff	Staff are responsible for maintaining the technology for business systems, including appropriate system accessibility, security and back-ups in accordance with ICT policies.
CMTEDD Digital Records Support Team	Maintaining and administering the EDRMS systems Provision of technical and functional support and advice Ensuring systems are updated where there are changes to configurations, such as, business functions and activities in the WhoG thesaurus and changes to records authorities.
Agency Security Advisor	The Agency Security Advisor provides advice on security policy and guidelines associated with the management of records
Managers and Supervisors	Managers are ultimately responsible for ensuring that all records produced by their area are captured, maintained and accessibly stored in the Objective, EDRMS, in accordance with this policy. Ensuring that staff, consultants and / or contractors under their responsibility are made aware of their records management obligations and what information resources and training is available to them. Advise the Director Records Management of any changes in the business environment, such as restructures. Ensure that all staff under their responsibility undertake annual records management training. Ensure that record and information management responsibilities are expressed in worker role descriptions, performance management plans
Staff, Volunteers, contractors, consultants and service providers	Staff, volunteers, contract staff, consultants and service providers must create and manage records in accordance with this policy and supporting procedures Undertake necessary training

Procedure

This Legislative Obligations

The *Territory Records Act 2002*, (the Act) sets out records management requirements for the ACT Government. The intent of the Act is to:

- a) encourage open and accountable government by ensuring Territory records are made, managed and, if appropriate, preserved in accessible form; and
- b) support the management and operation of Territory agencies; and
- c) preserve Territory records for the benefit of present and future generations; and
- d) ensure that public access to records is consistent with the principles of the *Freedom of Information Act 2016*.

The Territory Records Office (TRO) assists Directorates across the Australian Capital Territory (ACT) to meet records management requirements as set out in the Act. The TRO is responsible for ensuring each Agency develops and maintains a Records Management Program that is appropriate and relevant to their functional requirements. The records management program includes requirements for the creation, management, protection, preservation, storage and disposal of and access to records.

The TRO does this by:

1. issuing standards and guidelines that set the minimum standards for the management of information, records and data in the ACT Public Service (ACTPS);
2. providing a range of advice documents on records management topics;
3. encouraging consistency in records management programs between agencies;
4. provision of assistance, advice and training in records management; and
5. monitoring disposal of records.

ACT Public Service

The ACT Government Digital Recordkeeping Policy for the ACTPS has three core principles providing direction for good recordkeeping. These are:





1. The ACTPS adopts a digital first approach to recordkeeping. All information generated or received is in digital form.
2. Recordkeeping in the ACTPS is compliant with relevant standards, regardless of format. In creating, managing, preserving and making records in digital formats the ACTPS will comply with the *Territory Records Act 2002* and the records management standards produced under the Act.
3. Digital recordkeeping is considered in all ICT systems. When making decisions about the introduction or upgrade of any ICT system, agencies must consider the:
 - business transactions that system will support;
 - records that will be required to be made of those transactions; and
 - ability of the system to appropriately manage, preserve and make accessible those records for as long as they are needed.¹

The ACT Health records management procedures support the above statements.

The ACT Health Records Management Program

¹ Digital Recordkeeping Policy for the ACTPS

The [ACT Health Records Management Program](#) provides a framework for ensuring records management requirements are met. The framework has four components to direct records management best practice.

Framework	Components
1. Requirements 	<ul style="list-style-type: none"> • <i>Territory Records Act 2002</i> • Territory Records Office (TRO) • TRO implementation guidelines • TRO Agency self-assessment checklist • Best practice international standards
2. Governance 	<ul style="list-style-type: none"> • Digital Committee • Strategy and planning • Records Management Program, Records Management Policy and Records Management Procedures • Roles and responsibilities • Annual work plans • Performance monitoring & compliance • Internal audits
3. Capabilities 	<ul style="list-style-type: none"> • Skilled records management resources • Corporate recordkeeping system, Objective • Whole of Government tools – business classification scheme, records authorities • Digital preservation • Training and communication.
4. Program Principles 	Strategy, Capability, Assess, Describe, Protect, Retain, Access - Principles to ensure records management practices support open & accountable government & records are managed & preserved

What is a record?

The *Territory Records Act 2002* (the Act) defines a ‘record’ as the information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation or in the course of conducting business. This includes information in written, electronic or any other form.

The Act requires all ACT Government organisations to make and keep full and accurate records and manage those records over time. Managing records includes:

- Creating, capturing and maintaining records to provide evidence of business activities.
- Taking action to protect the authenticity, reliability, integrity and useability as business context and requirements for management over time change.

The international standard, ISO 15489, Records Management², describes records as evidence of business activity and information assets. Any set of information regardless of structure or form can be managed as a record, including:

- Office documents (i.e., Word, Excel, PowerPoint), e-mail, digital images
- Information and data held within, and extracted from, business systems
- Datasets used for analysis
- Audio (e.g., voicemails) or video, including hosted materials on websites (e.g., YouTube)
- Communications on social media applications
- Handwritten documents
- Paper, microform, digital
- Maps, plans, drawings, photographs etc.

This means all documents, information and data made or received by ACT Government organisations that provide evidence of a business activity are records. Regardless of form or structure records should possess the following characteristics to ensure they can be considered authoritative evidence of business events or transactions.

- Authenticity – authentic records can be shown to support the business transaction, created as part of a business process by authorised representatives.
- Reliability – records are reliable in that they are a trusted, full and accurate representation of business transactions and activities.
- Integrity – records can be protected against unauthorised alteration so the records can be shown to be complete and unaltered; any changes to the records can be tracked.
- Useability – records can be located, retrieved and available for use.

The records management procedures manual provides best practice guidance to ensure ACT Health records possess the above characteristics.

Benefits of good recordkeeping

Records are an essential part of transparent and accountable Government. Records provide evidence, explain actions, justify decisions and demonstrate the process undertaken.

Implementation of best practice records management processes and procedures provides significant benefits to agencies, such as:

- Contributing to business efficiency and accountability;
- building corporate memory;
- compliance with best practice standards and methodologies;
- supporting improved productivity (through ease of access to information for real time decision making);
- enabling re-use of past work instead of re-inventing the wheel;
- providing evidence when decisions or actions are challenged;

² ISO 15489-1:2016, Information and documentation — Records management — Part 1: Concepts and principles

- documenting the rights and entitlements of individuals and organisations;
- preserving information assets in order to meet legal requirements; and
- ensuring records of corporate / historical significance and/or value are retained and preserved.

Who manages records?

All ACT Health employees are responsible for managing their own records. This includes:

- Capturing all records, including email, which document business activities into the corporate recordkeeping system, Objective.
- Titling documents and records to ensure they can be retrieved easily by all users.
- Ensuring records are consistent, accurate, reliable and complete.

The Records Management Team delivers all aspects of centralised records management services to ACT Health. These services include:

- Strategic direction
- Program, Policy and Procedure development and implementation
- Developing business rules
- Administration and Maintenance of Objective
- Training
- Governance and Quality Assurance
- Management of legacy paper records
- Archival and disposal activities

Records Management at ACT Health

Records management at ACT Health is underpinned by the following approach to the management of information.

1. The creation, capture and management of records are integral parts of conducting business, in any context.
2. Records, regardless of form or structure, are authoritative evidence of business when they possess the characteristics of authenticity, reliability, integrity and useability.
3. Records consist of metadata, which describes the context, content and structure of the records, as well as their management through time.
4. Decisions regarding the creation, capture and management of records are based on the analysis and risk assessment of business activities in their business, legal, regulatory and societal contexts.
5. Systems for managing records, regardless of their degree of automation, enable the application of records controls and the execution of processes for creating, capturing and managing records. They depend on the defined policies, responsibilities, monitoring and evaluation, and training in order to meet identified records requirements.

Records management comprises a range of processes for creating, capturing and ongoing management of records.

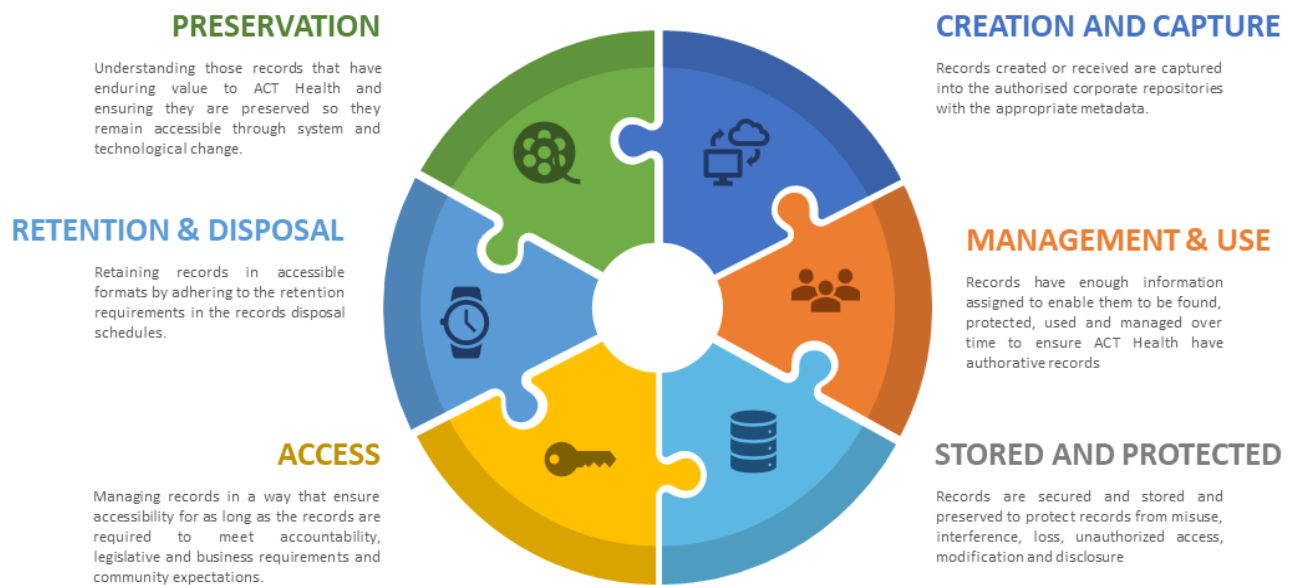


Figure 1: RM processes

Creation and Capture

Whenever business action is undertaken, all staff involved must create and capture records that document or facilitate the transaction of a business activity. If the record is not an automatic or direct by-product of business, the record should be made and captured into the corporate recordkeeping system as soon as practical after the event.

The following sections provide guidance on the creation and capture of records.

What records should be captured

The following documents are examples of business records that should be captured in the corporate recordkeeping system, Objective

- Letters, submissions, ministerial, reports, briefs, enquiries and responses
- Agreements/contracts, joint ventures and Memorandum of Understanding (MOU's)
- Statistical data e.g., Key Performance Indicators (KPIs) / scorecards
- Investigation cases, complaints
- Business plans / cases
- Workplace Safety records
- Accreditation, quality assurance and risk management documentation/evidence
- Financial transactions, such as receipts, invoices, salary reports, budget, spreadsheets procurement and tender documents
- Personnel employment records
- Committees/working groups and / or task force etc. agenda and minutes
- Policies and procedures.

The importance of a record may not always be apparent when it is first created. If you answer yes to any of the questions below then the information is to be considered as a record and captured into a formal record keeping system:

- Is there a statutory requirement to make or keep particular records?
- Has a decision been made or a course of action authorised?
- Are there any financial or legal implications that may come under scrutiny to ensure accountability?
- Does the record act as evidence to support a particular recommendation, conclusion, decision or pronouncement?
- Do you require the record so as to be able to report to internal or external bodies?
- Has a decision been made which will impact on another individual, business unit, branch or ACT Health as a whole?
- Has a decision been made which needs or may need supporting evidence or a record of the decision/making processes?
- Will the record document a change to policy, procedure or methodology, and why these changes were made?
- Is the record a document in the process of being drafted that is being sent to others for feedback, comment or approval?
- Does the transaction have to be approved by a more senior employee?
- Does the document convey information about matters of public safety or public interest, or involve information about which contractual undertakings are entered into?
- Is the record of interest or importance to others outside your immediate working environment?
- Will the record be of use to you or your immediate working environment in the future as a record of how something was done, or why it was done?
- Is the record of historical significance?

When to capture a record

All incoming correspondence or records received as part of doing business, must be captured into the corporate recordkeeping system. Records must be captured upon receipt or as soon as practicable after receipt. It is always safer, and more efficient, to capture records from creation, rather than at a later stage. If a delay occurs there is a risk important records may not be captured resulting in loss of critical information that could impact decision making processes or even the reputation of ACT Health.

The following guidance is provided:

- The officer involved in the business transaction or activity is responsible for ensuring records are captured into the corporate recordkeeping system.
- Staff are required to ensure appropriate records are created. For example, draft (or a particular version of a draft) must be captured as part of the record when it is submitted for approval, circulated for comment, revised as a result of comments, and when it is finalised.
- Staff must not maintain individual or separate files or records systems.

Management of email and instant messages

Records in email and instant messaging format have the same significance as other electronic business records. Emails and instant messages should be captured in the recordkeeping system if they relate to business. The mixture of formal and informal communications undertaken using email and instant messages can cause confusion for staff about what to regard as a record, and what the responsibilities to capture these records are. Generally speaking, electronic messages should be regarded as a record when they:

- approve or authorise actions
- constitute formal communications between staff e.g., memos relating to official business
- signify a policy change or development
- relate to projects or activities being carried out
- contain advice or provide guidance
- constitute formal communications between staff and outside recipients about official business, or
- facilitate an ongoing project or activity being carried out.

Emails and instant messages are “discoverable” in litigation. They will need to be produced in court if required under a subpoena and are subject to copyright, privacy and defamation legislation. In order to maintain their value as evidence, messages must be inviolate. This requires they are maintained in a system which prevents them from being altered or manipulated from their original state. Therefore, emails and instant messages of ongoing value must be captured in Objective.

The following guidelines apply to emails and instant messages which have ongoing value as evidence of ACT Health business:

Business Rules	
Sending an email or instant message	<ul style="list-style-type: none">• it is the responsibility of the initiator of a message sent either internally or externally to keep a record of that message if it is appropriate.• outgoing messages should only be captured once they have been sent.
Receiving an email or instant message	<ul style="list-style-type: none">• if you receive a message from a staff member, it is the sender’s responsibility to capture the message as a record if necessary.• you are responsible for capturing messages as records that you receive from outside the organisation.• where you are copied a message (i.e. you are not the main recipient), you should check whether the main recipient is a staff member, or is from outside the organisation. If the latter, you will need to capture a record of that message.• if there are several main recipients of a message, the person who is mainly responsible for the matter or project should capture the message as a record. In cases where you can predict the group of people who will be receiving emails on the matter or project, it may be helpful to agree on one person as

	being responsible for the capture of messages relating to that matter or project.
Chains of emails or instant messages	Often messages become part of a series of replies. In these cases, it makes sense to capture the last message in the series, which will include all previous exchanges, rather than separately capturing all the messages.
Attachments	Attachments to emails and instant messages should be saved both as records in their own right and also as a part of the email/instant message. The email/instant message provides the linking of multiple documents received as attachments at one time. The context of the attachments is provided, in part, by the email/instant message 'envelope'. However, the attachments should also be extracted and saved independently to enable continuing access to the contents.

Receipt of hardcopy documents

Where hardcopy documents have been received by ACT Health they must be digitised and captured into Objective. This is business process digitisation. In business process digitisation, the business action takes place on the digital record and therefore the official record of the action is the digital record. The official records must be identified as the one which is used in the transaction of business and captured into the corporate recordkeeping system with the appropriate metadata to ensure the records can be understood, used and managed. Refer to [Section 3.2.1](#) for information on key metadata to be applied to digital records. Refer to the section on [Preservation](#) for guidance on the digitisation of hardcopy records.

Once records have been digitised and captured into Objective the source (hardcopy) records can be disposed of in accordance with the requirements as set out in the [Converted or Digitised Source Records RDS \(NI2020-435\)](#) and the [TRO Records Advice, Digitisation and disposal of Source Records](#).

Titling records

Naming conventions

When capturing records into Objective the titling of documents should be clear and concise and not require interpretation. Titling should clearly reflect the content and subject matter and users should understand what something is about without having to open the file. Consistent titling will ensure records can be searched, located and retrieved in a timely manner.

The following rules are provided.

Business Rules	
Language	✓ Write in natural language and plain English so the title makes sense
Legislation	✓ Use regulations short name e.g., Information Privacy Act 2014.
Approved versions	✓ PDF and save as final
Repetition/redundancy	✗ Don't use words such as "word document" or "spreadsheet" in titles

<ul style="list-style-type: none"> Avoid duplicating words 	<ul style="list-style-type: none"> ✗ Finance Folder ✗ Email from John.msg ✗ Spreadsheet 2010.xls
<ul style="list-style-type: none"> Avoid where possible duplicating words already used in the folder title. 	<ul style="list-style-type: none"> ☐ Complaints ✗ Complaint from Mr. J Jones.docx ✓ Jones, Jack 12345 2010.06.10
Abbreviations	<ul style="list-style-type: none"> ✓ Use abbreviations and acronyms if very obvious e.g., ACT, NSW (See also <i>Approved Abbreviations</i> below) ✓ Don't use unusual abbreviations or acronyms that would not be widely known or could be misinterpreted
Emails	<ul style="list-style-type: none"> ✓ Ensure you capture business emails into Objective ✓ Don't include "Re" or "Fw" as part of titles when capturing emails into Objective IQ. Including these makes it difficult to sort by title
Persons Name	<ul style="list-style-type: none"> ✓ [First Name] [Surname]
Noise words	<ul style="list-style-type: none"> ✗ Don't use words like if, but, so, and, for etc unless required for clarity

Approved Abbreviations	
ACT Health approved abbreviations / acronyms	<p>Only commonly used abbreviations are to be used, such as:</p> <ul style="list-style-type: none"> NSW – New South Wales VIC – Victoria QLD – Queensland TRO – Territory Records Office, etc. <p>Acronyms can change over time. Avoiding the use of uncommon acronyms as much as possible will ensure continued understanding of the records.</p>

Document Naming Convention		
Format Rules		
Date - Calendar	[YYYYMMDD]	
Date - Financial Year	[YYYY/YYYY]	
Name	[Surname, First Name]	
Business Rule		
Naming Rule	[Description of subject/topic]	
Document Type	Convention	Naming Example
Advice	Received [Name] – [Subject/Topic] – [Date]	
Contract/Agreement	[Vendor/Provider] – [Subject/Topic] – [Date]	
Approval	[Topic] – [
Correspondence	Received [Name] - [Topic] – [Date]	
Correspondence	Response [Name] - [Topic] – [Date]	

Media Release	[Media Outlet Name] - [Subject matter] – [Date]	
Presentation	[Event Name] - [Title] – [Department] - [Date]	
Reports	[Subject Topic] – [Department] - [Date]	
Authorisation	[YYYYMMDD] Approved [Name] – [Topic]	20210920 Approved – Peter O’Halloran CIO – Camera Purchase
Plan	[YYYY/YYYY] [Topic]	2021/2022 Digital Solutions Business Plan

Management and Use

ACT Government organisations are obliged to ensure records receive appropriate metadata for the management and use of those records for as long as they are required to be retained. The **TRO’s Guideline to Principle 4: Describe Principle**, details requirements for ensuring ACT Health records will be understandable and allow them to function as records that are evidence of business activities. This is done through the application of metadata captured with the records when registered into the corporate recordkeeping system, Objective.

Key Metadata for records

Metadata is descriptive information that helps people understand, use and manage records over time. Some metadata is automatically applied to records upon capture in Objective, additional metadata may be required to be captured by the user.

Key minimum metadata fields applied to records in order for them to be managed effectively include:

System generated or process metadata	End user applied
<ul style="list-style-type: none"> • Date of creation • Creator (of the record) • Unique Identifier – distinguishes records from other records • Creating Application (where applicable) – the data format that provides the structure for a digital image • Business function/activity • Management / audit history • Disposal information, e.g., records authority, disposal class ID, disposal action, disposal trigger date, disposal action due • Use history 	<ul style="list-style-type: none"> • Title (or name) – to facilitate retrieval • Additional keywords (if applicable) • Classification • Document type

The capture of the above metadata ensures:

Records are:

- Complete and unaltered
- Adequate
- Accurate and trustworthy
- Authentic
- Findable and readable
- Secure from unauthorized access, alteration and deletion.

Objective supports the following recordkeeping processes:

- Creation and capture
- Linking records to business context
- Linking records to people, agents and relationships between records (contained, aggregation, contained by)
- Applying or changing access rules
- Secure storage
- Measures for continued useability
- Migration and conversion
- Disposition including destruction and transfer

Refer to the Objective [Quick Reference Guides](#) for more information on creating files, folders and capturing documents.

Business Function/activity - functional classification

A key piece of metadata applied to records is business function and activity. In Objective this is referred to as the Primary Keyword. The application of business function and activity is applied through the functional thesaurus. This provides a consistent, structured, and uniform vocabulary classification system used to classify ACT Health administrative records by business function and activity. Business function and activity provides records with important contextual information enabling them to be understood over time and links them to the context of their creation.

The functional thesaurus works in conjunction with the Whole of Government Records Disposal Schedules covering both general administrative (common) functions, as well as functions more applicable to the core business of ACT Health and other Directorates.

It is important to note each file based on the function and activity it refers to will vary with regards to how long by law it needs to be retained. It is therefore important to ensure the most appropriate function and activity is applied to files and subject matter.

When creating files in Objective the **Primary Keyword** field is used to select the business function and activity the file relates to. Refer to the [Objective IQ Quick Reference Guide, Creating Files](#).

The functional thesaurus used by Health consists of the following business functions:

n

Whole of Government Common Functions	
Finance and Treasury Management	The function of managing financial resources and providing strategic financial and economic advice and services to the ACT Government.
Strategy and Governance	The function of establishing the strategic direction and governance framework for ACT Government and its organisations, and overseeing the management of their operations through systematic planning, controlling and managing the overall structures, framework and direction of the organisations to meet government goals, Objective IQs and priorities and ensure overall performance and conformance in the delivery of goods, services or programs.
Government and Stakeholder Relations	The function of establishing formal communication channels and relationships between the ACT Government, its organisations and other governments and for establishing rapport with the community and raising and maintaining the Territory's or organisation's broad public profile.
Human Resources	The function of managing all employees and volunteers in the organisation from recruitment through to separation.
Information and Communications Technologies	The function of managing the organisation's technology and telecommunications resources and services through the planning, provision, development or acquisition of information and communication technologies.
Property, Equipment and Fleet	The function of acquiring, supplying, maintaining, operating, managing and disposing of property, facilities, vehicles or equipment owned, rented, leased or used by the organisation.
Records and Information Management	The function of managing the records and information resources of government and its organisations to ensure recordkeeping compliance and to meet their operational needs and, if appropriate, to allow public access to the records consistent with the Territory Records Act 2002 and the Freedom of Information Act 1989.
Solicitor and Legal Services	The function of providing solicitor and other legal services to the ACT Government, Ministers and organisations.
Whole of Government Core Functions	
Student Management	The function of managing students by supporting them throughout their attendance at schools and tertiary educational institutions and assisting them to undertake and successfully complete their studies.
Training and Tertiary Education	The function of developing, planning, funding, managing and reporting on education and training opportunities, programs and initiatives in the ACT.
ACT Health Core Functions	

Public Health Protection	The function of managing risks to public health through regulation, scientific analysis, and the implementation of strategies for the prevention of, and timely response to, public health risks and events. This function includes regulatory and policy activities relating to food safety, communicable disease control, environmental health, health emergency management, pharmaceutical products and radiation sources.
Patient Services Administration	The function of providing sports and active recreation services to the community and industry with the aim of promoting active lifestyles through fostering participation in, and supporting the advancement of, sporting activities, events and programs.
Health Treatment and Care	The function of providing patient/client health care and treatment by a health service provider. Includes individual health evaluation, diagnosis, treatment, care, progress and health outcomes of clients and patients.
Population Health Care Management and Control	The function of managing the programs and health services for the population through the provision of injury, illness and disease mitigation and reduction programs, lifestyle awareness and promotion of healthy lifestyles and low risk behaviours, population health monitoring and strategic health care planning.

Stored and protected

In accordance with the TRO Protect Principle, ACT Health must ensure records are stored in a manner that ensures they are secure and protected from misuse, interference, loss, unauthorised access, modification, and disclosure. Refer to the [TRO Guideline to Principle 5: Protect Principle](#).

This means that:

- Measures are in place to ensure a secure environment in which to manage records. This environment is the corporate recordkeeping system - Objective for digital records and the Digital Solutions Division warehouse for legacy paper records.
- Security classifications have been implemented and are applied to records.
- Privacy requirements are met.
- Access to information is controlled to meet privacy and security considerations.

Business teams should observe the following standards when storing records:

- Official records should not be maintained outside of the corporate recordkeeping system, Objective.
- Official records should be maintained with security appropriate to their classification.
- Digitised records will be stored in formats that are widely available (TIFF, PDF, JPEG).
- Physical files must not be maintained as the official record for any new records created after 1 January 2023.

Corporate recordkeeping system – Objective

Objective is the corporate recordkeeping system. Records should be captured in Objective unless they are required to be captured in an authorised business system. Objective provides a controlled environment for the management of records, providing users with easy functionality to manage records in a dashboard style

interface. Objective provides users with the capability to manage work in progress documents in a secure home folder that is like a users' H: drive

Please refer to the **Objective IQ Quick Reference Guides** for guidance on the use of Objective.

Business systems

Business systems are systems that are utilised for a specific purpose such as financial, human resources or service requests. These systems are used for the collection of information into structured forms for particular purposes. Records created in these systems do not need to be duplicated into Objective.

Examples of frequently used business systems are:

- HRMIS and Chris21/HR21 for personnel related forms and information
- APIAS and HRIMS for invoice processing and other financial activities
- Service Now (also known as Snow) for certain services from CMTEDD (such as HR and Finance)
- JIRA for service requests for Digital Solutions Division services.

Unauthorised or temporary storage locations

The following are unauthorised or temporary storage location and should not be used for the storage of ACT Health records. These repositories or storage devices do not have the functionality required to ensure appropriate long-term management of ACT Health records.

Unauthorised / temporary storage locations	Rationale
Shared drive and One Drive	<p>Using the shared drive environment for capturing records poses the following risks:</p> <ul style="list-style-type: none">• Difficulty finding and retrieving information due to large volumes of uncontrolled information;• records can be accidentally deleted;• structures evolve informally and are subject to individually designed filing structures;• it can be difficult to identify the status or latest version of a record;• records lack context, metadata is missing and records cannot provide reliable evidence of actions;• information is never disposed of leading to large volumes of storage which become costly to maintain and contribute to inability to find and use relevant information;• lack of recordkeeping functionality, for example, audit controls, security controls able to match Government-wide guidelines and retention and disposal rules; and• ACT Health will be unable to demonstrate authenticity, integrity and trustworthiness of uncontrolled records.

Unauthorised / temporary storage locations	Rationale
Portable flash memory electronic storage devices	<p>These devices should only be used for transferring data or for the temporary storage of information.</p> <p>Flash memory devices are the most common portable storage device in use today and create many issues surrounding their use, including security and privacy. They should not be used as a solution for the storage of records.</p>
Computer hard drives and desktops	<p>Computer hard drives and desktops should not be used to capture and store records.</p> <ul style="list-style-type: none"> • Access to information is restricted to the owner of the computer. • Hard drive and desktops are not backed-up. • Information could be compromised if a laptop is lost. • Information is lost if the computer malfunctions.

Security Markings

Only a small percentage of ACT Health official records are sensitive; most information should not be restricted unless necessary. Staff should only access information that their job function requires them to access. Typically, security marked records contain personal, commercial or operationally sensitive information relevant to ACT Health business. These records need to be protected. Security controls minimise risk to the confidentiality, integrity, reliability and availability of records.

Restriction should only be placed on access to records where specifically required by business needs or the regulatory environment. The need for restriction may change over time. Security classifications do not directly reflect nor imply exemption from disclosure.

Over-classification may hinder the open and effective conduct of ACT Health business. Where a business record requires confidential or secure treatment, it is to be marked appropriately and treated in accordance with the security classification.

Classifications reflect the Australian Government Protective Security Policy Framework(PSPF) Classification Scheme articulated within ICT Security Standards.

Dissemination Limiting Markers (DLMs) approved for use by the ACT Government that are in use at Health are:

Term	Definition	Examples
Official	Official is for everything that is government business. Most routine government information would fall under this marking.	<ul style="list-style-type: none"> • Emails, document and normal day to day internal government correspondence.

Term	Definition	Examples
For Official Use Only (FOUO)	This marking is to be used on information where compromise may cause limited damage to national security, the Office or other agencies, commercial entities or members of the public.	<ul style="list-style-type: none"> • Tender responses • Correspondence outlining contractual requirements.
Sensitive	This marking is to be used on information where the release or loss of this information could cause damage to individuals, organisations or the government.	<ul style="list-style-type: none"> • the disclosure of which may be limited or prohibited under legislation. • secrecy provisions of enactments may apply;
Sensitive – Personal	This marking is used for information that contains a fact or opinion, whether true or not, about an individual or an individual who is reasonably identifiable. This marking should be applied to all sensitive personal information as defined under the <i>Information Privacy Act 2014</i> and personal health information under the <i>Health Records (Privacy and Access) Act 1997</i> .	<p>Personnel record such as</p> <ul style="list-style-type: none"> • Medical certificates. • Performance and development plans.
Sensitive: Legal	This marking is used to identify information that is subject to legal professional privilege.	Correspondence seeking or receiving advice from any legal professional body, including the ACT Government Solicitor.
Cabinet	This marking should be used on everything related to cabinet documents and cabinet matters. These documents have specific handling requirements as detailed in the Cabinet Handbook.	Cabinet documents and related correspondence.

Security Markings / DLMs are used to clearly indicate the level of sensitivity / confidentiality surrounding a record, in hardcopy or digital format, providing a clear indication of the level of protection that should be applied to the record. For example:

- a) no sensitive or security classified information is left unattended on a desk (i.e., it is stored appropriately).
- b) ICT equipment (computers and media devices) is locked when not in use or attended by the user.
- c) electronic media and devices containing classified or sensitive information are secured with appropriate encryption.
- d) keys to classified storage devices are secured.
- e) keys are not left in doors and drawers (at the end of the day or for an extended period of time).
- f) being mindful of who is present and therefore able to hear a conversation surrounding highly sensitive and / or confidential matters both within the workplace as well as outside of the workplace and in earshot of the general public.

- g) when transferring sensitive or security classified information it is done so using transfer methods authorised by ACT Health.

Information is also provided in the ACT Government publication, Governance in the ACTPS.

Access

Wherever possible or practical ACT Health supports making records available to staff and the public unless there is a legitimate reason to withhold them.

This general statement is subject to legislative requirements for access to records established within the *Territory Records Act 2002* and the *Freedom of Information Act 2016*.

The following guidance is provided:

Access requirement	Guidance
Establish access rights for staff	<ul style="list-style-type: none"> • Access to records is based upon needs determined by functions undertaken by staff, not by seniority. • Manager must establish access rights for staff to records documenting their activities. • Staff shall be allotted access rights to the records of the business activity/ies they require to conduct their job. • All staff and contractors are permitted to access and view records associated with their business activities.
Document access rights for staff	<ul style="list-style-type: none"> • Access permissions shall be documented and implemented through the corporate recordkeeping system.
Ensure staff know their rights and responsibilities	<ul style="list-style-type: none"> • Staff are not permitted to disseminate or provide copies of, or information from, ACT Health official records unless in line with approved business procedures. Disciplinary action or Penalties may apply. • Staff and past staff or contractors are entitled to access (and correct if required) their personnel records under Freedom of Information provisions. • Personal information will only be used to support the business activity in which it was legitimately collected.
Negotiating access	<ul style="list-style-type: none"> • Where access to ACT Health records is requested for records not normally required for the conduct of the job, or which is beyond the permissions allocated to them, such requests shall be submitted to the relevant senior manager for determination • The Chief Information Officer (in conjunction with relevant functional area Executive) make access determinations for ACT Health records.
Documenting access	<ul style="list-style-type: none"> • All attempts to access and view records are automatically logged in the corporate records management system.

Access requirement	Guidance
Monitoring access	<ul style="list-style-type: none"> All attempts to access records to which a staff member is not routinely entitled will be reported to the relevant functional area Executive for further action. Disciplinary action may result.
Determine rights for external parties to access to records	<ul style="list-style-type: none"> Members of the public, clients, customers, and any others about whom personal information is maintained, are entitled to access, and correct if required, personal information held by ACT Health under Freedom of Information provisions. All such requests are to be directed to and managed by the staff member responsible for Freedom of Information.

The **Objective Quick Reference Guide on Objective Privileges** provides information on access controls in the corporate recordkeeping system.

Requests for information

Business Units and staff should not handle requests for access to information from the public. Information must be requested through the ACT Health Freedom of Information (FOI) Officer. FOI and other information access requests from the public should be referred to the ACT Health FOI Officer for action.

When requested records are deemed to have reached the 20-year open access period and are available with no exemptions, requests will be managed by the Archives ACT Office in consultation with the ACT Health FOI Officer and Records Management team.

Information sharing

If records need to be shared with an external party and email is not appropriate, the endorsed corporate solution (normally, but not always, Kiteworks) is to be used. Further information regarding the endorsed corporate solution is on Health HQ.

The sharing of information between ACT Health and appropriate third parties can support more informed policy making, program management, research and service planning. When using the authorised platform to share information with external parties, it is important to adhere to the following recordkeeping requirements to ensure the integrity of ACT Health records:

- Ensure you are authorised to share the information, following any approved business procedures,
- Ensure records have been captured in Objective prior to sharing with external parties.
- If you are working collaboratively on a document with external parties ensure major versions or significant changes to the content of the record are captured in Objective.
- Ensure sharing of information is done in accordance with ACT Health privacy policies.

Note: It is important to remember that the file sharing application does not retain information long term so records must also be saved in Objective.

Retention and disposal

The *Territory Records Act 2002*, states Agencies must not:

- a) abandon or dispose of a record; or
- b) transfer or offer to transfer, or be a party to arrangements for the transfer of, the possession or ownership of a record; or
- c) damage a record; or
- d) neglect a record in a way that causes, or is likely to cause, damage to the record.

This obligation applies to records in all formats, digital and physical.

ACT Health may only destroy records if:

- the Director of the TRO has issued an applicable Records Disposal Schedule that authorises the destruction, or
- [normal administrative practice](#) provisions apply to the information.

ACT Health is subject to the following Records Disposal Schedules

Schedule name	Date Effective	Instrument No
Finance and Treasury Management Records	27 February 2017	NI2017-83
Government and Stakeholder Relations Records	27 February 2017	NI2017-84
Health Treatment and Care	8 December 2017	NI2017-629
Human Resources Records	27 February 2017	NI2017-79
Information and Communications Technology Records	27 February 2017	NI2017-85
Patient Services Administration	24 December 2013	NI2013-590
Population Health Care Management & Control	8 May 2009	NI2009-209
Property Equipment and Fleet Records	27 February 2017	NI2017-86
Public Health Protection	29 March 2019	NI2019-161
Records and Information Management Records	27 February 2017	NI2017-87
Solicitor and Legal Services Records	27 February 2017	NI2017-88
Converted or Digitised Source Records	21 July 2020	NI2020-435
Strategy and Governance Records	27 February 2017	NI2017-89
Student Management	14 October 2016	NI2016-568
Training and Tertiary Education Records	7 July 2015	NI2015-363

Schedule name	Date Effective	Instrument No
Preserving records containing information that may allow people to establish links with their Aboriginal and Torres Strait Islander heritage	25 March 2011	NI2011-162
Protection of records relevant to the Royal Commission into Institutional Responses to Child Sexual Abuse	1 February 2013	NI2013-42

Normal Administrative Practice

ACT Health generates a significant amount of material in daily operations including some of which is of little value to the organisation, today or in the future. Normal Administrative Practice (NAP) allows agencies to destroy certain types of low-value and short-term records in the normal course of business.

NAP sits alongside TRO disposal permissions provided through records authorities. NAP cannot be used to dispose of information that is, or should be, covered in a records authority. NAP is only applied to business information not covered (and does not need to be covered) under a records authority such as duplicates, transitory material, externally published material, and unofficial information. In other words, information that is not needed to document the business of ACT Health. This type of information can be destroyed in accordance with a NAP without formal permission from TRO.

By letting staff, contractors and consultants destroy certain types of information NAP helps ACT Health manage information efficiently while meeting the requirements of the Act. This means:

- NAP allows ACT Health to reduce the amount of unnecessary information it holds;
- high value business information is more accessible as systems are not over burdened with low value or ephemeral information;
- savings can be made on storage costs;
- staff are provided clear guidance to enable them to make NAP decisions.

In the course of carrying out administrative business activities, various iterative processes can occur that result in the creation or receipt of facilitative or transitory information, including:

- rough working papers and background notes to support the development of other documents;
- rough notes taken prior to and/or during visits or meetings which are later either formally transcribed or referenced only by the relevant staff member;
- routine/iterative drafts which do not substantiate subsequent major drafts or final documents;
- copies of records held for temporary reference;
- published material acquired for reference purposes;
- global email messages and notifications received regarding business activities and operations, or circulation copies of ACT Health instructions, procedures, circulars or newsletters;
- informational material received from other agencies or organisations including catalogues, price lists, promotional materials etc.;
- transitory messages giving minor instructions of a trivial nature only to further a more specific activity (e.g., telephone messages);
- documents created in error, or which do not proceed to become official records.

Below are some specific examples of the type of information to which NAP can be applied within ACT Health.

Examples of NAP records

Items that can be destroyed according to NAP	Included (DESTROY under NAP)	Excluded (DO NOT destroy under NAP)
Routine correspondence and informal communications	<ul style="list-style-type: none"> • Emails that facilitate an action but do not provide evidentiary value such as, emails regarding meeting reminders • Personal communications • 'for your information' messages and 'with compliments' slips • Listserv messages • Voice mail, text messages and chats in MS Teams that do not document business • System reminders • Alerts • Bounce backs • Parts of an email thread where the full thread is saved in a system with appropriate information management functionality • Emails that were sent to multiple recipients, one of whom is responsible for capturing the message into a business system with appropriate information management functionality • Un-used forms 	<p>Emails communications that document:</p> <ul style="list-style-type: none"> • The delivery of a business record to an internal or external stakeholder • Provide evidence of an approval or of an action • Discussions with senior management, external bodies, providers, participants and industry professionals that contain decisions, guarantees, advice regarding key course of action, legal and financial matters and key work processes
Working & background information	<ul style="list-style-type: none"> • Rough working notes taken during meetings, video / telephone calls that are not intended for further use or circulation to others and where key decisions and outcomes are formally captured • Working papers that support development of drafts and have no further value after the document has been produced • Documents incorporated into a final document • Spreadsheets, system printouts for calculations or to verify data that do not form part of final documents where the decisions behind the calculation methodology are documented elsewhere 	<ul style="list-style-type: none"> • Working documents that contain significant decisions, reasons and actions or contain significant information that is not in the final document • May need to be used to support or provide evidence of processes and activities • Document a change in the development of the final product
Drafts	<p>Draft documents that:</p> <ul style="list-style-type: none"> • Are not intended for further use • do not contain significant comments and feedback from other parties • do not become official records of business activities and not intended for further use or reference 	<p>Major drafts formally circulated internally or externally for review, comment, and consultation and which incorporate substantial input for legal, senior management or external stakeholders. For example;</p> <ul style="list-style-type: none"> • agreements

Items that can be destroyed according to NAP	Included (DESTROY under NAP)	Excluded (DO NOT destroy under NAP)
	<ul style="list-style-type: none"> that are routine and only used to develop or complete other documents for internal circulation or external release 	<ul style="list-style-type: none"> high level plans, strategies or reports. ACT government submissions
Duplicates or copies	<p>Duplicate copies of records held for reference/information purposes where the original / master has been captured elsewhere in ACT Health systems. Includes:</p> <ul style="list-style-type: none"> Circulation copies of agency instructions, meeting minutes, advice distributed to staff Copies of documents where the original has been sent to another business area for processing e.g., invoices Electronic documents or emails captured in Objective. Once an electronic document or email has been saved into Objective, the resulting record in Objective is the corporate record. The copy on the network drive or in Microsoft Outlook can be considered a duplicate Convenience copies of procedures, guidelines or reports Copies of records held in personal drives Internal newsletters Emails received by secondary recipients (cc'd) for reference, but which are required to be actioned by the primary recipient 	<ul style="list-style-type: none"> The master copy or original of any ACT Health business record, kept by the creator, primary recipient, or person responsible for processing / actioning
External publications	<ul style="list-style-type: none"> Published materials and resources produced by external parties and held by ACT Health for reference only. 	<ul style="list-style-type: none"> Master copy / original of publications produced by ACT Health
Promotional Material	<ul style="list-style-type: none"> External catalogues Junk mail (SPAM), unsolicited offers for goods and services etc. Unsolicited promotional material that has no value to ACT Health 	<ul style="list-style-type: none"> Promotional material developed by ACT Health Promotional material that may support / validate decisions.
Invitations, Appointment diaries and calendars	<ul style="list-style-type: none"> Staff invitations, appointment diaries and calendars used to record routine day-to-day operations and activities such as office outlook calendars. 	<ul style="list-style-type: none"> Where accountability requires a record of meeting with contacts Recording of important events and attendance. Diaries belonging to the Director General
Unofficial information	<ul style="list-style-type: none"> Unofficial personal email 	
Empty files that were created in error or in anticipation of a proposed project or action that did not occur		

It is important to consider the **nature and sensitivity** of a record deemed as able to be destroyed under NAP. Please consider any privacy implications and **shred** records (or place in a secure wastebin) prior to disposal.

Records disposal

Records disposal is not just the destruction of records. Disposal is a range of processes, as described below

Disposition Process	Guidance
Destruction	<p>Ensuring records are destroyed so they are no longer useable or accessible.</p> <ul style="list-style-type: none"> the physical destruction of carriers of digital information such as hard drives or discs. Destruction of digital information by purging or overwriting email, documents or data in business systems. Physical destruction of paper records <p>Digital information is not destroyed by deletion.</p>
The transfer of its custody or ownership	<ul style="list-style-type: none"> Information is transferred to another Agency in a machinery of government change. Where an agency is merged with another agency Business functions are transferred to / from another government jurisdiction or the agency is privatised. donation to a community or appropriate group. Transfer of ownership must be authorised by the Director of Territory Records Office 3
Archiving	<ul style="list-style-type: none"> Records designated as “Retain as Territory Archives (RTA)”. These records must be kept and stored to ensure continued access and availability.
Damage or alteration	<ul style="list-style-type: none"> Damage or alteration changes the record and needs to be approved as a disposal action. Alteration could occur during a system migration.
Transfer to secondary storage	<ul style="list-style-type: none"> Hardcopy records that are not in day-to-day use may be transferred to secondary storage facilities.

Physical records

Where a business unit has physical records to be managed the Records Management Team must be contacted to discuss the collection of physical records. Requests can be made via [JIRA Assist](#).

The Records Management Team will arrange to prepare the records by cataloguing and boxing, and transfer them to the storage repository.

The following process should be referred to when Business Units either want to return recalled records or request records from Records Management, Mitchell.

3 Territory Records Office, Records Advice, Overview of disposal and destruction of ACT Government records, information and data.

Recall / retrieving physical records

Physical records in storage can be retrieved at any time prior to their destruction by completing the **Paper File Retrieval Request** form in [Jira Assist](#).

Request for urgent records will be actioned within 1 working day. Non urgent records will be actioned within 5 working days.

Any requests to Records Management for records shown as being in the possession of another business area will be directed to that business area and current holder.

Delivery of retrieved records

Single records or up to 2 boxes will be sent via the ACT Government internal mail service (ACT Shared Services Records Services) to the local distribution / collection point.

Large numbers of records, or records deemed highly sensitive or records required urgently, will otherwise be delivered directly to a Business Unit by the Records Management team.

Preservation

Digitisation of paper records

ACT Health digitises paper records:

1. convert hardcopy documents to a digital format as part of normal business processes;
2. to provide easier access to older physical records; and
3. to reduce the physical holdings of long-term retention records in paper format.

Business Process Scanning

All documents received in paper format that result from or relate to a business activity can be scanned. This includes documents received by individual staff members or through normal mail and courier services. It excludes documents received solely for information such as catalogues, advertisements, flyers for conferences and the like.

Scanning of documents received is done using the multi-function devices. These devices have scanning settings verified to meet recordkeeping requirements for technical compliance with TRO guidance.

Once scanned a document is automatically sent to your email. The scanned image must then be captured to the appropriate location in Objective.

Business staff scanning records MUST ensure:

- The quality of the scan is adequate, that is:
 - The text and detail of the document is legible
 - The image is upright, not skewed or incorrectly centred.
 - Is the dimension clear – if a document has been reduced/enlarged for scanning, are the dimensions of the original clearly identifiable.
 - Is the image cropped or incomplete (image completeness).
 - Are the original colors preserved (color fidelity)?

- Documents are scanned individually not together.
- Documents are provided with a title in line with the naming conventions guidance.

If the above requirements are met the original paper document can be destroyed. The scanned image will become the record on which any action will take place.

Access to older records

Where business teams have physical records that require scanning the Records Management Team provides a scanning service so that access to older, high value records is improved. The **Paper File Digitisation Request Form** must be completed. Once completed the Records Team will contact the requesting officer to discuss requirements and arrange for the files to be scanned and then captured in the appropriate location in Objective.

Once records have been digitised, quality control checked and captured into Objective the source (hardcopy) records can be disposed of in accordance with the requirements as set out in the Converted or [Digitised Source Records RDS \(NI2020-435\)](#), [TRO Records Advice](#), [Digitisation and disposal of Source Records and ACT Health requirements](#).

Monitoring the scanning process

The Records Management team will undertake quality assurance to ensure the quality of digitised records scanned by the team is maintained. Records of any problems or remedial actions recommended will be maintained to demonstrate the compliance of their scanning process with best practice, and therefore to enable defense of digital records. The Records Management team will work with business teams to ensure quality of digitised images are captured as records.

Digitisation technical specifications

When digitising records technical specifications must be adopted to satisfy requirements for destroying source records after digitisation. The requirements are designed to ensure a digitisation effort results in the creation of a full and accurate copy of the physical original. The TRO provides advice on the digitisation of records and the minimum technical requirements. Please refer to [TRO records advice](#), Digitisation Technical Specifications.

Business Systems Assessment and Planning

The TRO provides a tool for ACT Government organisations to assess systems against recordkeeping requirements and standards to determine the suitability of business systems for managing records, particularly records that are of high value and high risk to the organisation. The business system assessment tool enables ACT Health to better manage information through:

- assessing records, information and data risks and values;
- identifying systems functionality required to manage records and data appropriately;
- providing solutions to address gaps in systems ability to manage records, information and data;
- manage the migration of records and data from one system to another;
- plan for system decommissioning to ensure records remain accessible for as long as required; and
- ensuring greater accountability and transparency.

Refer to [Appendix 1](#) for the assessment tool.

The assessment of business systems as part of ACT Health records management program ensures the system register is kept up to date and that records management requirements met.

Records management arrangements with outsourced service providers

Outsourced arrangements where the provider captures, creates, receives or manages records that are the property of the Directorate must explicitly outline to the provider the requirement to manage these records in accordance with the *Territory Records Act 2002* and in accordance with ACT Health recordkeeping practices and requirements.

Implementation

This procedure will be implemented and communicated to the Directorate through the Records Management intranet page.

References and Related Documents

References

- AS ISO 15489-1:2016 - Information and documentation — Records management — Part 1: Concepts and principles
- SA/SNZ TR ISO 26122:2008 – Work Process Analysis for Recordkeeping
- AS: 5044-2010 - AGLS Metadata Standard.
- AS/NZS 5478:2015 Recordkeeping Metadata Property Reference Set.
- ISO: 16175-1:2020 - Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records
- The Territory Records Office Standard and Guidelines for Records and Information Governance

Legislation

- *Territory Records Act 2002*
- *Dangerous Substances ACT 2004*
- *Freedom of Information Act 1989*
- *Evidence Act 2011*
- *Information Privacy Act 2014*
- *Health Records (Privacy and Access) 1997*
- *Electronic Transactions Act 2001*
- *Financial Management Act 1996*
- *Medicines, Poisons and Therapeutic Goods Act 2008*

- *Public Sector Management Act 1994*
- *Radiation Protection Act 2006*
- *Work Health and Safety Act 2011*
- *Working with Vulnerable People (Background Checking) Act 2011*

Supporting Documents

A range of policies relevant to the management of records must be applied alongside this policy, including:

- ACT Government's Open Government Policy
- ACTPS Digital Records Policy
- ACT Government Policy on the Selection and Implementation of Electronic Document and Record Management System (EDRMS) Capabilities

Definitions

Term	Definition
Clinical Record	Also referred to as a “Health Record”
Business classification scheme (BCS)	A conceptual representation of the business functions and activities performed by an organisation. Represented as a hierarchical scheme for identifying and defining the functions, activities and transactions an agency performs in the conduct of its business, and the relationships between them. Also referred to as a “Thesaurus”.
Digital Record	A record that is communicated and maintained in a digital format. Same as an electronic record.
Disposal	<p>A range of processes associated with implementing decisions such as retention, damage or alteration, deletion or destruction of records. Disposal may also include the migration or transmission of records between systems, and the transfer of custody or ownership of records.</p> <p>Disposal of a record, includes the deletion or destruction of the record from a recordkeeping system.</p>
Health Record	<p>Means any record, or any part of a record:</p> <p>(a) held by a health service provider and containing personal information; or</p> <p>(b) containing personal health information</p>
Metadata	Structured descriptive data that must be captured in a recordkeeping system to enable a record to be understood, verified, managed and used. It is data describing context, content and structure of records and their management over time.
Normal Administrative Practice (NAP)	A process that allows agencies to destroy certain types of low value and short-term information in the normal course of business.
Electronic document and records management system (EDRMS), Objective	Objective is the corporate recordkeeping system for ACT Health. Objective is designed to capture, manage and protect business information in order to ensure access to authoritative records and meet governance and regulatory compliance obligations.
Records	Information created, received, and maintained as evidence and information by an organisation or person, in

Term	Definition
	pursuance of legal obligations or in the transaction of business (AS ISO 15489)
Records Management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (AS ISO 15489).
Records Management Program	A records management program is implemented in ACT Health in compliance with section 16 of the Territory Records Act 2002. The program is documented which describes the means by which ACT Health will manage its records. The program is approved by the agency's Principal Officer (Director-General).

Version Control

Version	Date	Comments
0.4	20 July 2022	Draft for consultation
1.0	8 August 2022	Updated and finalised draft

Disclaimer: *This document has been developed by the ACT Health Directorate specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and the ACT Health Directorate assumes no responsibility whatsoever.*

Attachment

Attachment 1 – Business Systems and Digital Recordkeeping Functionality Assessment Tool

Attachment 1:

Business Systems and Digital Recordkeeping Functionality Assessment Tool, Territory Records Office

BUSINESS SYSTEMS AND DIGITAL RECORDKEEPING FUNCTIONALITY ASSESSMENT TOOL

Note: The use of this tool does not constitute an endorsement of the systems being assessed. It is for assessing systems according to recordkeeping requirements in order to determine system suitability.

It is standard practice for agencies to adopt business systems that conduct significant business transactions and frequently these systems are not able to perform as recordkeeping systems, even though they are designed to capture and maintain ACT Government records. The Business Systems and Recordkeeping Functionality Assessment Tool is a checklist which allows an agency to undertake a detailed assessment of the existing recordkeeping functionality of their current business systems and aligning it with the principles of Territory Records Standard – Number 6: Digital Records.

Territory Records Standard – Number 6: Digital Records states that compliant agencies will incorporate digital recordkeeping into business processes and tools. This Standard explains that there are records which should be retained in a digital capacity in order to retain their content, context and structure. Records created and managed within a digital recordkeeping system fit into this category of best retained in their native environment.

The assessment has been broken up into the following sections:

- **Recordkeeping Requirements**
- **Business System Requirements**
- **Metadata Requirements**
- **Risk Management Requirements**

A checklist of the six essential descriptive elements from Territory Records Standard – Number 3: Description and Control against the business system should be included as part of Section 4 of the agency's Records Management Program. The Business Systems and Digital Recordkeeping Functionality Assessment Tool is

the next step to understanding the overall compliance of the recordkeeping functionality of business systems identified as supporting ACT Government records in a digital environment.

SYSTEM TO BE ASSESSED	
Date of assessment	
Assessed by	
System name and version	
Summary of the business activities the system supports	
Business owner	
System administrator(s)	

Criteria assessment measures

Yes = the system complies with the requirement

Currently not available – could be done with change to the system configuration and/or procedures = A gap has been identified but can be remedied. An action should be given explaining how.

No – system is not capable = The system is not able to meet the requirement. Risks should be identified for not being able to develop or enhance the system to comply.

Section 1 - Recordkeeping Requirements

Recordkeeping requirements create a framework to accountably manage records and other business information. The requirements are derived from regulatory sources, business needs and community expectations that govern how records are created, captured, maintained for evidential purposes, accessed and disposed of.

Criteria	Description	Assessment	Comments / Actions
<p>1.1 <i>Has the business system been identified as capturing records?</i></p>	<p>The business system has been identified as capturing digital records.</p> <p>Policy, procedures and business rules that dictate how and what records should be captured into the system are available.</p> <p><u>NOTE: If the business system has been identified as not capturing ACT Government records, there is no need to proceed with the assessment.</u></p>	<p>Yes</p> <p>No</p>	

Criteria	Description	Assessment	Comments / Actions
<p>1.2 <i>Has a Function and Activity classification from the Whole of Government Thesaurus of Recordkeeping Terms been identified for records captured in the business system?</i></p>	<p>The function and activities of records captured have been identified against terms in the <i>Whole of Government Thesaurus of Recordkeeping Terms</i>.</p> <p>Classification places records into their business context. The whole of government classification scheme is provided in the <i>Whole of Government Thesaurus of Recordkeeping Terms</i>.</p> <p>The Thesaurus is directly linked to the functional <i>Whole of Government Records Disposal Schedules</i> required for the sentencing and disposal of all records of the Territory, regardless of format and storage location.</p>	<p>Yes</p> <p>No</p>	<p>Function:</p> <p>Activity/Activities:</p>

Criteria	Description	Assessment	Comments / Actions
1.3 <i>Is the business system involved in supporting high risk business activities?</i>	<p>Business systems required to support high risk activities carried out by the agency are known and their recordkeeping functionality assessed.</p> <p>Examples of high risk business activities could include:</p> <ul style="list-style-type: none"> • regular, routine and/or direct contact with individuals • impacts on individual’s rights and entitlements • the creating and managing contracts or legal agreements on behalf of the ACT Government • processes that are considered open to corruption • significant or major agency projects or programs • significant investments to the economy. 	<p>Yes</p> <p>No</p>	
1.4 <i>Does the business system contain records that will be of long term value or deemed to become Territory Archives?</i>	<p>Records determined to be long term temporaries or eventually becoming Territory Archives have been identified.</p> <p>Records that are required to be retained for long periods, or permanently, will require more stringent controls that will ensure they remain assessable.</p> <p><i>Refer to Criterion 2.9 – Can the business system manage disposal of records in a managed, systematic and auditable manner?</i></p>	<p>Yes</p> <p>No</p>	

Criteria	Description	Assessment	Comments / Actions
1.5 <i>Has this business system replaced a previous business system or systems?</i>	Previous systems that have performed the same requirements of the current system existed. These systems may still hold related records that may need to be managed or migrated.	Yes No	

Section 2 - Business System Requirements

Business system requirements ensure that the overall governance and required software components of a business system are managed, available and used efficiently.

Criteria	Description	Assessment	Comments / Actions
2.1 <i>Is there an established business owner for the business system?</i>	The business system has a known business owner who is responsible for the overall care and management of the business system.	Yes No	
2.2 <i>Is the business system well documented?</i>	Documentation of the business system's configuration, metadata schema, data dictionaries, any system customisation and/or enhancements is available. Documentation is needed to understand and manage the information within the system as well as to assist with any necessary system migration or record export.	Yes No	

Criteria	Description	Assessment	Comments / Actions
<p>2.3 <i><u>If applicable:</u></i></p> <p><i>Is the migration of records from one business system to another controlled and fully documented?</i></p>	<p>The migration of records from predecessor systems, including upgraded versions of the same system, must be planned and carried out in a controlled manner to minimise the risks associated to loss or corruption.</p> <p>Migration plans include:</p> <ul style="list-style-type: none"> • processes used to physically carry out the migration between business systems; • the identification and mapping of metadata migrated and how it is persistently linked to records; • details regarding any changes or manipulations to records and their metadata necessary during the migration process; • migration processes are tested before implementation into live system; • records are maintained post migration. 	<p>Yes</p> <p>No</p> <p>Not applicable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>2.4 <i>Does the business system manage access controls on metadata elements and business rules?</i></p>	<p>The business system is able to provide restrictions on users being able to edit metadata elements and business rules applied.</p> <p>The alteration, deletion or addition of metadata elements should be controlled by administrative users only. This maintains the integrity of the business system and therefore greater accountability of business operations. The requirements for appropriate metadata should be fully mapped before implementation.</p> <p>The creation of ad hoc metadata without full consideration can mean costly and/or time consuming remediation which can potentially limit the useability, integrity, manageability and effectiveness of the overall data within the business system.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
<p>2.5 <i>Does the business system manage access controls that, if required, can restrict or permit access to the defined records by specified individuals or groups?</i></p>	<p>Information security and protection mechanisms should be in place.</p> <p>Business systems should have safeguards which provide access controls to how records are managed within the system. Limits can be imposed that only allow users with appropriate permissions to access records in particular ways (e.g. viewing, printing, editing, copying, transmitting).</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>2.6 <i>Does the business system have an audit log of any actions and activities performed in or by the system?</i></p>	<p>The business system maintains an audit log of changes or additions made to records.</p> <p>An audit log should be maintained to identify which users have accessed records as well as any actions performed on or by the system.</p> <p>Audit logs give the ability to detect breaches of security, the inappropriate alteration or deletion of records and ensure that actions are being carried out according to assigned roles and responsibilities.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
<p>2.7 <i>Does the business system capture full and fixed records in a variety of file formats?</i></p>	<p>The business system is capable of capturing full and fixed records in a variety of file formats.</p> <p>Hardcopy systems are required to handle multiple formats of physical records. Business systems need to be able to have the same ability to capture records in a variety of formats. The business system should allow users to capture and store records received by the system in their native format.</p> <p>Business processes are increasingly being carried out online and the information created by these activities may be the only evidence available of some transactions or decisions.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>2.8 <i>Does the business system identify the software application used to create each record?</i></p>	<p>The business system is able to identify software applications used to create records.</p> <p>The application name and version used of all software applications are required to assist in accessing records at risk of software obsolescence. Identification can be defined at:</p> <ul style="list-style-type: none"> • the system or module level where data is unstructured and created using the same application; • the system or module level where all records are structured and created through the same application; and • the individual record level where a variety of digital objects have been captured. 	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
<p>2.9 <i>Does the business system retrieve and display records in a human readable form?</i></p>	<p>Business systems need to present data and other document objects in a form which allows for human viewing that is easily understood. This can be on screen, as an exported or printed document/extract, or other suitable method.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>2.10 <i>Does the business system produce reports on or about records in the business system, including their management?</i></p>	<p>The business system is able to produce reports on or about records in the business system, including their management.</p> <p>The business system should have the ability for administrators and users to query and create reports on the actions carried out on records, including the aggregation of records. Reports are required as part of the records management for the monitoring of records related responsibilities such as use patterns, sentencing and destruction activities.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
<p>2.11 <i>Does the business system create and maintain links between records and metadata that show the content, context and structure of the records?</i></p>	<p>Links between records and metadata that give the content, context and structure of the records can be created and maintained.</p> <p>For information to be capable of functioning as a record there needs to be additional descriptive data that connects it to the business and computing environment in which it is created and used – this is called metadata. Metadata allows for the identification, authentication and contextualisation of records for as long as they need to be kept.</p> <p>Business systems must demonstrate all records are assigned at least a minimum level of metadata. Metadata can be applied automatically or manually to the records.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>2.12 <i>Can the business system ensure the interoperability of records across platforms and domains of use over time?</i></p>	<p>The business system ensures the interoperability of records across platforms and domains of use over time.</p> <p>Interoperability means the business system will work with other systems or products. Records will often need to be kept beyond the life of the hardware and/or software used to create them. Records should always be readable and able to be converted, where necessary, for migration to other technology platforms.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
<p>2.13 <i>Is there an upgrade strategy for future development of the business system in place?</i></p>	<p>An upgrade strategy for the business system has been developed.</p> <p>An upgrade strategy provides a plan for the continuation of the business system. In many instances, the records contained in the business system will be required beyond the potential ‘life’ of the software application.</p> <p>The upgrade strategy provides for an evaluation of the expected lifespan of the current business system and how any future transitions (e.g. to new versions of the software) will occur.</p>	<p>Yes</p> <p>No</p>	

Section 3 - Metadata Requirements

Metadata, whether point of capture or associated with subsequent processes, ensures authenticity, reliability, usability and integrity over time and is an inextricable part of records management. Metadata fixes the record into its business context and establishes proper control.

Criteria	Description	Assessment	Comments / Actions
<p>3.1 <i>Does the business system create a unique identifier for each record?</i></p>	<p>A unique identifier is created for each record generated within the system.</p> <p>A unique identifier can be an identification number, alphanumeric code or serial number applied to the record.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
<p>3.2 <i>Does the business system capture a title for each record?</i></p>	<p>An appropriate, meaningful description explaining what each record is about is captured.</p> <p>The description may be known as the Title field or Subject field but both serve the same purpose.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
3.3 <i>Does the business system capture the date each record was created?</i>	<p>The date of when each record is created or captured into the system is provided.</p> <p>For object based records added to the system, the creation date may not necessarily be the same as the date in which it was captured.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	
3.4 <i>Does the business system identify who or what process creates and edits records?</i>	<p>The business system identifies the person, process, or system that creates and edits records in the system.</p> <p>An audit log of individuals or other forms of creating (e.g. migration process) and editing mechanisms, is maintained to ensure authenticity and integrity of records.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>3.5 <i><u>If applicable:</u></i> <i>Does the business system identify records migrated into the system from other systems?</i></p>	<p>Where records have been migrated from predecessor business systems the current business system indicates this previous history, including the date the migration occurred.</p> <p>The business system needs to ensure that any metadata elements carried over from predecessor systems remain linked to each record throughout their existence. Also, records that have been destroyed within predecessor systems and have identifiers of their existence and destruction are carried over.</p> <p><i>Refer to Criterion 4.4 – Is the migration of records from one business system to another controlled and fully documented?</i></p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>3.6 <i>Does the business system allow for the application of disposal actions and triggers to records?</i></p>	<p>The business system allows for the application of disposal actions and triggers to be applied to records.</p> <p>Business systems need to be able to accommodate the disposal of records in a systematic and accountable way that is consistent with mandated records management practices. The destruction of records should be distinguishable from an ad hoc deletion so that destruction is carried out only by authorised users.</p> <p>Business system should allow for the appropriate sentencing (preferably on creation) which will lead to the eventual disposal of records. Disposal triggers in the <i>Whole of Government Records Disposal Schedules</i> vary so they should be based on active metadata of the records (e.g. date last actioned/modified). All records within a business system may well have the same disposal action as the records are all the same so the disposal action can be applied to the whole business system. But there may be business systems that contain records with a selection of record classes so disposal processes will need to be applied at the record level within the business system itself.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>3.7 <i>Does the business system allow for the review of disposal actions and triggers?</i></p>	<p>The business system allows for the review of disposal actions and triggers.</p> <p>The value of records can alter over time, providing a different purpose for maintaining a record longer than the originally intended business purpose. As a result, reviews of disposal actions should be able to be conducted.</p> <p>Any disposal freezes placed on records should be able to be applied to records within the business system. The hold on disposal actions should also be able to be applied for events including impending litigation or the receipt of a discovery order.</p>	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Criteria	Description	Assessment	Comments / Actions
<p>3.8 <i>Does the business system identify that a record was destroyed (deleted) from the system?</i></p>	<p>The business system identifies all records which have been destroyed under lawful means.</p> <p>Identifiers should remain when a record has been destroyed from a business system, including:</p> <ul style="list-style-type: none"> • The date each record was destroyed from the system is captured. There will be an authentication that records were retained for the minimum retention period as dictated under class disposal triggers. • The identity of who undertook the destruction process. It is recommended that automated bulk destruction based on pre-defining coding is not used due to risks related to inappropriate destruction of records. • The authority (i.e. RDS and class number) under which the record was destroyed is provided. This may be held in a manual system outside of the business system. 	<p>Yes</p> <p>Currently not available – could be done with change to the system configuration and/or procedures</p> <p>No – system is not capable</p>	

Section 4 - Risk Management Requirements

Risk management requirements are designed to reduce or eliminate the risk of certain kinds of events happening or having an impact on the business system and its captured records.

Criteria	Description	Assessment	Comments / Actions
4.1 <i>Are risks associated with recordkeeping and the business system identified?</i>	<p>A risk assessment has been carried out to identify and mitigate possible low, high and acceptable risks associated with recordkeeping and the business system.</p> <p>The risk assessment may be included in the agency's risk register or a risk management plan.</p>	<p>Yes</p> <p>No</p>	
4.2 <i>Is a risk treatment plan available to minimise risk to recordkeeping and the business system?</i>	<p>A risk treatment plan is established outlining how risks will be managed. Treatment plans are implemented and regularly reported on.</p> <p>The risk treatment plan may be included in the agency's risk management plan.</p>	<p>Yes</p> <p>No</p>	

Criteria	Description	Assessment	Comments / Actions
4.3 <i>Has the business system been identified to contain vital records?</i>	<p>Vital records are records considered essential to the continuing operation of the agency in the event of a disaster and will have severe consequences to the agency if they are completely lost or destroyed. If they are able to be recreated from other sources in any way, they will most likely be costly and time consuming to do so.</p> <p>Vital records predominately document the agency's legal and financial position as well as being critical for preserving the claims, rights and entitlements of individuals.</p>	<p>Yes</p> <p>No</p>	
4.4 <i>Is there an established framework for responding to disasters affecting the business system?</i>	<p>Counter disaster measures for the business system have been established and are documented.</p> <p>Disaster planning includes disaster prevention, response, salvage and recovery. Vital records should be known and identified within the agency's disaster management plan. The plan should be regularly reviewed and updated to reflect the current environment.</p>	<p>Yes</p> <p>No</p>	

Criteria	Description	Assessment	Comments / Actions
4.5 <i>Is regular testing done on the recovery and restoration processes of the business system?</i>	<p>Regular testing is carried out on the recovery and restoration processes of the business system.</p> <p>Regular testing ensures that recovery and restoration processes are understood and can be effectively implemented in a disaster recovery environment.</p>	<p>Yes</p> <p>No</p>	
4.6 <i>Is training provided to users of the business system?</i>	<p>Training is provided to users of the business system.</p> <p>Training should include initial training on the business system to new users and have the availability of refresher training.</p> <p>Training may need to be divided into difference categories such as user and administrator level training.</p>	<p>Yes</p> <p>No</p>	

Criteria	Description	Assessment	Comments / Actions
<p>4.7 <u><i>If applicable:</i></u> <i>Have all risks associated with storing records in a cloud environment been identified and managed?</i></p>	<p>A detailed risk assessment of the recordkeeping risks associated with cloud computing has been carried out. Risks include:</p> <ul style="list-style-type: none"> • the inability to adequately control Territory records e.g. security or privacy; • entities in another State or country may take control or claim ownership of the records; • records may not be returned upon request at the finalisation of a contractual arrangement; • the storage provider goes out of business. <p>Contracts for cloud storage arrangements need to ensure that the ACT Government has the continuing responsibility for the full management and access of any records held by the provider.</p>	<p>Yes</p> <p>No</p> <p>Not applicable</p>	