Public Sector Organisations

Standard
Secondary Document

Northern Territory Public Sector Organisations Records and Information Management Standard

Effective management of records and information underpins accountability in the conduct of government business.

23 October 2017
Version 1.1

Document details	
Document title	Records and Information Management Standard
Contact details	Office of Digital Government Department of Corporate and Information Services (DCIS) Northern Territory Government (NTG).
Date and version	23 October 2017 Version 1.1
Approved by	Lauren Jane Moss, Minister Corporate and Information Services
Date approved	2 February 2018
Document review (for example, annually)	As required.

Change history			
Version	**Date**	**Author**	**Change details**
1.0	15 June 2017	Digital Policy	Consultation draft
1.1	23 October 2017	Digital Policy	Post consultation updates

Contents

.

1 Introduction/purpose

This Standard specifies requirements for the management of Northern Territory Government (NTG) records and information. This Standard covers all information assets in any format and in any system owned or managed by public sector organisations (PSO) as defined in Section 5 of the *Information Act* (the Act).

This Standard assists chief executive officers, senior managers, system administrators, records managers, and all personnel responsible and accountable for creating and keeping evidence of the operations of a PSO.

A record is a piece of information which has been created or used by a PSO to come to a decision, formulate advice, conduct a transaction, or in some way document government business.

Records and information management support business operations and accountability requirements by ensuring the creation, maintenance, useability and sustainability of records and information needed for short and long term business operations.

2 Principles

These principles specify the core requirements for the effective management of records and information, and must be adhered to by personnel to provide accountability and transparency in the conduct of NTG government business.

i. Governance – effective management of records management systems to ensure the records of a PSO meet requirements of its regulatory environment and community expectations of accountability and transparency.

ii. Capture – records are adequately captured and stored to protect their authenticity and integrity as a full and accurate representation of the transaction(s) to which they attest, and can be depended on in the course of subsequent transactions.

iii. Discovery – the record can be readily located, retrieved, interpreted and preserved for the duration the record is required to be retained.

iv. Security – information security protects the confidentiality and integrity of records through controls on their storage, access and handling.

v. Disposal – records are disposed of in accordance with the *Information Act.*

These records and information management principles, when integrated into business policies, procedures and systems, will create reliable records and trustworthy evidence of business activity.

3 Authority

This standard draws authority from Part 9 of the *Information Act.* As required by the Act the standard has been endorsed by the NT Information Commissioner, with the Minister for Corporate and Information Services approving the Standard by notice in NT Government Gazette number G7 of 14 February 2018.

4 Scope

This Standard applies to all personnel of PSOs as defined in section 5 of the *Information Act* unless otherwise stated.

5 Responsibilities

i. Chief executive officers of a PSO have overall responsibility for ensuring that records and information management undertaken within their organisation complies with Part 9 of the Act.[1]

ii. Chief executive officers must ensure that their organisation's annual report includes a statement about compliance with the Act.[2]

iii. A PSO must keep full and accurate records of its activities and operations and must implement practices and procedures for managing its record and information resources.[3]

iv. All personnel of a PSO are responsible for ensuring that adequate records of the business they conduct on behalf of the organisation are identified and captured in records management systems as soon as possible after creation or receipt of the record.

v. All personnel are responsible for the security and integrity of the records and information they handle in their duties as an NTG employee.[4]

6 Standards

6.1 Governance

6.1.1 Governance framework

6.1.1.1 PSOs must establish governance frameworks to ensure records and information are managed in accordance with the requirements of the regulatory environment in which the PSO operates.

i. The regulatory environment can consist of legislation and regulations; mandatory standards of practice; voluntary codes of practice; and community expectations regarding sector specific accountability and organisational behaviour.

ii. A risk management approach should be taken to allow the sharing and re-use of records and information within government, the community and industry.

iii. Records and information management processes and systems should be regularly monitored and reviewed to ensure compliance with business needs and the regulatory environment.

iv. Records and information are managed in a manner which preserves their evidential integrity through system migrations and machinery of government changes.

6.1.1.2 Records must document the complete range of business undertaken by the organisation.

6.1.1.3 A custodian must be identified as the responsible officer for the management of record and information assets.

---

[1] *Information Act* s 131
[2] s 131(2) of the *Information Act (*the *Act)*.
[3] s 134 of the Act
[4] Office of the Commissioner for Public Employment 2011, *Code of Conduct – Employment Instruction 12.* See section 14

6.1.2 Policies and procedures

6.1.2.1 The records governance framework must include the development and implementation of policies and procedures which control the creation, capture, management and disposal of records.

i. Records and information management policies and procedures are approved by the PSO Chief Executive Officer or appropriate delegate.

ii. Records management responsibilities are described, assigned and promoted to all personnel. Appropriate records management training is provided to all Personnel.

iii. Records and information management requirements are integrated into standard operating procedures, systems and business practices to ensure records which meet the recordkeeping obligations of the organisation are created in the normal course of business.

iv. Responsibility for ensuring that records and information management is integrated into work processes, systems, and services is allocated to business owners, business units and their managers.

6.1.2.2 Contractual arrangements which a PSO enters into must include records and information management requirements, with provision for any sub-contractors to be subject to the same, where the contractor handles NTG records.

i. Agreements with service providers ensure full control and ownership by the NTG of any records or information for which a PSO is the responsible organisation.

ii. Agreements with service providers include provisions which establish management and handling conditions of NTG records and information.

6.1.2.3 All contractual arrangements which relate to the handling of personal information must hold contractors and sub-contractors to the Information Privacy Principles as defined by the *Information Act*.

6.1.2.4 All contractual arrangements which relate to the handling of sensitive or security classified information must hold contractors and sub-contractors to the same security requirements that PSOs must adhere to.

6.1.3 Records management systems (RMS)

6.1.3.1 A PSO must capture and maintain records of its business into RMS and incorporate metadata with the record at the time of the activity or shortly afterwards.

i. RMS may incorporate a combination of automated and manual systems. These systems may be centralised or decentralised.

ii. RMS are capable of using and supplying metadata to manage records in an accountable and effective way, regardless of the system or combination of systems being used, including details of hard-copy records.

6.1.3.2 Disaster recovery and other back-up systems are not RMS and must not be used or relied on to provide evidence of the activities or operations of an organisation.

6.1.3.3 The organisation must define minimum metadata requirements for the capture and management of its records appropriate to the regulatory, business or industry environment in which it operates.[5]

i. Business systems being used as RMS should be designed to capture relevant metadata automatically.

ii. Metadata is properly managed and preserved over time, including through system changes, upgrades and decommissioning.

6.1.3.4 RMS must have documented policies, assigned responsibilities and formal methodologies for their management.

i. Compliant RMS are managed to meet all requirements of the regulatory environment and arising from business and stakeholder expectations.

6.1.3.5 RMS must not allow unauthorised modifications to any records (including metadata), and where authorised modifications are performed, they must be fully documented.

6.1.3.6 When decommissioning or upgrading RMS a PSO must develop a strategy for the extraction and preservation of records in an appropriate format for migration or storage for later extraction.

i. System upgrades need to be planned and implemented methodically to safeguard the retention and usability of records for the full period of time they need to be retained.

ii. It is important to properly plan and test migration processes for records requiring long-term retention to mitigate the effects of technological obsolescence.

6.1.3.7 The RMS must incorporate business rules that avoid duplication of records.

6.1.3.8 Recordkeeping must occur in all environments in which the organisation carries out its business.

i. Business systems which hold the only evidence or record of the business activity they transact should be considered a records management system for the purposes of this standard and be managed as a records management system.

6.1.3.9 PSOs must assess and document existing business systems to address risk associated with any lack of recordkeeping functionality.

i. Business systems, having been designed and built principally to automate a particular business process, may not have all the functionality of a purpose built records management system.[6]

---

[5] Standards Australia 2006, *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*, AS ISO 23081.1:2006

[6] Specifications for recordkeeping functionality in business systems should be based on: International Standards Organisation 2010, *Principles and functional requirements for records in electronic office environments: Module 3: Guidelines and function requirements for records in business systems,* ISO 16175-3:2010(E).

ii. Records held in business systems do not all have the same risk profiles. Business systems managing high-value/high-risk records should undergo a more extensive risk assessment than systems managing low-value/low-risk records.

6.1.3.10 When new business systems are being designed and implemented, or existing systems upgraded, incorporation of records management functionality must be considered.

i. PSO Records Managers should be consulted to determine system recordkeeping requirements.

ii. Risk assessment of the level of evidence required to properly document the transactions in the business system should be used to identify any opportunities to improve records management functionality.

6.1.3.11 RMS must provide sufficient security for the long term storage and access of records.

6.1.3.12 RMS holding high-value/high-risk records must monitor and log access and event history.

6.2 Capture

6.2.1.1 The organisation must capture and manage records to ensure it can operate effectively and deliver its services.

i. Capture of records and information into records management systems is driven by the business rules and processes of the organisation.

ii. Not every piece of information created or received needs to be captured and managed. The business rules and processes should aid personnel to identify what type of information created or received is a record which needs to be captured and managed within the governance framework.

6.2.1.2 Appropriate metadata regarding a record must be captured.

i. Appropriate metadata provides meaning and context and enables the retrieval and use of records and information, supporting ongoing management.[7]

ii. Metadata defining a record's characteristics at its time of creation or capture, fixing it into the business context of the organisation, is point of capture metadata.

iii. Process metadata also accrues over time as the record is used and managed.

6.2.1.3 Unstructured information which meets the requirements of a record must be captured into a records management system to ensure the integrity of the information.

i. Unstructured information outside a records management system or on a local area network does not have strict business rules governing its use, nor business specific protections on the security and integrity of the information.

[7] Standards Australia Limited/Standards New Zealand 2015, *Recordkeeping metadata property reference set (RMPRS),* AS/NZS 5478:2015

6.3 Discovery

6.3.1 Records must be accessible

6.3.1.1 PSOs must be able to find records and information promptly, and be able to read and produce them when required for as long as they need to be retained.

i. Search precision and recall should meet the information needs of all stakeholders, including searches related to legal discovery orders and subpoenas, freedom of information requests, audits, and investigations and inquiries.

ii. Records and information are searchable, retrievable and available in open formats, including within business systems, to facilitate appropriate sharing and re-use by government, the community and industry.

6.3.1.2 PSOs must implement measures to mitigate the effects of technical obsolescence of records and information management systems, for example system upgrades and data migration programs, to preserve the usability of long term records and information.

i. Records in all formats need to be stored and maintained to ensure accessibility for the length of the retention period of the record. This includes the physical storage environment, management of control records and security.

6.3.1.3 PSOs must apply an authorised functional classification system to title or label records.

i. Classification of records by business function facilitates better control over the retention, security and disposal of records as business functions remain relatively stable through administrative and organisational changes.

ii. Classification schemes within a records management system allow for controlled titling, or the application of other meaningful tags, to records at the point of capture. A uniform classification may be applied to all records within a RMS if appropriate.

iii. Industry accepted classification schemes relevant to the appropriate discipline of the organisation may also be used to classify functional records.

6.3.2 Records must be usable

6.3.2.1 Open and technology neutral formats must be used for long-term storage and access.

i. Examples of open digital file formats are: TXT, PDF/A-1; XML; TIFF; and JPEG.[8] Adoption of open digital formats, in general, facilitates easier reuse and value-adding of the corporate information resource.

ii. Proprietary file formats should be avoided for long-term storage as vendors may discontinue support, or not provide continuity, in newer versions of software.

[8]Standards Australia 2006, Long-term preservation of electronic document-based information. AS ISO 18492-2006: See section 6.4 Migrating electronic document-based information, and section 6.4.4 Migration to standard formats, p.12

6.3.2.2 Storing records in encrypted form is not permitted and encrypted records must be decrypted before being captured into records management systems.

i. PSOs should avoid the misuse of digital (information) rights management technology and encryption. While encryption and digital signatures may have a valuable role to play in ensuring the authenticity and integrity of records in transmission, they present risks to the ongoing useability of the record as decryption keys and public keys for digital signatures may expire while the record is still required.

6.4 Security

Use of the protective markings described in Sections 6.4.3, 6.4.4 and 6.4.5 apply only to PSOs listed as an agency in the Administrative Arrangements Order, which are referred to in this standard as NTG PSOs. Other PSOs are encouraged to model their protective markings and associated handling procedures on the NTG PSO requirements if applicable.

6.4.1 Secure access to records

6.4.1.1 Records and information must be protected from unauthorised or unlawful access, destruction, loss, deletion or alteration.

i. Access to sensitive records and information should be on a need-to-know basis, i.e. information access is to be determined by whether it is required in order to perform a duty or meet a legal right or obligation.

ii. Business unit managers are responsible for determining who should have a 'need-to-know' regarding official records and information, and to allocate and document appropriate personnel security profiles.

iii. Penalties may apply if an organisation fails to store information securely and this results in a privacy breach. Penalties may apply to an individual, if the individual mishandles information in accordance with offence provisions of the *Information Act*.

6.4.1.2 Access to record and information systems must be monitored and controlled.

i. Access to official records is restricted to users with the appropriate security profile.

ii. The movement and alteration of official records is undertaken in compliance with security requirements of the records.

iii. Audit logs of records management systems are to be monitored to ensure compliance with security requirements.

6.4.1.3 All personnel accessing records and information systems must have an approved security profile mapped to the record and information systems to which they have access.

6.4.1.4 PSOs must assess the value of information contained in the records they possess and implement appropriate security handling procedures based on a risk analysis of the likely impact of unauthorised disclosure.

6.4.2 Protective markings

6.4.2.1 A protective marking must be assigned to a record identified as being sensitive or requiring a security classification, indicating the level of protection required during the use, storage, transmission, transfer and disposal of the information.

i. Appropriate protective markings for sensitive information are defined and any related handling procedures documented. Protective markings should be based on risk analysis of the likely impact of unauthorised disclosure of the information.

ii. Personnel creating a record, or actioning a record received from outside the organisation, are responsible for allocating an appropriate protective marking in accordance with approved standard operating procedures.

iii. Protective markings available for use by NTG PSOs are: Security Classifications; Dissemination Limiting Markers; and Caveats.

6.4.3 NTG PSO: Security classification system

6.4.3.1 NTG PSOs must apply the NTG Security Classification System to protect sensitive information from unauthorised access.

i. Information security in NTG PSOs is to be aligned with requirements detailed in the Australian Government's Protective Security Policy Framework (PSPF) where appropriate and applicable.[9]

ii. The NTG Security Classification System is modelled on the Australian Government Security Classification System (AGSCS) and applies to information in any format. The AGSCS is part of the PSPF.[10]

NTG security classifications aligned with the PSPF classifications:

Classifications	Comments
PUBLIC	Information which can be freely published
UNCLASSIFIED	Official information which does **not** require a security classification (though may be marked with a Dissemination Limiting Marker (DLM)). For internal NTG use only. Must be examined and deemed **public** before release.
PROTECTED (Security Classification)	Where compromise could cause damage to the national interest, organisations or individuals
CONFIDENTIAL (Security Classification)	Where compromise could cause significant damage to the national interest, organisations or individuals
SECRET (Security Classification)	Where compromise could cause serious damage to the national interest, important economic and commercial interests or threaten life.
TOP SECRET (Security Classification)	Where compromise could cause exceptionally grave damage to the national interest.

i. Security classifications are to be determined in line with the degree of protection the information

[9] Attorney-General's Department, *Protective Security Policy Framework Home Page*, Australian Government. Available from: https://www.protectivesecurity.gov.au/Pages/default.aspx

[10] Protective Security Policy Committee (approved November 2014, amended April 2015), *Information Security Management Guidelines: Australian Government Security Classification System*, Attorney-General's Department, Canberra.

in the record requires.

ii. Records should only be security classified when the consequences of compromise warrant the expense and effort of increased security protection.

iii. When a decision is made to security classify a record, an organisation should consider whether a time limit for the classification be set.

6.4.3.2 Security classifications must be applied by the originator of the document at the time it is created or received.

6.4.3.3 The default classification for documents will be UNCLASSIFIED, with the creator of the document required to assess whether an alternative classification or DLM is required.

i. The vast majority of NTG PSO records will fit into the UNCLASSIFIED classification.

ii. The classification of UNCLASSIFIED is applied to records and information not requiring a security classification. Although the information does not require a security classification it may still be of a sensitive nature which requires protection through the use of a DLM.

iii. Documents at the UNCLASSIFIED level are not open for immediate public release. A change of classification to PUBLIC is required before release or publication.

iv. UNCLASSIFIED and PUBLIC records may remain unmarked.

6.4.3.4 All Cabinet documents and associated records are to be marked as 'Sensitive: Cabinet' and carry a security classification of at least PROTECTED or higher.

i. Some classes of law enforcement information may have a minimum classification of PROTECTED.

6.4.3.5 Use of CONFIDENTIAL, SECRET and TOP SECRET classifications, which are considered national security classifications, is limited within the NTG.

i. Refer to the Australian Government guides listed as key references for more information and guidance on use of these classifications.

6.4.4 NTG PSO: Dissemination limiting markers

6.4.4.1 DLMs, other than For Official Use Only (FOUO), must be used where disclosure of the information marked by the DLM may be limited or prohibited by legislation or regulation, or other legal obligation.

i. The PSPF defines a base set of DLMs: FOUO; Sensitive; Sensitive: Cabinet; Sensitive: Legal; Sensitive: Personal.

ii. More than one DLM may be applied to documents where appropriate and justified (Exclusion: FOUO is used as a stand-alone marker only).

iii. The NTG allows the authorised definition of new DLMs if they are based on a legislative or regulatory requirement, or other legal obligation, which is dependent on the information contained in the document.

iv. A DLM should not reference the business unit responsible for the management of the

information. System access controls should be used where access needs to be limited to organisational units.

v. The "Sensitive" DLM cannot be used without an annotation that indicates the reason for the sensitive marking of the document. Annotations may specifically, or in a generic manner, reference legislation and regulations, or contractual arrangements, which require the protection of the information.

6.4.4.2 FOUO must only be used to mark UNCLASSIFED information and cannot be used in combination with another DLM.

i. The FOUO DLM can be used where no specific legislative or regulatory protection of information is required but the information is still considered sensitive.

ii. The FOUO DLM does not require an annotation as to the reason why the information has been marked.

6.4.5 NTG PSO: PSPF Caveats

6.4.5.1 NTG PSOs must refer directly to the PSPF guides for advice on caveats as the requirement within the NTG is unlikely and if used, would be very limited.

i. Caveats, when described within the context of the PSPF, are supplementary markings which indicate additional special handling requirements. Examples of caveat categories include: Codewords; Source Codewords; Eyes Only; Australian Government Access Only; Releasable to; Accountable material.

6.4.6 Reclassification and review of protective markings

6.4.6.1 A PSO must have procedures in place to review and declassify classified records.

i. Records can be reclassified if protection is no longer necessary or is no longer needed at the original level. Classifications should be reviewed when records become inactive or are transferred to secondary storage or the NT Archives Service.

ii. If a record is transmitted to another PSO, only the originating organisation (i.e., the organisation that assigned the original classification) can reclassify or declassify a record.

iii. If an organisation is abolished or amalgamated, the organisation assuming the former agency's responsibilities is deemed the originating organisation for the purpose of re-classification and declassification.

iv. Inappropriate over-classification can have detrimental effects, eg, the volume of security classified records becomes too large for an organisation to protect adequately, or the discoverability of records is impaired where the classification is unwarranted.

6.4.6.2 Records must be declassified or downgraded when protection is no longer necessary or is no longer needed at the original level.

6.4.7 Physical security

6.4.7.1 Access to areas where security classified records are held or used must be restricted.

i. All the organisation's systems, workplaces and storage areas which contain official records are to be designed and managed to protect them from unauthorised access, alteration or deletion, and personnel are aware of and follow the procedures to ensure this.

6.4.7.2 When security classified records are not in use, they must be stored in an appropriately secured environment.

i. During absences from their workplace and at close of business personnel are responsible for ensuring that records and systems are secured appropriately.

6.5 Disposal

6.5.1 Records disposal schedules

6.5.1.1 Records and information must be kept for as long as they are needed for business, legal and accountability requirements, including community expectations.

i. Records retention decisions are to be based on compliance with legal and governance requirements of the organisation, its business needs, and the needs of internal and external stakeholders, including the wider community.

ii. Appraisal of records includes assessment of their possible value as Northern Territory archives and their identification in disposal schedules as permanent value records for transfer to the NT Archives Service.[11]

iii. When records have been assigned a temporary status in accordance with an approved records disposal schedule, the defined disposal actions are the minimum length of time those records must be kept.

iv. If required an organisation may retain records for periods longer than that specified in a disposal schedule, for example when a legal hold or disposal freeze is in force, however this should be documented in agency policy and procedure.

v. If longer retention becomes an ongoing agency requirement, this should be considered in any review of the appropriate disposal schedule.

6.5.1.2 All organisational records, including records in business systems, must be covered by a current and authorised records disposal schedule.

i. Disposal schedules should be reviewed when major legislative or policy change affects the regulatory environment.

ii. Records disposal schedules do not apply to records created prior to 1 July 1978. All such records should be appraised by the Archives Service in accordance with Archives Management Standard Disposal of Government Records Created Prior to 1 July 1978.

[11] NT Archives Service, *Appraisal characteristic statement for the identification of permanent public sector organisations records*.

6.5.1.3 Records disposal schedules must be jointly approved by the Chief Executive Officer of the PSO responsible for the related function, the Director of the Records Service, and the Director of the Archives Service.

i. An approved records disposal schedule permits a PSO to retain or destroy its records in accordance with the *Information Act*.[12]

ii. Determining the retention or destruction of records requires a thorough and systematic analysis of the regulatory environment the organisation operates within and of the business activities it conducts against all records to identify minimum retention periods.

iii. The process to develop a records disposal schedule requires consultation between business unit managers and records managers from within the PSO, supported by advice from the Records and Archives Services.

6.5.2 Short-term and transitionary records

6.5.2.1 PSOs must dispose of short-term or transitory records.

i. Short-term or transitory records include: background notes; office messages; meeting requests; deliberative drafts of reports; and documents and briefs with no significant impact upon the final product or decision.

ii. Destruction of these records is permitted because they are duplicated or incorporated into records captured elsewhere, or are for short-term use only, and have little or no evidential or historical value. This routine destruction of ephemeral and facilitative information is referred to as normal administrative practice.

iii. Destruction of records of this nature, which have been captured into a records management system requiring the definition of a disposal class, is permissible using the *Disposal Schedule for Records of Short Term Value*.[13]

6.5.3 Disposal of records

6.5.3.1 PSOs must dispose of records and information in accordance with the provisions of the *Information Act* and be able to prove such action has been performed with due regard to the business, legal and governance requirements, as well as community expectations.*[14]*

i. Implementation of the provisions of a disposal schedule (sentencing records for destruction or transfer) needs to be approved, systematic, planned and documented.

ii. Where records are sentenced for transfer to the NT Archives Service, standards and procedures issued by the NT Archives Service are to be followed.

iii. Whatever the format of records due for destruction, the appropriate level of security for the records is to be observed until they are completely destroyed. Destruction certificates or other evidence of destruction are to be obtained and retained by the PSO.

iv. The PSO is to ensure that whenever destruction is permitted by a current and authorised

[12] *Information Act* s 145(2)(b)
[13] NT Archives Service 2003, *Disposal Schedule for Records of Short Term Value, No.2003/10*
[14] *Information Act* s 145

records disposal schedule, all copies and versions of official records are properly destroyed and are not recoverable (including electronic versions of records held in the organisation's information back-up practices).[15]

v. A PSO should ensure suitably qualified and experienced personnel manage the records disposal processes across the organisation. All personnel are to be trained in their responsibilities relating to the retention and disposal of records.

6.5.3.2 PSOs must implement procedures to ensure that records subject to a disposal freeze, discovery order or legal hold are identified and marked to ensure they are not destroyed.

i. Destruction of records in accordance with approved records disposal schedules may be suspended as a result of a legal hold or disposal freeze for records which may be, or are likely to become, the subject of investigation or litigation.[16]

6.5.3.3 All records disposal actions must be approved, fully documented and captured in the RMS.

6.5.4 Archives

6.5.4.1 Permanent records deemed to be archives must be transferred to the Archives Service in compliance with an approved current Records Disposal Schedule.

i. The Archives Service issues Standards for the management of archives and permanent records, including the transfer of permanent records to the Archives Service.[17]

7 Definitions

Term	Explanation
Archives	Records of permanent value that forms part of the Northern Territory Archives.
Archives Service	The organisation established to perform the archives functions for the Northern Territory. At the time of publication this is the NT Archives Service of the Department of Tourism and Culture.
Business system	A system which stores and manages information to automate business activities and processes, including policy, procedures and business rules governing its use.
Classification	Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system.
Contractual Arrangements	A formal agreement between two or more parties, including between PSOs. Contractual arrangements include, but are not limited to, procurement contracts, funding contracts, deeds, contracts under seal, service level agreements, exchange of letters, and grant agreements.

[15] NTG PSOs should refer to the Media Destruction Standard when disposing of records storage media.
[16] NT Archives Service; NT Records Service 2011 (Aug), *Records Disposal Freeze Policy for NT Public Sector Organisations*
[17] NT Archives Service 2007 (Aug), *Transfer of archives (*Archives Management Standard).

Term	Explanation
Custodian	The individual or agency that has the responsibility for the creation, collection, use, rule setting and integrity of the data.
Disposal	Disposal of a record includes transferring the possession or control of the record; destroying, donating or selling the record; also includes damaging or abandoning a record.[18]
Information	Knowledge communicated or received. The result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.
Information Asset	A body of information which is defined and managed as a single collection so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
Metadata	Structured or semi-structured information which serves to provide context or additional information about other information ["data about data"]. For example, information which enables the creation, management and use of records through time.
Protective Marking	Protective markings are security labels assigned to official information which indicate the minimum level of security protection required. For example: security classifications; dissemination limiting markers; caveats.
Record	Recorded information in any form (including data in a computer system) that is required to be kept by a PSO as evidence of the activities or operations of the organisation.
Records Management	An integrated framework of governance arrangements, processes, systems, and tools that enable organisations to create and maintain trustworthy evidence of business activity in the form of records.
Records Management System	A system which manages the capture, maintenance and disposal of records. Records management systems maintain evidence of business transactions in accordance with organisational policy and procedure (includes business systems which keep records). A records management system can consist of technical elements, such as software, and non-technical elements including policy, procedures, people and other agents, and assigned responsibilities
Records Service	The organisation established to perform the records functions for the Territory. (This involves standards setting and provision of advice at a whole of jurisdiction level. At time of publication this is the Digital Policy Unit of the Office of Digital Government, Department of Corporate and Information Services)
Unstructured Information	Unstructured information refers to information that is not contained within a database, or organized in some pre-defined manner, and which has no defined data structure or model giving the information context. Examples of unstructured information include word processing documents, emails, spreadsheets, and instant messages.

[18] Definition based on *Information Act* definition.

8 Glossary of Acronyms

Acronyms	Full form
DLM	Dissemination Limiting Marker
FOUO	For Official Use Only
NT	Northern Territory
NTG	Northern Territory Government
NTG PSO	Public sector organisation listed as an agency in the Administrative Arrangements Order
PSO	Public Sector Organisation as defined in Section 5 of the *Information Act*
PSPF	Protective Security Policy Framework

9 Key references

- **Australian and international standards**
    - International Standards Organisation 2010, *Principles and functional requirements for records in electronic office environments*: *Module 3: Guidelines and function requirements for records in business systems*, ISO 16175-3:2010(E).
    - International Organisation for Standardization 2016, *Information and documentation – Records management – Part 1: Concepts and principles*, ISO 15489-1:2016(E).
    - Standards Australia International 2002, *Records Management – Part 2: Guidelines,* AS ISO 15489.2 – 2002.
    - Standards Australia Limited/Standards New Zealand 2012, *Information and documentation – Management systems for recordkeeping – Fundamentals and vocabulary*, AS/NZS ISO 30300 – 2012: (ISO 30300:2011, MOD)
    - Standards Australia Limited/Standards New Zealand 2012, *Information and documentation – Management systems for recordkeeping – Requirements*, AS/NZS ISO 30301 – 2012: (ISO 30301:2011, MOD)
    - Standards Australia Limited/Standards New Zealand 2015, *Recordkeeping metadata property reference set (RMPRS),* AS/NZS 5478:2015
- ***Information Act* (NT)**
    - *Information Act*
- **Protective Security Policy Framework (PSPF) – Security classification**
    - Protective Security Policy Committee (approved November 2014; amended April 2015), *Information Security Management Guidelines: Australian Government Security Classification System*, Attorney-General's Department, Canberra.
    - Protective Security Policy Committee (approved 21 June 2011; amended April 2015), *Information Security Management Guidelines: Protectively Marking and Handling Sensitive and Security Classified Information*, Attorney-General's Department, Canberra.
    - Protective Security Policy Committee (approved 1 November 2014; amended April 2015), *Protective Security Governance Guidelines: Basic Impact Levels*, Attorney-General's Department, Canberra.