Records Management Standards for Public Sector Organisations in the Northern Territory

August 2010
Overview of the standards

**Standard 1 – Governance (including identification of records)**
*Records must be created within a managed framework*

NT public sector organisations must have a framework in place that ensures the creation, capture and maintenance of adequate records for the business they conduct. This framework should be planned, adequately resourced and made known to all staff.

**Standard 2 – Capture**
*Records must be captured into the corporate records management system*

NT public sector organisations must capture corporate records into the corporate records management system. Where this is not possible, information about the record (metadata) is to be entered into the corporate records management system.

**Standard 3 – Discovery**
*Records must be findable and accessible for as long as they are required*

NT public sector organisations need to be able to find records promptly and be able to read and produce them when required for as long as the records need to be retained.

**Standard 4 – Security**
*Records must be secure*

NT public sector organisations must create, store, use and make records available securely with due regard to permitting access to those with a genuine need to know the information in the records.

**Standard 5 – Disposal**
*Records must be disposed of systematically and accountably*

NT public sector organisations must dispose of records 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 toward the retention and disposal of records.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>1</td>
</tr>
<tr>
<td>Authority</td>
<td>1</td>
</tr>
<tr>
<td>Responsibility</td>
<td>2</td>
</tr>
<tr>
<td>Review of the standards and previous standards</td>
<td>2</td>
</tr>
<tr>
<td>Basis for these standards</td>
<td>2</td>
</tr>
<tr>
<td>Other legislation affecting records management</td>
<td>3</td>
</tr>
<tr>
<td>Other documents and publications consulted</td>
<td>4</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>4</td>
</tr>
<tr>
<td>Standard 1 Governance (including identification of records) –</td>
<td>5</td>
</tr>
<tr>
<td>Records must be created within a managed framework</td>
<td></td>
</tr>
<tr>
<td>Standard 2 Capture – Records must be captured into the corporate</td>
<td>8</td>
</tr>
<tr>
<td>records management system</td>
<td></td>
</tr>
<tr>
<td>Standard 3 Discovery – Records must be findable and accessible</td>
<td>11</td>
</tr>
<tr>
<td>for as long as they are required</td>
<td></td>
</tr>
<tr>
<td>Standard 4 Security – Records must be secure</td>
<td>14</td>
</tr>
<tr>
<td>Standard 5 Disposal – Records must be disposed of systematically and</td>
<td>17</td>
</tr>
<tr>
<td>accountably</td>
<td></td>
</tr>
<tr>
<td>Compliance requirements</td>
<td>20</td>
</tr>
<tr>
<td>Definitions</td>
<td>22</td>
</tr>
</tbody>
</table>

For information and advice, please contact:

Records Policy Unit  
ICT Division  
Department of Business and Employment  

Email: NTG.RecordsPolicy@nt.gov.au  
Telephone: (08) 8924 3847  
Facsimile: (08) 8924 3880  

The Records Management Standards for Public Sector Organisations in the NT are issued pursuant to Sections 137 and 138 of the *Information Act*. 
Introduction

Purpose
The purpose of the Records Management Standards for Public Sector Organisations in the Northern Territory is to provide policy advice at a whole of jurisdiction level which public sector organisations, as defined in the Information Act, must follow in order to underpin their business activity and comply with good governance principles and the legislative requirements of the Act.

A public sector organisation is defined in the Act as any of the following:

(a) an Agency;
(b) a Government Business Division;
(c) a Government owned corporation;
(d) a local authority;
(e) a statutory corporation;
(f) a person appointed, or body established, by or under an Act or by the Administrator or by a minister;
(g) the Police Force of the Northern Territory;
(h) a person holding an office or position under an Act;
(i) a court of the Territory;
(j) a tribunal of the Territory;
(k) a person or body declared by the Regulations to be a public sector organisation.1

An object of the Act is to promote efficient and accountable government through appropriate records and archives management by public sector organisations.2 To accomplish this the Act further states that Northern Territory public sector organisations must keep full and accurate records of their activities and operations.3

The Act also provides members of the public statutory rights of access to information created, received and maintained by NT public sector organisations (freedom of information). In addition, during the normal course of conducting their business, NT public sector organisations also collect personal information relating to individuals and this information needs to be protected and managed with due regard to the Information Privacy Principles in the Act.

Efficient records management enables the sharing and transmission of business information over time and space. It uses tools such as electronic document and records management systems, metadata and classification schemes to manage records and their links to the business context in which they were created. It also uses records disposal schedules to determine for how long records are to be retained in accordance with business requirements, the regulatory environment in which business is conducted, and broader community expectations.

Authority
These standards are issued in accordance with Part 9 of the Information Act. This is the legislative framework from which the standards are derived and provides the authority for NT public sector organisations to implement the policy advice contained herein.

The NT Information Commissioner has endorsed the standards.

The Minister for Business and Employment has approved the standards via NT Government Gazette No. G31 of 4 August 2010. The standards take effect from this date.

---

1 Information Act, s.5(1)
2 Information Act, s.3(1)(d)
3 Information Act, s.134(a)
Responsibility

In accordance with section 131(1) and (2) of the Act, the chief executive officer of an NT public sector organisation is responsible for ensuring the organisation complies with Part 9 of the Act. This includes ensuring that the organisation’s annual report includes a statement about compliance.

It is vital that the culture of the organisation reinforces the value and importance of good recordkeeping and that it is something that is a standard expectation of all staff. Such expectations need to be regularly articulated by the chief executive officer through line management channels.  

Section 134 of the Act outlines the responsibility of public sector organisations:

A public sector organisation must:

(a) keep full and accurate records of its activities and operations;

(b) implement the practices and procedures for managing its records necessary for compliance with the standards applicable to the organisation; and

(c) make arrangements for the records service and archives service to monitor the management of its records.

Consequently, all staff of NT public sector organisations are responsible for ensuring that adequate records of the business they conduct on behalf of the organisation are identified and captured for proper management into the approved corporate records management system as soon as possible after creation or receipt of the record.

The legislation also states the records service and the archives service must provide advice and training to assist public sector organisations to comply with Part 9 of the Act. The Records Management Standards for Public Sector Organisations in the NT, as well as other advice and guidelines produced by the respective services, assist organisations to fulfil their business and governance requirements with respect to managing records.

Review of the standards and previous standards

In accordance with Section 139 of the Act, these standards are to be reviewed at least once every three years.

These standards were issued following a review of the previous records management standards for the Northern Territory Government issued in October, 2003. Consequently, the following standards have been superseded and no longer apply to NT public sector organisations:

- Using the Records Management Standards
- Planning and Implementing Records Management
- Identifying and Capturing Records
- Classifying and Titling Records
- Records Security and Access
- Records Disposal

Basis for these standards

These standards are issued pursuant to Sections 137 and 138 of the Information Act.

---

Records Management Standards for Public Sector Organisations in the NT

The standards are based on the principles and guidelines in Australian Standard AS ISO 15489: 2002—Records Management.

Other national and international standards that have been consulted in the development of these standards are:

- AS/NZS 4360: 2004—Risk Management
- AS 5037: 2005—Knowledge management – a guide
- AS 5090: 2003—Work process analysis for recordkeeping
- AS ISO 15801: 2006—Electronic imaging — Information stored electronically - Recommendations for trustworthiness and reliability
- AS ISO 22310: 2006—Information and documentation - Guidelines for standards drafters for stating records management requirements in standards
- HB 171: 2003—Guidelines for the management of IT evidence

Records and information standards from other Australian jurisdictions that have influenced the development of these standards are:

- Information Standard IS40: Recordkeeping Queensland State Archives, 2009
- Adequate Records Management Standard, State Records of South Australia, 2008
- Standard No.7: Standard on Full and Accurate Records, State Records NSW, 2004

Other legislation affecting records management

As well as the Information Act, other NT legislation which may affect records management in public sector organisations includes:

- Audit Act
- Criminal Code Act
- Electronic Transactions (Northern Territory) Act
- Evidence Act
- Evidence (Business Records) Interim Arrangements Act
- Financial Management Act
- Inquiries Act
- Limitation Act
- Local Government Act
- Procurement Act
- Public Sector Employment and Management Act
• Surveillance Devices Act

• other legislation and industry regulations relevant to the unique functions and operations of each public sector organisation.

Other documents and publications consulted
Other documents and publications consulted during the development of these standards are:

• NT Public Sector Principles and Code of Conduct
• Australian Government Protective Security Manual, August 2005
• NT Government ICT Policy, End User ICT Services, May 2009
• NT Government ICT Strategic Intent (2010–2015), June 2009
• NT Government Application Strategy (2010–2015), June 2009
• NT Government Archives Management Standards
• Information Act Guideline - Locating and Collating Records, Office of the Information Commissioner, January 2007
• Information Act Guideline - Sufficiency of Search, Office of the Information Commissioner, January 2009

Acknowledgments
The Records Policy Unit, Department of Business and Employment, would like to thank staff from the following Northern Territory public sector organisations for their assistance in developing these standards:

• Office of the Information Commissioner
• NT Archives Service
• PowerWater Corporation
• Department of Housing, Local Government and Regional Services
• Darwin City Council
• CouncilBIZ
Standard 1 – Governance (including identification of records)
Records must be created within a managed framework

Policy statement
NT public sector organisations must have a framework in place that ensures the creation, capture and maintenance of adequate records for the business they conduct. This framework should be planned, adequately resourced and made known to all staff.

Explanation
Records are generated as a result of business activities and processes. They are a valuable organisational asset and their proper management supports improved productivity by enabling easy access to the information needed to make the right decisions at the right time. Records constitute the corporate memory of an organisation.

The identification and proper management of corporate records is fundamental to a well-functioning organisation. Records support business activity and provide a basis for efficient service delivery. They provide the mechanism whereby organisations can account for their decisions and actions. Records also provide evidence for the public to confirm or claim their public rights and entitlements, as well as providing individuals with evidence to justify decisions made by public sector organisations.

From a regulatory perspective, records contain information that could be

- subject to discovery in litigation;
- subject to a freedom of information request;
- used during an audit or official investigation;
- used to correct information that is inaccurate, incomplete or out of date;
- used to investigate a complaint about a breach of privacy; or
- used to determine the extent to which an organisation is complying with the privacy provisions of the Information Act.5

NT public sector organisations must be able to rely on the authenticity of the records upon which decisions are made or actions are taken. This can only be done if there is a clear and systematic framework for the making and managing of corporate records and that this framework is made known to all staff, adhered to during the normal course of business and able to withstand external scrutiny.

In its guideline Locating and collating records, (January 2007), the Office of the NT Information Commissioner states:

Searching for records relating to a [freedom of information] application can be a challenging and time-consuming activity. The task is certainly assisted by having a good records management system [framework] in place, and ensuring that it is diligently adhered to.6

A records management framework consists of defining the policies and procedures for the creation, capture and management of an organisation’s records, providing adequate resources for the implementation of the policies and procedures, and capturing and managing records in a system that has proper records management functionality, ie manages records classification, security, retrieval, tracking, disposal and version control. It also consists of training staff in implementing the procedures and using the system.

5 Information Act, s.86(1)(e)
6 Website of the Office of the NT Information Commissioner, accessed 27 October 2009
Implementation advice

Definition
There are a number of definitions of what a record is:

- Recorded information in any form (including data in a computer system) that is required to be kept by a public sector organisation as evidence of the activities or operations of the organisation, and includes part of a record and a copy of a record.\(^7\)

- Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.\(^8\)

Basically, a "record" is a piece of information which has been created or used by a public sector organisation to come to a decision, formulate advice, or conduct a transaction. The organisation needs to capture the record to ensure it can demonstrate how and why it acted in the way it did in line with its business, governance, legal or community requirements, and provide the rationale behind such action.

However, a record is not just a collection of data. It is the consequence or product of an event and therefore linked to business activities. A distinguishing feature of records (as opposed to just "information") is that their content must exist in a fixed form, that is, be a fixed representation of the business transaction.\(^9\) In order to “fix” the record as a true representation of a business transaction, request received, advice given, or decision made, it needs to be captured into the corporate records management system.

Identifying a record
Records are identified as such because of their content not their format. Almost all business is now conducted electronically, especially using email functionality. During the normal course of conducting business, individuals must make a decision about what constitutes a record based on the informational content of the message or document they create or receive. They must then capture this record into the corporate records management system in accordance with the business rules the organisation has for such capture.

The following questions provide some guidance for staff when deciding if a piece of information they have created or received is a record:

<table>
<thead>
<tr>
<th>What is a record?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does this relate to the work I perform for my organisation?</td>
</tr>
<tr>
<td>Did I create or receive it in the course of this work?</td>
</tr>
<tr>
<td>Is it evidence of work I or my organisation have performed?</td>
</tr>
<tr>
<td>Does it support a decision I or my organisation have made?</td>
</tr>
</tbody>
</table>

---

\(^7\) Information Act, s.4

\(^8\) AS ISO 15489:2002—Records Management, Part 1: General, Clause 3.15

While all records are information, not every piece of information created or received is a record which needs to be captured and managed within the corporate framework. For example, some email messages are distributed for information only. In this case, the originator would be expected to maintain a record of the message while recipients may delete the message after reading PROVIDING the message is not then used as the basis for further action, decision or advice by the recipient. If this is the case then the message would need to be captured along with a record of all subsequent action.

**Normal administrative practice**

Organisations are permitted to dispose of short-term or transitory records (eg, background notes, office messages, meeting requests, and drafts of reports and briefs with no significant impact upon the finished product/position) as part of normal administrative practice. Destruction in this manner usually occurs because the records are duplicated, unimportant or for short-term use only. Destruction of records of this nature is also permissible using the *Disposal Schedule for Records of Short Term Value*.10

The following is a guide to using normal administrative practice to dispose of ephemeral information in the normal conduct of business.

<table>
<thead>
<tr>
<th>Normal administrative practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Is the record covered by a specific law or current records disposal schedule?</td>
</tr>
<tr>
<td>If it is then normal administrative practice does not apply. If not, is the record:</td>
</tr>
<tr>
<td>• needed to clarify, support or give context to an existing record?</td>
</tr>
<tr>
<td>• needed to show how the organisation’s business was carried out?</td>
</tr>
<tr>
<td>• needed to show how a decision was made?</td>
</tr>
<tr>
<td>• needed to show when or where an event happened?</td>
</tr>
<tr>
<td>• needed because it indicates who made the decision or gave the advice?</td>
</tr>
<tr>
<td>• needed because it contains information on the rights or obligations of government or private individuals?</td>
</tr>
<tr>
<td>• a formal draft of a Cabinet submission?</td>
</tr>
<tr>
<td>• a draft of an agreement or legal document?</td>
</tr>
<tr>
<td>• likely to form part of a record that will be needed to support legal proceedings?</td>
</tr>
<tr>
<td>• subject to a legal hold order?</td>
</tr>
</tbody>
</table>

If the answer to all these questions is **no**, then you can consider destroying the record as normal administrative practice. If the answer to any question is **yes**, the record cannot be destroyed using normal administrative practice and should be subject to retention or destruction using a records disposal schedule.

---

10 *Disposal Schedule for Records of Short Term Value, No.2003/10, Northern Territory Government (2003)*
Standard 2 – Capture
Records must be captured into the corporate records management system

Policy statement
NT public sector organisations must capture corporate records into the corporate records management system. Where this is not possible, information about the record (metadata) is to be entered into the corporate records management system.

Explanation
Once identified as a corporate record, the record must be captured into the corporate records management system in accordance with the business rules the organisation has for such capture. This will help facilitate:

- **Efficiency**, by allowing the use, re-use, reference to and central distribution of records thereby making correct and authentic information readily available when needed;
- **Sound use of financial resources**, by allowing timely disposal of non-current records;
- **Accountability**, by enabling the creation of a complete and authoritative record of official activities;
- **Compliance**, by demonstrating that legal requirements have been met; and
- **Risk mitigation**, by managing the risks associated with illegal loss or destruction of records, and from inappropriate or unauthorised access to records.11

The purpose of capturing records into the corporate records management system is to establish a relationship between the record, its creator and the business context within which it was created via the metadata captured with the record.12 Capturing records into the corporate records management system links records to business activities helping to ensure their authenticity and inviolability.

Capturing the metadata (information about the record) at the same time enables the retrieval and use of the record and supports its ongoing management for as long as it is required to be retained. The metadata defines the record’s characteristics at its point of capture, fixing it into the business context of the organisation and enabling effective records management processes to take place even when the record itself is not able to be captured into the corporate records management system.13

The corporate records management system must be the primary repository of the corporate records of the organisation, or at least the primary repository of information about corporate records, eg when hard copy records are maintained or where a business system retains the record. Whenever a record is required the system should be the first source to be searched.

The NT Government ICT Policy, End User ICT Services, (May 2009), states:

Shared network file systems, workstation file systems, and personal e-mail databases are not approved records management systems and must not be used for storage of electronic records.14

---

14 ICT Policy, End User ICT Services, Section 7. Records management, 7.2 Approved records management system, p.13 NT Government (May 2009)
Users should not store work in progress in the computer hard-disk [including lap tops] and other portable media (eg CD, DVD, USB stick, Smart Phone, etc) since it is not backed up, it is not sufficiently secure, and could be lost if the computer suffered a malfunction or was otherwise lost.15

A document not managed within the corporate records management system cannot be guaranteed to be a true representation of what it purports to be, ie a genuine record of a business transaction, decision made or advice given in the normal course of conducting business. This is because in an unstructured environment there are few rules governing the authenticity, integrity and use of information (how it was created, by whom, which version it is, who has had access to it, its security classification), and formal scrutiny is difficult. It therefore cannot be seen as the best evidence of the organisation’s business if it is required in a court case or by a formal inquiry or judicial hearing, and may be difficult to defend if challenged.

Failure to capture records into the corporate records management system can lead to adverse consequences for some organisations. The NT Information Commissioner has reported:

Some organisations have encountered difficulties in processing an FOI (freedom of information) request. In some cases, this has been the result of inadequate record management systems. The organisation has therefore been unable to locate the information that is being sought.16

In contrast, capturing electronic documents or messages that are records into the corporate records management system will help ensure:

- **Authenticity** – the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred.
- **Reliability** – the record can be trusted 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.
- **Integrity** – the record is complete and unaltered, and protected against unauthorised alteration. This characteristic is also referred to as ‘inviolability’.
- **Usability** – the record can be located, retrieved, preserved and interpreted.17

**Implementation advice**

NT public sector organisations need to implement processes to ensure records are captured into the corporate records management system systematically. This means making the system available to all staff who create and capture records, promoting its use and providing the necessary training on what to capture and how to capture it into the system.

An automatic interface between normal electronic applications used to conduct business (eg, office software, the corporate email system) into the records management system, enables users to capture records of business almost seamlessly at creation or receipt of the record. Minimum metadata requirements identified as mandatory for the organisation will assist end users to enter the required data about the record simultaneous to the record’s capture.

However, as business processes become more completely automated, corporate records can exist outside of the formal corporate records management system, often being created in business systems serving specific purposes. The electronic information generated by such activities may serve as the only evidence of specific transactions or decisions. Maintenance of this evidence in the form of fixed records is necessary for operational viability and accountability of the organisation. This means that a business system that creates but does not manage

---

16 Annual Report of the Office of the NT Information Commissioner 2008-2009, 8.1 Need for proper records management systems, p.43
records needs to interface with the corporate records management system to either capture the record itself or the metadata associated with the record.

In instances where an organisation does not yet have full electronic document and records management functionality, the only option is to maintain records in hard copy format and capture the associated metadata into the corporate records management system.

Whatever system or combination of systems is used, it should be capable of using and supplying metadata to manage records in an accountable and effective way. Systems must not allow unauthorised modifications to any records (including metadata), and where authorised modifications are performed, they must be fully documented.18
Standard 3 – Discovery
Records must be findable and accessible for as long as they are required

Policy statement
NT public sector organisations need to be able to find records promptly and be able to read and produce them when required for as long as the records need to be retained.

Explanation
There is little point in retaining records as authentic corporate information if they are difficult to find when needed or can no longer be accessed due to technological obsolescence. Information (in the form of records), like any other asset, needs to be classified, structured, validated, valued, secured, monitored, measured and managed efficiently and effectively.19

There are a number of reasons why records need to be accessed:

• for the current operational requirements of an organisation, eg, to confirm decisions made, advice given or action taken, or as background to the conduct of further business;
• in response to requests for information in accordance with the Information Act (freedom of information);
• in order to be produced in an official inquiry or for other regulatory or investigative purposes, eg, by the Auditor-General or the Ombudsman, or in a court of law.

It is essential that an organisation is able to access the required records in a timely and efficient manner, especially where there are limits imposed upon the time taken to access and produce the records (eg, in accordance with the Information Act, or in legal discovery). In the Annual Report of the Office of the NT Information Commissioner 2008-2009, it was reported that:

Some complaints are delayed because certain agencies have poor records management systems and it is difficult, or even impossible, for them to locate the information that is being sought.20

Such situations need to be avoided because penalties may apply if an organisation fails to store information securely and this results in a privacy breach. There are penalties if a person mishandles information in accordance with the legislation.21

Implementation advice

Records must be findable
The ability to find records promptly is dependant upon the allocation of meaningful metadata to a record on creation or receipt. Part of this process involves classification.

The optimum method of classifying records is based on an analysis of the unique business functions and activities of the organisation, independent of the organisation’s administrative structure. Classification of business functions and activities acts as a powerful tool to assist the conduct of business and in many of the other processes involved in the management of records.22

20 Annual Report of the Office of the NT Information Commissioner 2008-2009, 1.3 Performance measures as set by Budget Paper 3, p.6
21 Information Act, sections 145-147
Functional classification is more flexible and stable as business units and structures are likely to change over time (eg, following an election), whereas government functions are relatively enduring even through administrative rearrangements. This method breaks down traditional organisational information silos and facilitates easier retention, security and disposal of records.

There are a number of recordkeeping tools that assist in the classification of records. The NT Government has adopted **Keyword AAA**, developed by the State Records Authority of New South Wales, which provides a controlled set of terms for use by many organisations in the classification of common administrative terms, eg, financial management, personnel, property management. NT Government public sector organisations have also built upon the core set of administrative terms contained in **Keyword AAA** to create terminology that describes the unique functions (as opposed to the common administrative terms) and activities of the NT Government.

**Keyword for Councils**, also developed by the State Records Authority of New South Wales, is designed for use in classifying, titling and indexing council records. This is able to be adopted by NT local authorities for classifying records.

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

Classification schemes within a corporate records management system allow for easy titling of records at the point of capture by all users.

**Records must be accessible**
Records must be able to be searched for, retrieved and rendered in accessible formats and media for as long as they are required for business, legal or community purposes. This may pose a challenge in the electronic environment as records may need to be retained for longer than the lifetime of the current technology. The **Information Act** states that public sector organisations must keep records in a form in which they are capable of being read and reproduced.

In addition, the Australian Standard AS ISO 18492—2006: **Long-term preservation of electronic document-based information**, states

Organizations increasingly face the challenge of ensuring the long-term accessibility of authentic electronic information that was created within reliable and trustworthy information systems and stored on electronic media that might be subject to technological obsolescence that if left uncorrected will make the document-based information irretrievable. It is essential, therefore, that organizations develop and apply a well-defined strategy for providing long-term preservation and retrieval of authentic electronic document-based information.

The use of the corporate records management system satisfies the above requirements to some degree in that the records are captured and managed in a secure environment over time, in accordance with known and applied business rules. The records in the system contain reliable information that has not been altered (unless it was done in accordance with normal business practice and such action is fully documented), or otherwise corrupted. System upgrades and migration (where necessary) are planned and implemented methodically and are usually coordinated centrally.

Capturing records into the corporate records management system is a fundamental step in ensuring they are able to be retrieved in the future.

---

24 Keyword for Councils, State Records New South Wales (2001)
25 Information Act, s.136
NOTE: It is important that NT public sector organisations 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 also present risks to the ongoing useability of the record because decryption keys and public keys for digital signatures may expire while the record is still required. For this reason, storing records in encrypted form is not permitted and encrypted records must be decrypted before being captured into the corporate records management system. The records management system should provide sufficient security for the long term storage of electronic records.

Standard 4 – Security
Records must be secure

**Policy statement**

NT public sector organisations must create, store, use and make records available securely with due regard to permitting access to those with a genuine need to know the information in the records.

**Note:** This standard provides advice to be followed for the management of non-national security information. For the management of national security information see the Guidelines for the Management of National Security Information.28

**Explanation**

It is essential that public sector organisations are aware of the value of information contained in the records they possess, and execute responsibility in accordance with the duty of care principle and the records management and privacy provisions of the Information Act. To fulfil this objective, organisations must implement an information security framework.29

The framework comprises the technology utilised to capture records, the security classifications for records and the security profiles of all staff in the organisation. A security framework needs to be in place that is managed according to standards, business rules and practices that are known by all in the organisation, is actively promoted and able to withstand scrutiny. The framework needs to be reviewed, audited and updated when necessary.

This standard has been developed using the Australian Government Protective Security Manual (2005) as a guide as well as taking into account the provisions of the Information Act, specifically Part 2 – General principles about disclosure of information, Part 9 – Records and archives management, and the Information Privacy Principles.

NT public sector organisations must adhere to the requirements of this standard. Organisations must ensure all staff are aware of the provisions of this standard, and adhere to them in the normal conduct of business. Organisations must also ensure security provisions are incorporated in contracts with contractors to ensure compliance with the Information Privacy Principles.

**Implementation advice**

**Records management system**

The first step in ensuring security of a record is to capture it into the corporate records management system. The system will be managed by rules and procedures that are designed to ensure the authenticity, inviolability and security of records. Security classifications for both records and staff must be managed within the system. Audit logs, which monitor and log access and activity, must be able to be produced by the corporate records management system.

**Records**

All records need to be allocated a security classification. The allocation of security classifications to records allows agencies to share and exchange information with confidence by ensuring a common recognition of confidentiality requirements and consistent application of protective security measures. It will help ensure the records they store are inviolate, that is they are tamper-free and protected from unauthorised alteration, deletion or loss. The classification system also protects the information of other governments, local authorities, commercial entities.

---

28 Guidelines for the Management of National Security Information, Northern Territory Department of the Chief Minister and the Northern Territory Archives Service (2006)
or individuals with which NT public sector organisations exchange information. In addition, it will assist in fulfilling the privacy requirements of the Information Act.

The staff member responsible for creating the record, or for actioning a record generated outside the organisation (receiving the record), must decide its security classification. When a record is created or captured the consequences of damage from unauthorised access to it need to be assessed in order to allocate the appropriate security classification.

**Staff**
In addition, all staff must be allocated a security classification (profile). Business unit managers must determine which of their staff have a ‘need to know’ regarding official records and allocate security classifications to them accordingly. They must also ensure that the allocation of security classifications to their staff is fully documented and that staff are aware of, and comply with, the appropriate protective security procedures for handling records, especially those requiring a degree of protection.

**Classification levels**
This table was developed from advice in the Australian Government *Protective Security Manual* (2005). It provides a guide to identifying the type of records which may require some degree of protection. The classifications are to be used whenever records containing such information are created and received.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Degree of protection</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Protected</td>
<td><em>Does the information the record contains need the highest degree of protection?</em></td>
<td>Unauthorised release could reasonably be expected to <strong>cause serious harm</strong> to an organisation or individual</td>
</tr>
<tr>
<td>Protected</td>
<td><em>Does the information the record contains need a substantial degree of protection?</em></td>
<td>Unauthorised release could reasonably be expected to <strong>cause harm</strong> to an organisation or individual</td>
</tr>
<tr>
<td>In-Confidence</td>
<td><em>Does the information the record contains need only a limited degree of protection?</em></td>
<td>Unauthorised release <strong>might possibly cause harm</strong> to an organisation or individual</td>
</tr>
</tbody>
</table>

Records requiring a degree of protection need to be further qualified by the use of a caveat which describes the particular category of confidentiality applicable to the record, eg, Cabinet-In-Confidence, Commercial-In-Confidence, Personnel-In-Confidence, Tender-In-Confidence.

An intermediate classification of NTG Restricted or Council/Shire Restricted may be applied to those records that are required for the conduct of regular business but which should not normally be released into the public domain. The vast majority of a public sector organisation’s records would fit into this classification.

Records which require no degree of protection and can be made available in the public domain immediately (eg, published information, web sites) are to be labelled “Unclassified”.

Use of access controls within the corporate records management system can further restrict access to records to certain individuals in a particular business unit rather than all staff in the organisation, whenever there is a need.

**Freedom of information**
The allocation of a security classification obliges caution in the storage of and access to a record. It does not, however, provide a reason for denying access to the record in accordance with the freedom of information provisions in the Information Act. A separate access regime

---

exists for determining rights of access to a record when a request has been received under these provisions of the legislation. An organisation must assign responsibility for determining such access requests to an appropriate staff member or unit.

**Business systems**

Whilst capturing records into the corporate records management system will ensure their security, records may also be created and stored in business systems and their capture into the corporate records management system may not be practical. In this instance, metadata about such records needs to be captured into the corporate records management system. It is important, therefore, that organisations ensure that the designers and operators of business systems that will create or store records understand the security as well as the operational requirements of the system. The security requirements outlined in this standard need to be built into the system at the design phase in consultation with the organisation’s records manager.

**Markings**

Once a record has been identified as requiring security classification, a protective marking must be assigned to it indicating the level of protective procedures that must be provided during the use, storage, transmission, transfer and disposal of the information. This needs to be observed whether the record is electronic or hard copy.

**Over classification and review of classification**

Records should only be security classified when the consequences of compromise warrant the expense and effort of increased security protection. Classifications thought to be inappropriate should be queried with the originator or the person now responsible. Inappropriate over-classification has a number of seriously detrimental effects, e.g., the volume of security classified records becomes too large for an organisation to protect adequately, or classification and security procedures may be brought into disrepute if the classification is unwarranted with the consequence that classifications and protective markings may be devalued or ignored by an organisation’s staff or external entities.

When a decision is made to security classify a record, an organisation must consider whether a time limit for the classification should be set. Records should be declassified or downgraded when protection is no longer necessary or is no longer needed at the original level. It might be possible to determine a specific date or event that will allow the record to be declassified.

If a record is transmitted to another public sector organisation, only the originating organisation (i.e., the organisation that assigned the original classification) can reclassify or declassify a record. If an organisation is abolished or amalgamated, the organisation assuming the former agency’s responsibilities is deemed the originating organisation for the purpose of reclassification and declassification.

**Physical security**

While security of the corporate records management system will protect the metadata of both electronic and hard copy documents as well as the electronic documents themselves, consideration needs to be given to the security of hard copy documents in the workplace.

Access to areas where security classified records are held or used must be restricted. When security classified records are not in use, they must be stored in an appropriate security container. During absences from their workplace, staff must ensure that records and systems are secured appropriately.

---

Standard 5 – Disposal
Records must be disposed of systematically and accountably

Policy statement
NT public sector organisations must dispose of records 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 toward the retention and disposal of records.

Explanation
The Information Act provides that a public sector organisation must not dispose of a record unless it is done in compliance with a relevant practice, procedure, standard, or in accordance with legislation or a court order.37

Although there are many pieces of legislation that require records to be created, there are few that actually stipulate the amount of time a record needs to be retained before it can be destroyed. A few exceptions include:

- taxation legislation which requires that generally, records need to be retained for five years;38
- the Workplace Relations Act which states that employers must keep a number of written records of their staff for seven years;39
- the Workplace Health and Safety Regulations which state an employer shall maintain a record of certain information for not less than 30 years.40

Records disposal schedules
The most common method used to determine the retention or destruction of records is the records disposal schedule process. This involves a thorough and systematic analysis of the business activity of an organisation and an assessment of the records which are produced as a result of that activity. A records disposal schedule is then produced which permits a public sector organisation to retain or destroy its records in accordance with the Information Act.41

Records retention decisions must be based on:

(a) the current and future business needs of the organisation;
(b) compliance with legal and governance requirements of the organisation;
(c) the current and future needs of internal and external stakeholders including the wider community.42

The schedules are approved by the chief executive officer of the public sector organisation responsible for the function to which the schedule relates, the director of the records service and the director of the archives service.

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.

37 Information Act, s.145
40 Workplace Health and Safety Regulations, s.69D
41 Information Act, s.145(2)(b)
Implementation advice
The records disposal schedule process involves in-depth consultation between business unit managers and records managers from public sector organisations. The records service provides advice and assistance on the development and implementation of records disposal schedules.

Implementation of the provisions of a disposal schedule (sentencing records for destruction or retention) needs to be systematic, planned and documented. It must be carried out by appropriately qualified and experienced staff who have a good understanding of the business to which the schedule relates.

Destruction of records
When records have been sentenced as temporary in accordance with an approved records disposal schedule, there is a set retention period for which they must be kept before they can be legally destroyed.

The destruction of a public sector organisation’s records needs to be clearly documented and captured in the metadata in the corporate records management system. In addition, notification of such destruction needs to be forwarded to the Records Policy Unit, Department of Business and Employment, which monitors the use of records disposal schedules.

While destruction of hard copy records is relatively straightforward, the destruction of electronic records needs to be similarly guaranteed. All copies of an electronic record which is due for destruction must be erased beyond its possible recompilation which includes any copy retained as part of the organisation’s information back-up practices.

Whatever the format of the records due for destruction, the appropriate level of security for the records must be observed until they are completely destroyed.

Procedures should be in place to ensure that records subject to discovery or legal hold are clearly identified and marked to ensure they are not destroyed pending the finalisation of related legal action.

Retaining electronic records
Section 136(1) of the Information Act provides:

A public sector organisation must keep records created at any time after the commencement of this section in a form in which they are capable of being read and reproduced, which may be an electronic form.

This has implications for the management of electronic records which need to be retained for longer than the technology used to create them. It is therefore important as part of a retention strategy to plan migration processes for records requiring longer term retention to mitigate the effects of technological obsolescence. Such processes may involve a change of media and/or change of computer hardware and/or software. A reliable method is to ensure that electronic records are stored in an industry standard format, or that viewers for each stored format are maintained.43 Proprietary file formats should be avoided for long term storage as vendors generally discontinue support or do not provide continuity in newer versions of software. Among the technology neutral formats that can be considered for this purpose are PDF/A-1, XML, TIFF and JPEG.44

If a strategy for managing long term electronic records is not established and adhered to, providing access to records in the future could be impossible and akin to their actual

43 AS ISO 15801—2006, Electronic imaging — Information stored electronically —Recommendations for trustworthiness and reliability, 7 Enabling technologies, 7.10 Migration, p.32
destruction. This could lead to a public sector organisation being in breach of s.136 and s.145 of the Information Act.

Archives
Records deemed to be of permanent value (ie retained forever) are archives and will ultimately be transferred to the archives service for inclusion in the Territory Archives. The archives service issues standards for the management of archives and permanent records, including the transfer of permanent records to the archives service.

---

45 Information Act, s.141(1)(a)
Compliance requirements

NT public sector organisations need to ensure they are working toward the following compliance requirements for managing records. Organisations will be monitored against these requirements in accordance with s.131A(a) of the Information Act.

Standard 1 – Governance (including identification of records) - Records must be created within a managed framework

1.1 The organisation has records management policies in place which are made known to all staff during induction training, and are promoted and made widely available to all staff regularly.

1.2 The organisation provides adequate resources (including budgetary requirements) to plan, develop and manage its records management responsibilities and to promote records management procedures throughout the organisation.

1.3 Regular training is provided to staff to provide skills to fulfil the organisation’s records management responsibilities.

1.4 The organisation ensures that its staff are able to identify a record in the course of conducting their daily business and know they must capture it as a corporate record.

1.5 The chief executive officer of the organisation reports on records management compliance in the annual report in accordance with s.131(2) of the Information Act.

Standard 2 – Capture - Records must be captured into the corporate records management system

2.1 The organisation promotes the corporate records management system as the repository for the capture and management of official records, or information about official records (metadata).

2.2 The organisation has procedures in place for the capture of official records into the corporate records management system and these procedures are available and made known to all staff.

2.3 The organisation is aware of the existence of official records in business systems and, where possible, has in place an interface between the business system and corporate records management system to automatically capture the record or its metadata.

2.4 The organisation has minimum metadata requirements for the capture of information about official records and these requirements are known to all staff who create or receive records.

2.5 Suitably qualified and experienced staff are employed to administer and troubleshoot the organisation’s corporate records management system, and to promote its use in the organisation.

Standard 3 – Discovery - Records must be findable and accessible for as long as they are required

3.1 All staff of the organisation are aware of the role and importance of the corporate records management system in providing access to official records.

3.2 The organisation is able to immediately locate any of its records when required for business purposes or in answer to an external request (eg freedom of information).

3.3 The organisation uses an authorised classification system to title official records and this scheme is promoted to and used by all staff who create or receive records.
3.4 The organisation has procedures in place to ensure that electronic records are able to be accessed and read for as long as they are required to be retained, including records held in business systems.

3.5 Any digital rights management technology is strictly administered by the organisation with due regard to the accessibility of records over time (eg decryption of encrypted records prior to capture in the corporate records management system).

**Standard 4 – Security - Records must be secure**

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

4.2 Security classifications for records are known by all staff and are assigned to all records at the time of creation or receipt in line with the degree of protection the information in the record requires.

4.3 A security classification/level is assigned to all staff by the respective business unit managers and is appropriate to the staff member’s need to know the information in the record in order to conduct legitimate business for the organisation.

4.4 The organisation has procedures in place to review and declassify official records that are classified “In-Confidence” and above at an appropriate time if protection is no longer necessary or is no longer needed at the original level.

4.5 The organisation assigns responsibility for monitoring access to, alteration and movement of official records, using audit logs within the corporate records management system and business systems containing records.

**Standard 5 – Disposal - Records must be disposed of systematically and accountably**

5.1 All the organisation’s records are covered by a current and authorised records disposal schedule.

5.2 The organisation nominates a suitably qualified and experienced staff member to manage the records disposal process, including the development and approval of disposal schedules, capturing the approved schedules into the corporate records management system, education and training of other organisation staff in the disposal process, and the sentencing of records for retention or destruction.

5.3 All records disposal action is fully documented and captured into the corporate records management system.

5.4 The organisation ensures that whenever destruction is permitted by a current and authorised records disposal schedule, all copies and versions of official records are properly destroyed including electronic versions of records held in the organisation’s information back-up practices.

5.5 The organisation has in place procedures to guarantee that records subject to discovery or legal hold are clearly identified and marked to ensure they are not destroyed pending the finalisation of legal action involving them.
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>A record of permanent value that forms part of the Territory Archives.</td>
<td>Information Act, s.4</td>
</tr>
<tr>
<td>Archives service</td>
<td>The organisation established to perform the archives functions for the Territory. Currently this is the NT Archives Service of the Department of Natural Resources, Environment, The Arts and Sport.</td>
<td>Information Act, s.4</td>
</tr>
<tr>
<td>Business classification scheme (BCS)</td>
<td>A conceptual hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposition of records. It defines the way in which records are grouped together (aggregated) and linked to the business context in which they were created or transmitted.</td>
<td>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 2 - Guidelines and Functional Requirements for Electronic Records Management Systems</td>
</tr>
<tr>
<td>Business system</td>
<td>An automated system that creates or manages data about an organisation’s activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers – for example, an e-commerce system, client relationship management system, purpose-built or customised database, and finance or human resources systems.</td>
<td>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 1 - Overview and Statement of Principles</td>
</tr>
<tr>
<td>Classification</td>
<td>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.</td>
<td>Australian Standard AS ISO 15489—2002: Records Management - Part 1:General, Clause 3.5</td>
</tr>
<tr>
<td>Disposal (sometimes referred to as Disposition)</td>
<td>(1) Range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposal schedules or other instruments.</td>
<td>Adapted from Australian Standard AS ISO 15489—2002: Records Management - Part 1:General, Clause 3.9</td>
</tr>
<tr>
<td></td>
<td>(2) (a) destroying or damaging the record;</td>
<td>Adapted from Australian Standard AS ISO 15489—2002:</td>
</tr>
<tr>
<td></td>
<td>(b) abandoning, donating, selling or transferring the possession or control of the record.</td>
<td>Records Management - Part 1:General, Clause 3.10</td>
</tr>
<tr>
<td>Document</td>
<td>Recorded information which can be treated as a unit, regardless of format and may include text/sms messages, voice messages, web page, blogs and wiki’s. A document may or may not be a record. (See also Record.)</td>
<td>Expanded from Australian Standard AS ISO 15489—2002: Records Management - Part 1:General, Clause 3.10</td>
</tr>
<tr>
<td>Document management</td>
<td>A process for providing a single reference point for working, collaborating and commenting on the most recent version of a document. (see also Records Management)</td>
<td>Adapted from AS 5037: 2005—Knowledge management – a guide,</td>
</tr>
<tr>
<td>Term</td>
<td>Explanation</td>
<td>Source</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fixed record</td>
<td>To be considered authentic and reliable evidence, a record must be fixed to a point in time and unalterable. Following its capture as a record any further processes must result in the creation of a new record or the augmentation of the existing record, rather than alteration to it.</td>
<td>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 3 – Guidelines and Functional Requirements for Records in Business Systems</td>
</tr>
<tr>
<td>Information</td>
<td>Knowledge communicated or received. The result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.</td>
<td>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 1 - Overview and Statement of Principles</td>
</tr>
<tr>
<td>Information management</td>
<td>Information management supports effective and efficient management of information in the service of defined user populations (eg organisation or societal group). It is concerned with the study and practice of processes that enable the creation, production, collection, organisation, storage, retrieval and dissemination of information resources which may be in any format and available from internal or external sources.</td>
<td>AS 5037: 2005—Knowledge management – a guide, Section A5</td>
</tr>
<tr>
<td>Metadata</td>
<td>Structured or semi-structured information, which enables the creation, management and use of records through time and within and across domains. [<em>Data about data</em>, eg, document number, title, author, date of creation, security classification, disposal information.]</td>
<td>Australian Standard AS ISO 23081.1—2006: Information and documentation — Records management processes — Metadata for records, Part 1: Principles</td>
</tr>
<tr>
<td>Proprietary software</td>
<td>Software that is owned exclusively by a single company that carefully guards knowledge about the technology or the product’s inner workings.</td>
<td>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 1 - Overview and Statement of Principles</td>
</tr>
<tr>
<td>Public sector organisation</td>
<td>A public sector organisation is defined in the Act as any of the following:</td>
<td>Information Act, s.5(1)</td>
</tr>
<tr>
<td></td>
<td>(a) an Agency;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) a Government Business Division;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c) a Government owned corporation;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(d) a local authority;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(e) a statutory corporation;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(f) a person appointed, or body established, by</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Explanation</td>
<td>Source</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>or under an Act or by the Administrator or by a minister;</td>
<td>(g) the Police Force of the Northern Territory;</td>
<td><strong>Information Act, s.4</strong></td>
</tr>
<tr>
<td>(h) a person holding an office or position under an Act;</td>
<td>(i) a court of the Territory;</td>
<td></td>
</tr>
<tr>
<td>(j) a tribunal of the Territory;</td>
<td>(k) a person or body declared by the Regulations to be a public sector organisation.</td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td>(1) Recorded information in any form (including data in a computer system) that is required to be kept by a public sector organisation as evidence of the activities or operations of the organisation, and includes part of a record and a copy of a record.</td>
<td><strong>Australian Standard AS ISO 15489—2002: Records Management - Part 1:General, Clause 3.15</strong></td>
</tr>
<tr>
<td>(2) Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recordkeeping</td>
<td>The systematic creation, use, maintenance and disposition of records to meet administrative, legal, financial and societal needs and responsibilities.</td>
<td><strong>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 1 - Overview and Statement of Principles</strong></td>
</tr>
<tr>
<td>Records management</td>
<td>(1) 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.</td>
<td><strong>Australian Standard AS ISO 15489—2002: Records Management - Part 1:General, Clause 3.16</strong></td>
</tr>
<tr>
<td>(2) The control of the creation, receipt, maintenance, use and disposal of records in accordance with professional and international standards of practice. Records management is distinct from document management, which is typically concerned with the provision of access, collaborative working and version control of documents, rather than the management of authenticity, reliability, integrity and useability over time.</td>
<td><strong>International Council on Archives - Principles and Functional Requirements for Records in Electronic Office Environments, Module 2 - Guidelines and Functional Requirements for Electronic Records Management Systems</strong></td>
<td></td>
</tr>
<tr>
<td>Records management system</td>
<td>Information system which captures, manages and provides access to records through time. [NOTE: includes managing classification, security, tracking and disposal of records.]</td>
<td>Adapted from <strong>Australian Standard AS ISO 15489—2002: Records Management - Part 1:General, Clause 3.17</strong></td>
</tr>
<tr>
<td>Records service</td>
<td>The organisation established to perform the records</td>
<td><strong>Information Act, s.4</strong></td>
</tr>
<tr>
<td>Term</td>
<td>Explanation</td>
<td>Source</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>functions for the Territory.</td>
<td>(This involves standards setting and provision of advice at a whole of jurisdiction level. Currently this is the Records Policy and Systems section of the ICT Division of the Department of Business and Employment.)</td>
<td>Australian Government Protective Security Manual (2005), 2.7 Principles of effective information security practice</td>
</tr>
<tr>
<td>Security classified</td>
<td>Official information is security classified when the compromise of that information could cause harm to the nation, the public interest, the Government or other entities or individuals.</td>
<td>Australian Standard AS ISO 18492—2006: Long-term preservation of electronic document-based information, 3.11 Definitions</td>
</tr>
<tr>
<td>Technological obsolescence</td>
<td>The displacement of an established technical solution in a marketplace as a result of major technological developments or improvements.</td>
<td>Australian Standard AS ISO 18492—2006: Long-term preservation of electronic document-based information, 3.11 Definitions</td>
</tr>
</tbody>
</table>