CAARA Policy 07

Principles on Full and Accurate Records

Adopted: 15 August 2000
Status: Current

Principles on Full and Accurate Records

Adopted: 15 August 2000

Status: Current

Table of contents

Executive Summary

The Council of Federal, State and Territory Archives (COFSTA) has issued these principles for use within the jurisdictions of the COFTSA members. Members may adopt or adapt the principles according to their jurisdictional and regulatory environments.

The principles in this document are drawn from current national and international best practice, notably Australian Standard AS 4390—1996: *Records Management,* Part 3: *Strategies*, Clause 5.3, and the work of the University of Pittsburgh's *Recordkeeping Functional Requirements Project*. COFSTA acknowledges this valuable basis for the standard.

This document establishes principles for making and keeping full and accurate records. In short, the principles are that:

1. **Recordkeeping should be *compliant:*** recordkeeping should comply with legal and administrative requirements.

2. **Recordkeeping should be *reliable:*** recordkeeping systems, procedures and practices should work reliably to ensure that records are credible and authoritative.

3. **Recordkeeping should be *systematic:*** records should be made, maintained and managed systematically.

4. **Recordkeeping should be *managed:*** recordkeeping must be managed through an identifiable records management program.

5. **Recordkeeping should be *audited:*** recordkeeping systems, procedures and practices should be audited to ensure compliance with regulatory requirements.

6. **Recordkeeping should be *routine*:** recordkeeping systems should be used when transacting business.

7. **Records should be *made:*** records should be made to document and facilitate the transaction of business and captured into recordkeeping systems.

8. **Records should be *retained:*** records should be retained for as long as they are needed.

9. **Records should be *complete:*** a record should contain not only the content, but also the structural and contextual information necessary to document a transaction. It should be possible to understand a record in the context of the organisational processes that produced it and of other, linked records.

10. **Records should be *comprehensive:*** records should document the whole of the business of a public sector body.

11. **Records should be *adequate:*** records should be adequate for the purposes for which they are kept.

12. **Records should be *accurate:*** records should correctly reflect what was communicated, decided or done.

13. **Records should be *authentic:*** records should be what they purport to be.

14. **Records should be *useable:*** records should be identifiable, retrievable, accessible and available when needed.

15. **Records should be *inviolate:*** records should be securely maintained to prevent unauthorised access, destruction, alteration or removal.

The principles are concerned with outcomes rather than with prescribing specific recordkeeping practices. Consequently, the examples should be viewed as guidance to help comply with each principle. The examples are followed by sources of further guidance relevant to the principle, where available.

The primary purpose of these principles is to promote recordkeeping best practice across the Federal and State and Territory Governments. This means that the building of systematic recordkeeping into business processes and systems should be done in such a way as to support and not hinder people's work.

Introduction

Background

These principles are adapted from the standard *Full and Accurate Records* issued in 1998 by the then Archives Authority of New South Wales (now State Records Authority of New South Wales). The NSW *State Records Act 1998* requires public sector bodies to make and keep full and accurate records of their activities. The NSW standard was prepared for issue under that legislation. The standard was issued to promote best practice in recordkeeping and to enable public sector bodies to prepare to meet their obligations under the NSW legislation.

The principles in this document are drawn from current national and international best practice, notably Australian Standard AS 4390—1996: *Records Management.* COFSTA acknowledges this valuable basis for the principles.

As described in the Australian Standard, records should be full and accurate to the extent necessary to:

'…*facilitate action by employees at any level of public sector bodies, and their successors;*

…*make possible a proper scrutiny of the conduct of business by anyone authorised to undertake such a scrutiny; and*

…*protect the financial, legal and other rights of the organization, its clients and any other people affected by its actions and decisions.' (Australian Standard AS 4390—1996: Records Management, Part 3: Strategies, Clause 5.3).*

The requirement to make and keep full and accurate records applies in all technological environments in which Government business is conducted, including the electronic environment.

Purpose

The purpose of these principles is to establish principles to guide public sector bodies in applying best practice in recordkeeping and in complying with the requirement noted above.

The principles are intended to function as:

- an authoritative statement of the basic responsibilities of public sector bodies in relation to recordkeeping

- a benchmark which can be used by Ministers, investigative bodies, the courts and any other person or body to whom or which the public sector body is accountable, to assess whether adequate records have been made, maintained and managed in specific cases and investigations

- a foundation upon which public sector bodies can establish internal policies, business rules, systems and practices

- a basis on which COFSTA members can develop standards or other specific products within their jurisdictions.

Structure

In short, the principles that guide the creation, making and keeping of full and accurate records are:

1. recordkeeping should be *compliant*

2. recordkeeping should be *reliable*

3. recordkeeping should be *systematic*

4. recordkeeping should be *managed*

5. recordkeeping should be *audited*

6. recordkeeping should be *routine*

7. records should be *made*

8. records should be *retained*

9. records should be *complete*

10.   records should be *comprehensive*

11.   records should be *adequate*

12.   records should be *accurate*

13.   records should be *authentic*

14.   records should be *useable*

15.   records should be *inviolate.*

This document is arranged according to these principles. Each principle is stated and explained, followed by examples of means of complying with the principle. The document is concerned, however, with outcomes rather than with prescribing specific recordkeeping practices. Consequently, the examples should be viewed as guidance to help comply with each principle, rather than as minimum compliance requirements. The examples are followed by sources of further guidance relevant to the principle, where available.

Definitions

For the purposes of these principles the following definitions apply. The definitions are taken from Australian Standard AS 4390—1996: *Records Management,* Part 1: *General,* except definitions marked *.

Accountability

The principle that individuals, organisations and the community are required to account to others for their actions. Organisations and their employees must be able to account to appropriate regulatory authorities, to shareholders or members, and to the public to meet statutory obligations, audit requirements, relevant standards and codes of practice, and community expectations.

Appraisal

The process of evaluating business activities to determine which records need to be captured and how long the records need to be kept, to meet business needs, the requirements of organisational accountability and community expectations.

Business activity

Umbrella term covering all the functions, processes, activities and transactions of an organisation and its employees. Includes public administration as well as commercial business.

Capture

A deliberate action which results in the registration of a record into a recordkeeping system. For certain business activities, this action may be designed into electronic systems so that the capture of records is concurrent with the creation of records.

Disposal

A range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of records in or from recordkeeping systems. They may also include the migration or transmission of records between recordkeeping systems, and the transfer of custody or ownership of records.

Documents

Structured units of recorded information, published or unpublished, in hard copy or electronic form, and managed as discrete units in information systems.

Electronic records

Records communicated and maintained by means of electronic equipment.

Evidence

Information that tends to prove a fact. Not limited to the legal sense of the term.

Function

The largest unit of business activity in an organisation or jurisdiction.

Metadata*

The simplest useful definition of metadata is "structured data about data." This very general definition includes an almost limitless spectrum of possibilities ranging from human-generated textual description of a resource to machine-generated data that may be useful only to software applications. Library catalogues represent a well established variety of metadata that has served for decades as collection management and resource discovery tools. *(From The Dublin Core: A Simple Content Description Model for Electronic Resources, accessed via url: *http://purl.org/dc* on 14 June 2000.)

Recordkeeping

Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.

Recordkeeping metadata *

Recordkeeping metadata is data describing context, content and structure of records and their management through time. *(from ISO *Standard on Records Management draft* dated May 2000)

Recordkeeping systems

Information systems which capture, maintain and provide access to records over time.

Records

Recorded information, in any form, including data in computer systems, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs and kept as evidence of such activity.

Records continuum

The whole extent of a record's existence. Refers to a consistent and coherent regime of management processes from the time of the creation of records (and before creation, in the design of recordkeeping systems), through to the preservation and use of records as archives.

Records management

The discipline and organisational function of managing records to meet operational business needs, accountability requirements and community expectations.

Transaction

The smallest unit of business activity. Uses of records are themselves transactions.

The Principles

1. Recordkeeping Should be Compliant

Recordkeeping should comply with legal and administrative requirements.

Explanation

Every public sector body operates in an accountability environment where the organisation as a whole, its chief executive and/or individual employees are accountable for decisions and actions. This environment can include:

- statutory rights and obligations

- audit requirements

- accountability to Ministers and boards for the carriage of programs

- possible scrutiny by investigative bodies like Royal Commissions, Parliamentary Committees and the Ombudsmen

- possible administrative or judicial review

- industry-based codes of practice

- management and reporting arrangements within the organisation, and

- the relationships of staff members and supervisors.

Every public sector body should be aware at the corporate or program level of the accountability requirements which bear upon it and how they affect recordkeeping and should take steps to comply with those requirements. Employees must understand how they are affected. There may be an audit requirement, for example, to keep evidence of receipt of payment for 7 years: recordkeeping will be compliant if recordkeeping practices ensure that adequate evidence of payment exists for the requisite period.

Examples of compliance with the principle

1. Legislation, regulations and formal directives to which the public sector body or program is subject have been systematically and comprehensively identified and documented.

2. Statements of best practice established by Government or applying in the industry in which the public sector body operates have been identified and are incorporated into standard operating procedures for all programs and supporting activities.

3. These sources are documented and kept up to date and associated recordkeeping requirements are identified.

4. Business rules and procedures governing work practices reflect obligations imposed by these recordkeeping requirements.

5. The procedures, forms and documentation for transactions which are governed by external rules/regulations routinely include references to those external rules and their currency.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 2: *Responsibilities* and Part 3: *Strategies*

Records Management Policy and Practice Manual(subject to review), State Records of South Australia, Section 1, 1996

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

2. Recordkeeping Should be Reliable

Recordkeeping systems, procedures and practices should work reliably to ensure that records are credible and authoritative.

Explanation

To document business transactions fully and accurately, it must be possible to demonstrate that records are what they purport to be. Thus, the recordkeeping system must operate in such a way that the records retrieved from it are credible and authoritative. This requires that recordkeeping systems, procedures and practices work reliably.

Examples of compliance with the principle

1. Recordkeeping systems, procedures and practices (and those aspects of business processes and systems which involve recordkeeping) are operating routinely at the time of the transactions documented by the records.

2. Procedures, guidelines and tools (such as classification schemes and disposal authorities) for performing recordkeeping processes are regularly vetted in accordance with approved review/audit programs and tested to minimise uncertainty, ambiguity and the need to exercise subjective judgement in routine tasks.

3. Standard procedures exist for reporting failures of any kind in recordkeeping systems, including systems failure in electronic recordkeeping and computerised records management systems.

4. Recordkeeping systems are subject to regular performance audits.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 3: *Strategies,* Appendix C: *Check List for Performance Testing of Records Management Systems*

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

3. Recordkeeping Should be Systematic

Records should be made, maintained and managed systematically.

Explanation

Records that will meet business needs, accountability requirements and other organisational needs cannot be made, maintained or managed in the absence of system. *Laissez faire* recordkeeping is inevitably poor recordkeeping. The constant evolution of business practices and processes, the dismantling of centralised recordkeeping systems and the increasing use of electronic information and communications systems in business have broken down the systems on which we could once rely to ensure that recordkeeping took place. All too often inadequate or no new systems have been established in their place.

Recordkeeping practices must be systematised through the design and operation of recordkeeping systems and of business systems and processes which incorporate recordkeeping. A recordkeeping system must have accurately documented policies, assigned responsibilities and formal methodologies for its management.

All records, regardless of format and the technological environment in which they are generated, should be captured into, and maintained in, identifiable recordkeeping systems. These systems do not have to be large or centralised or accessible by everyone in the organisation. They can be based on workgroups; they can be designed to meet the specific needs of business units; they can control access and security to meet requirements for confidentiality. They do not have to be dedicated recordkeeping systems: they can be business application systems which incorporate the functionality required to keep records.

Examples of compliance with the principle

1. Recordkeeping systems are implemented and operating in all areas of the organisation.

2. Policies, rules and procedures require all recordkeeping in the organisation to take place through recordkeeping systems.

3. Support for recordkeeping is integrated into policies, business rules, standard operating procedures and the design of work processes and of information, business application and communication systems.

4. Policies, business rules, standard operating procedures, system administration procedures, and user guidance and instructions governing the operation and management of each recordkeeping system are documented and kept up to date.

5. Changes to recordkeeping systems are documented and auditable.

6. The commissioning and decommissioning of recordkeeping systems is documented.

7. Policies, business rules and standard operating procedures instruct employees (including agents and contractors) performing work in unstructured processes to make appropriate records of the transactions in which they participate.

8. Employees (including agents and contractors) receive appropriate training and guidance in the use of recordkeeping systems.

9. Written guidelines and training are provided to help employees (including agents and contractors) and workgroups meet their recordkeeping responsibilities.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 2: *Responsibilities* and Part 3: *Strategies*

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

4. Recordkeeping Should be Managed

Recordkeeping must be managed through an identifiable records management program.

Explanation

Recordkeeping systems must have accurately documented policies, assigned responsibilities, and formal methodologies for their management. This applies equally to dedicated recordkeeping systems and to business application systems functioning as recordkeeping systems.

Examples of compliance with the principle

1. Records management operations and systems are organised according to the needs and structure of the public sector body, the nature of its business and the prevailing technological and regulatory environments.

2. The records management program is identifiable from all other corporate programs.

3. The records management program is supported by corporate policy.

4. The records management program is planned and allocated appropriate resources.

5. Formal responsibility for all aspects of the records management program is appropriately assigned.

6. The records management program is appropriately located within the organisational structure of the public sector body.

7. The records management program is staffed by personnel with appropriate skills and knowledge.

8. The records management program is implemented throughout the organisation.

9. The records management program is regularly measured.

For further guidance

Standard on Records Management Programs, State Records Authority of New South Wales, 1999

The Records Management Policy and Procedure Manual Template for South Australian Government Agencies, The RMAA South Australian State Government Chapter, 1997.

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

5. Recordkeeping Should be Audited

Recordkeeping systems, procedures and practices should be audited to ensure compliance with regulatory requirements.

Explanation

Recordkeeping practices, systems and procedures of public sector bodies operate within a regulatory regime. This regime may consist of standards and requirements to ensure the creation, management and disposal of full and accurate records. It is essential that the recordkeeping practices, systems and procedures are audited on a regular basis. The audits will:

- identify areas of non-compliance within existing regulatory requirements

- identify problem areas for public sector bodies, thus allowing for internal corrective actions

- improve the quality and reliability of public records.

Examples of compliance with the principle

1. A public sector body has developed, or adapted, internal self assessment tools for their records management practices, systems and procedures.

2. A public sector body is implementing external audit requirements to their records management practices, systems and procedures.

3. The internal auditors of a public sector body conduct audits of the records management practices, systems and procedures of the organisation.

4. Public sector bodies have developed and implemented planned records management audit regimes.

5. Public sector bodies monitor and update their internal audit regimes as external audit requirements are altered and updated.

6. Corrective actions are implemented as necessary following audits of records management practices, systems and procedures.

For further guidance

Australian Standard AS 4390 – 1996: Records Management, *Part 3:* Strategies, *Appendix C* Check List for Performance Testing of Records Management Systems

Records Management Adequacy Project; "The Minimum Compliance Requirements for a Records Management Program", **(NB Working Title only)** State Records of South Australia, 2000

Records Management Adequacy Project; Statement of Adequate Records Management **(NB working title only)**, State Records of South Australia, 2000

Records Management Adequacy Project, "The Guideline for the Development of a Records Management Program in South Australia", **(NB working title only)**, State Records of South Australia, 2000

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

6. Recordkeeping Should be Routine

Recordkeeping systems should be used when transacting business.

Explanation

Making records and capturing them into recordkeeping systems should be a normal part of work. Building recordkeeping into business processes and systems should be done in such a way as to support, and not hinder, peoples' work.

Business processes and systems should be designed to make it easy, or even automatic, to make appropriate records of all transactions.

Electronic business technologies provide unprecedented opportunities to put this principle into effect. Provided that the necessary specifications, based on identified recordkeeping requirements, can be furnished, it is feasible to design business application systems which automate all or most of the recordkeeping associated with using them. This kind of approach is particularly valuable when it can be applied in conjunction with business process re-engineering and/or the re-design of electronic information systems.

Examples of compliance with the principle

1. Adequate recordkeeping is a part of all business processes.
2. Business application systems and electronic information systems used in business processes are designed or modified to make the capture of records as easy as possible or, where possible, entirely transparent to the user.

3. Records are created in a recordkeeping system only through the execution of a business transaction.

4. It is possible to show that all recordkeeping systems and/or documented exception procedures have been operating at all times.

For further guidance

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

7. Records Should be Made

Records should be made to document and facilitate the transaction of business and captured into recordkeeping systems.

Explanation

Records document decisions and actions taken in the course of conducting the business of a public sector body. Records should emanate directly from the transaction of business. In many cases, the very ways in which people and organisations do business results naturally in the creation and accumulation of records. In other cases, a record must be made on purpose because conducting the transaction does not, by itself, generate a record.

Records may be made as the means by which a transaction occurs. For example, a contract itself has a legal effect; an electronic message itself conveys information. Alternatively records may be made to record what was decided or done. For example, minutes of a meeting are made after the meeting. In either case, the record is then kept as evidence of the transaction.

Records need to be captured into recordkeeping systems that can maintain and demonstrate the connection between the record and the transaction(s) that generated it or which it was made to document.

Examples of compliance with the principle

1. The functions and activities of the public sector body which require records to be made are identified and documented.

2. Inwards communications (such as electronic messages, faxes, telephone conversations and correspondence) with external persons and bodies are kept.

3. Copies of outwards communications with external persons and bodies are kept.

4. Internal communications are kept.

5. Minutes or other records are made of meetings, consultations, and deliberations involving the making of decisions or the transaction of business.

6. Records are made of oral decisions or commitments.

7. Records are made of the individual exercise of a discretionary judgement.

8. Policy and procedures for the capture of records into the recordkeeping systems of the organisation are established and implemented.

9. All records are captured as a matter of course into the organisation's recordkeeping systems.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 3: *Strategies,* Clause 8: *Cases*

Records Management Policy and Practice Manual

Records Management Policy and Practice Manual(subject to review), State Records of South Australia, Section 1, 1996

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

8. Records Should be Retained

Records should be retained for as long as they are needed.

Explanation

Records should be retained for as long as they are needed to meet business needs, the requirements of organisational accountability and community expectations. The length of time for which a record must be retained is determined by the requirements for retention of evidence that are associated with the business activity which the record documents. These requirements should be identified systematically through an appraisal process.

A record is retained so long as its content, and the structure and context supporting the meaning of content, are needed. Deletion of content or structure should only occur when authorised.

The disposal of records should take place only in accordance with the relevant Federal, State or Territory archives/records legislation. The retention and disposal of public records is governed by the records or archives legislation of a particular jurisdiction or Executive direction where no legislation exists.

The process of disposing of records should be accountable, documenting the nature and time of disposal action and the identity of the person taking the action. Only authorised people should take disposal action. This applies equally in the electronic environment, where such techniques as building audit trails into electronic recordkeeping systems can be used to document authorised disposal action. Where destruction of records is authorised, it must be done in a way that is secure and complete.

Examples of compliance with the principle

1. Records appraisal and disposal practices are established and maintained in accordance with the disposal provisions of the relevant records/archives legislation

2. Records disposal takes place in an accountable process.

3. It is possible to identify that the disposal action occurred, when it occurred, who took the action, and that the person was authorised to do so.

4. Audit trails record the disposal of electronic records in electronic recordkeeping systems.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 5: *Appraisal and disposal*

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

9. Records Should be Complete

A record should contain not only the content, but also the structural and contextual information necessary to document a transaction. It should be possible to understand a record in the context of the organisational processes that produced it and of other, linked records.

Explanation

A record comprises content, structure and context. The elements that make up the structural and contextual parts of the record are known as recordkeeping metadata.

The *structure* of a record, that is, the relationships between the metadata elements comprising a record, provides an essential part of its meaning. In a

letter, for example, structural metadata includes the different components of the letter (addressee, data, text, sender, etc.) and the order in which they appear. If they appear in a different order, or if some do not appear at all, the letter will make no sense. Maintaining structure is a particularly important requirement for electronic records.

The use of standard templates for the creation of documents provides a common structure, which is easier to maintain than multiple structures. Records in the form of electronic documents must be maintained with associated metadata in ways that retain layout, formatting and other elements of the document's structure. Thus it is not enough to retain a richly formatted document as an ASCII file: it must be retained in a format which enables the record to be rendered with its structure intact. The information content and structure of electronic records must be retained in reconstructable relations, particularly when migrating them to new software environments.

The *context* in which records were created and used in the course of business should be apparent. To document decisions and activities, it is necessary to be able to show who did what, where, when, how, and why. In some kinds of records the *content* and the *contextual information* (who took part in the transaction, when, as part of what larger activity) are separate metadata elements, which must both be maintained. Thus it is not enough to keep just the content of electronic mail messages: contextual data, such as the name and position of sender and recipient, date and time of sending, whether and when it has been read, copies sent to other people, and links to replies must also be captured and maintained.

A record must also carry the contextual linkages to other records that are necessary to understand the transaction in which it was created and used. The links between records which document a sequence of activity must be maintained.

Examples of compliance with the principle

1. Appropriate recordkeeping metadata is captured and maintained with the record.

2. The date (and time, if necessary) of a transaction is always part of the record.

3. Inwards communications are date-stamped (and time-stamped, if necessary) on receipt.

4. Document templates are used to date- and time-stamp a document on creation and to standardise the form/structure of documents.

5. Sufficient information about the business activity context in which records are made and used, and other metadata, is maintained to enable records to be understood when they are retrieved.

6. The chronological relationship between individual records which form a cumulative record of business activity is preserved.

7. An electronic mail message that is a reply to a previous one contains the previous message or a reference to it.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 3: *Strategies*

Records Management Policy and Practice Manual(subject to review), State Records of South Australia, Section 3, 1996

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

10. Records Should be Comprehensive

Records should document the whole of the business of a public sector bodies.

Explanation

Records should be made of all facets of the public sector body's operations. Recordkeeping should not be selective, so that some parts of the business have no records at all. Recordkeeping should take place in all technological environments in which the organisation carries out its business.

Records must be made for all those business transactions for which a requirement for evidence exists. While evidence of some types of transactions need only be maintained for a short time, this does not diminish the requirement for evidence during that period of time.

Public sector bodies should ensure that the operations of outsourced functions are documented adequately to satisfy recordkeeping requirements to which it is subject.

Examples of compliance with the principle

1. A public sector body has developed and promulgated common corporate policy and standards relating to recordkeeping throughout the public sector bodies.

2. Employees understand their obligations to make and keep records in the course of their duties.

3. Employees (including agents, contractors etc.) receive appropriate training and guidance in the use of recordkeeping systems.

4. Recordkeeping systems operate to capture and maintain records documenting all aspects of a organisation business, including business which is carried out electronically.

5. Records are made for all business transactions for which any requirement for evidence exists.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 2: *Responsibilities* and Part 3: *Strategies,* Clause 8: *Cases*

The Records Management Policy and Procedure Manual Template for South Australian Government Agencies, The RMAA South Australian State Government Chapter, 1997.

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

11. Records Should be Adequate

Records should be adequate for the purposes for which they are kept.

Explanation

Records are kept to support future business activity and to meet accountability requirements. A record must be adequate to the extent necessary to:

- facilitate action by employees (including agents and contractors) at any level and by their successors

- make possible a proper scrutiny of the conduct of business by anyone authorised to undertake such scrutiny, and

- protect the financial, legal and other rights of the organisation, its clients and any other people affected by its actions and decisions.

What is adequate will depend on the purpose of the record, that is, the requirement for evidence or other organisational need that it must meet. For example, a major policy initiative will be extensively documented, while a routine administrative action can be documented with an identifiable minimum of information.

There must be adequate evidence of the conduct of business activity to be able to account for that conduct within the context of relevant accountability requirements. The principal way of ensuring that this evidence exists is to keep full and accurate records.

Examples of compliance with the principle

1. A public sector body has identified what constitutes adequate evidence to meet or support each identified accountability requirement. This process can include a risk assessment, covering the likelihood of needing the evidence and the consequences of not having it.

2. The reasoning behind any decision based on a risk assessment is documented and the decision authorised at an appropriate level.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 3: *Strategies*, Clause 8: *Cases*

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

12. Records Should be Accurate

Records should correctly reflect what was communicated, decided or done.

Explanation

Recordkeeping procedures and practices must be designed to ensure that a record correctly reflects what occurred. Business processes and systems should be designed to make it easy, or even automatic, to make accurate records of transactions.

Falsifying information in a record is illegal.

Examples of compliance with the principle

1. Business rules and codes of conduct require employees (including agents, contractors etc.) to make records which accurately reflect the transactions which they intend to document.

2. Originals of inwards communications (or legally admissible copies) are kept.

3. Copies of outwards communications are signed or initialled.

4. Minutes of meetings are signed when confirmed.

5. Records creation requirements are considered in the design or redesign of any business process or system.

6. Quality control measures are built into the design of recordkeeping systems, to ensure the accuracy of data entered into them.

For further guidance

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

13. Records Should be Authentic

Records should be what they purport to be.

Explanation

It must be possible to prove that records are what they purport to be and that their purported creators, including the senders of communications, indeed created them. The recordkeeping system must operate so that the records derived from it are credible and authoritative. It should be possible to show that the recordkeeping system was operating normally at the time the records were captured by the system.

Ensuring that a record is authentic does not necessarily make it any more reliable. An authentic record can contain false or inaccurate information which may render it unreliable. Ensuring authenticity, however, minimises risk.

Examples of compliance with the principle

1. The authorised creators of records and their authorised roles in business activity are documented and kept up to date.

2. Information systems used for the conduct of business or for recordkeeping contain safeguards to prevent unauthorised users from conducting transactions or making records of them.

3. Recordkeeping systems operate normally on any given business day.

4. Recordkeeping systems should be secure to preserve the evidential quality of records.

5. Migration of records from one system to another should be controlled and documented to preserve the evidential quality of the records.

For further guidance

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

14. Records Should be Useable

Records should be identifiable, retrievable, accessible and available when needed.

Explanation

To be able to be used, records must be maintained in such a way that they can be quickly and easily identified and retrieved when they are required. Availability is different, however, from accessibility. Records are not available unless retrieval systems are adequate, but access to records may be tightly restricted (for example, for security or privacy reasons). It is not necessary that access to records be unrestricted to comply with this principle.

It is necessary, however, that the records be clearly in the control of a public sector body and available to meet its information and evidential needs when required. Small local and personal records systems which render the records inaccessible to others needing access to them (for example, in an employee's filing cabinet, on a personal computer's hard drive or in a small, unmanaged peer to peer network), should be discouraged. Official records should not be maintained personally or privately by employees. Even if access to records is limited to one person, it must be possible to demonstrate that, in the event of sudden death or removal, procedures are in place to ensure that the records automatically and routinely become available to that person's successor.

In situations where the entire record may not be made accessible for legitimate reasons, a copy should be provided with relevant portions of the record masked and a record made of its use linked to the original record. In designing

recordkeeping systems, privacy and other confidentiality requirements must be identified to ensure that records are useable while meeting those requirements.

To be useable, it must be possible to migrate or transmit a record to another system without loss of content, context and structure.

Examples of compliance with the principle

1. A public sector body knows what records it has and what records it no longer has.

2. A public sector body knows where all its records are.

3. Records are captured into corporate recordkeeping systems.

4. Records are registered, classified and otherwise controlled using systems and methods which verify their existence and enable them to be retrieved quickly and easily when needed.

5. Each record can be uniquely identified.

6. Paper-based records are managed in filing systems and are not allowed to circulate unattached or uncontrolled around the organisation.

7. Recordkeeping systems incorporate effective searching and retrieval tools.

8. Records are maintained in such a way that they can be adduced as evidence under the relevant evidence legislation and court rules.

9. The creation or use of masked records is documented and included in the audit trail.

10. Electronic records are maintained and accessible to users in electronic form.

11. Where records are maintained in technologically dependent forms, including microform or digital images, the equipment and software necessary to render them in human-readable and useable form is available and maintained over time.

12. Alternatively, where records are maintained in technologically dependent forms, they are migrated to new technological environments with minimal loss of functionality and ensuring their continued authenticity.

13. Recordkeeping systems incorporate adequate security controls to deny access to unauthorised users.

14. Records can be understood by all who are entitled to have access to them.

For further guidance

Australian Standard AS 4390—1996: *Records Management*, Part 4: *Control*

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000

15. Records Should be Inviolate

Records should be securely maintained to prevent unauthorised access, destruction, alteration or removal.

Explanation

Records should be kept using facilities, materials and methods which promote their survival undamaged for as long as they are needed. Records should be protected from tampering, unauthorised alteration, and from accidental or intended damage or destruction. The protection can include the physical security of premises, the selection of appropriate materials and systems, and procedures which hinder loss or unauthorised alteration.

No information in a record may be deleted, altered or lost once the transaction which it documents has occurred. Of course, records can legitimately be destroyed, but, while they exist, they must be inviolate.

Federal, State or Territory records/archives legislation may provide that a person must not, among other things, damage or alter a record, outside certain strictly defined exceptions. Such exceptions would include the correction of incomplete, incorrect, misleading or out of date personal information under any relevant Freedom of Information Act.

Where information is added to an existing record, for example by annotating it, (this addition is really part of a new transaction) the added information should be initialled and dated. For an electronic record, an appropriate annotation tool should be used. That is, additional information should never be added to a record in such a way that it appears to be part of the original record.

Examples of compliance with the principle

1. Recordkeeping systems and storage facilities are protected from unauthorised access, destruction or theft, or from accidental damage by fire, flood, and vermin.

2. For file based records, folios are numbered as they are attached to the file, to hinder their unauthorised removal, and their attachment is recorded on the file's minute sheet and/or using records management software.

3. Storage media and related technologies and practices for maintaining electronic records are specified, designed, operated and maintained in such a way that records cannot be altered. This can include the use of WORM disk storage systems, software and hardware based security controls and audit trails.

4. Electronic records are captured and maintained in a records data store to which users have read-only access.

5. Records appraised as requiring long-term retention are stored in an air-conditioned, dust-free environment, with stable and controlled temperature and humidity.

6. Records are maintained with appropriate security or other access restrictions. Where access to records is restricted for security, privacy, commercial or other reasons, measures to ensure such restrictions operate effectively and consistently.

7. Sound data management practices are in place, especially regular backups, copying programs, and the exercising and cleaning of storage media.

8. Disposal decisions are recorded, authorised and monitored.

For further guidance

Australian Standard AS 4390—1996: *Records Management,* Part 6: *Storage*

IM&T Blueprint Memorandum Number 3.3: Security, NSW Office of Information Technology, 1997

IM&T Guideline: Security of Information Systems, NSW Office of Information Technology, 1996

IM&T Guideline: Security of Electronic Information Systems, NSW Office of Information Technology, 1997

South Australian Government Information Technology Security Standards in an Outsourced Environment, Office of Information Technology (now available from the Government Information and Communication Services), 1994.

South Australian Government Information Technology Security Guidelines, Office of Information Technology (now available from the Government Information and Communication Services), 1994.

Government Recordkeeping Manual, State Records Authority of New South Wales, 1999

Manual for the Design and Implementation of Recordkeeping Systems (exposure draft), State Records Authority of New South Wales and National Archives of Australia, 2000