arts and culture

Department:
Arts and Culture
REPUBLIC OF SOUTH AFRICA

MANAGING ELECTRONIC RECORDS IN GOVERNMENTAL BODIES:

POLICY, PRINCIPLES AND REQUIREMENTS

National Archives and Records Service of South Africa
April 2006

National Archives and Records Service of South Africa
Private Bag X236
PRETORIA
0001

Fax: (012) 323 5287
Fax to e-mail: 086 682 5055
E-mail: erecords@dac.gov.za

http://www.national.archives.gov.za

ISBN 1-919965-02-05

First Edition, Version 1.1, April 2003
First Edition, Version 1.2, April 2004
Second Edition, April 2006

Acknowledgement

In the compilation of these Policy Guidelines, considerable use has been made of guidelines produced by other National Archives and related institutions and individuals and made public on the Internet. In some cases, material derived from these sources has been used verbatim. Specific acknowledgement of the sources is made in the Bibliography.

Content

PREFACE

The increasing use of electronic systems by governmental bodies to conduct their business has significantly changed the way that records are created and kept. Electronic record keeping poses particular challenges to governmental bodies and to the National Archives and Records Service, both of which need to ensure that reliable records are maintained over time as evidence of official business for the purposes of accountability, operational continuity, disaster recovery and institutional and social memory. With paper-based records, provided a well-structured file plan is maintained and the records are physically protected, the evidence they contain remains accessible and readable over time. However, in the rapidly-changing technological environment, the same cannot be said of electronic records.

It is essential for governmental bodies to give specific consideration to the preservation of electronic records as part of a formal policy of managing records. To promote strategies for the appropriate management of electronic records of government, the National Archives and Records Service of South Africa Act (No 43 of 1996, as amended) contains two provisions specifically regarding electronic records systems: that the National Archivist shall determine the conditions subject to which electronic records systems shall be managed, and also the conditions subject to which public records may be electronically reproduced (section 13(2)(b)(ii) and (iii)). As with other public records, the legislation provides that electronic records may not be disposed of without the written authorisation of the National Archivist (section 13(2)(a)). The legislative provisions regarding archival custody take the special needs of electronic records into account, in that while public records that have been appraised as having archival value are to be transferred to archival custody after 20 years, the National Archivist may in consultation with the head of a governmental body identify records which should remain in its custody or should be transferred to archival custody at an earlier time (section 11(2)(b)).

The purpose of this document is to provide guidance to governmental bodies to assist them to comply with legislative requirements regarding electronic records as an integral part of the strategic management of their records resources. The policy, principles and requirements contained in this edition build on the guidelines that were established in the first edition, which was entitled *Managing electronic records in governmental bodies: Policy guidelines,* versions 1.1 and 1.2 of which were published in April 2003 and April 2004 respectively. This second substantially expanded edition entitled *Managing electronic records in governmental bodies: Policy, principles and requirements* places more emphasis on the requirement to create authentic electronic records that are useable and reliable for as long as they are required for functional, legal and historical purposes. The guidance proposes a strategy that is aligned with international standards and best practices. Without such strategic management, the records of governmental bodies will be insecure and the effective functioning and accountability of bodies, based as it is on the information held in their own records, will be jeopardised. And there will be no long-term institutional and social memory of the present age in the custody of the National Archives and Records Service.

Dr Graham Dominy
NATIONAL ARCHIVIST
APRIL 2006

Second Edition
April 2006

1. INTRODUCTION

Records are the output of the business and administrative processes of a governmental body. In other words, the final proof that a business or administrative process was transacted. It serves as essential proof of the business that was conducted and should remain unaltered over time for as long as they are needed. As evidence of official business records have on-going use as a means of management, accountability, operational continuity, legal evidence and disaster recovery. They also form the memory of the institution that created them, and by extension, they are part of society's memory and the broader cultural heritage. In some cases records also have a bearing on the rights of citizens. A body's ability to function efficiently and give account of its actions could be negatively affected if sound records management principles are not applied. The need for effective management of records is enhanced by the Public Finance Management Act, 1999, the Promotion of Access to Information Act, 2000, the Promotion of Administrative Justice Act, 2000, and the Electronic Communications and Transactions Act, 2000 in terms of which governmental bodies have an obligation to manage their records properly, to provide access to information contained in records, provide reasons for administrative decisions and to ensure the authenticity of records.

Since one of the National Archives and Records Service's objectives is to preserve public records with enduring value for use by the public and the state, the National Archives and Records Service is not only concerned with the management and accessibility of records over a short period of time. Records created in electronic and paper-based record keeping systems contain the memory of the decision-making of government and its impact. The National Archives and Records Service has a responsibility to ensure that this memory is maintained and protected for centuries to come. To facilitate this the National Archives and Records Service's role in terms of the National Archives and Records Service of South Africa Act, 1996 as amended is to promote efficient administration by regulating the records management practices of governmental bodies to ensure the sound management of the information resources.

Records management is a process of ensuring the proper creation, maintenance, use and disposal of records to achieve efficient, transparent and accountable governance. In short, sound records management ensures that all the records that governmental bodies creates in the conduct of their official business are, and remain, authoritative and authentic.

The impact of technology on official business and therefore on records management is not a new phenomenon. For example the introduction of the telegraph, typewriter and the telephone fundamentally altered the way business was done and records were kept.

The advent of the computer altered record keeping even more. Computerised systems offer significant advantages over conventional manual methods. In particular, they can manipulate large amounts of information and generate a wide range of information products. Computers offer speed, precision, diversity, flexibility and a rich and comprehensive documentation of process, and it is no wonder that they have been so quickly embraced around the world as a critical information management and communication tool.

However, the unique and fragile nature of electronic data demands a re-evaluation of the way governmental bodies manage records. Processes and procedures created to meet the needs of record keeping in the paper environment do not apply equally to electronic records. A reassessment of records management programmes is therefore required. In order to meet record keeping responsibilities, governmental bodies must ensure that electronic records are accessible and readable over time. An active programme committed to managing and preserving records from their creation to final

disposal is a prerequisite of meeting these responsibilities. Any breakdown in the records management process increases the chance that electronic records that still have value to the body will become unreadable and inaccessible over time.

1.1 Statutory and regulatory framework

The statutory and regulatory framework in which sound records management is founded is the following:

The Constitution, 1996

Section 195 of the Constitution provides amongst others for the:
- effective, economical and efficient use of resources;
- provision of timely, accessible and accurate information; and requires that
- the public administration to be accountable.

National legislation enacted to give effect to the provisions in this section is the following:

The National Archives and Records Service of South Africa Act (Act. No. 43 of 1996 as amended)

Section 13 of the Act contains specific provisions for efficient records management in governmental bodies. It provides for the National Archivist-
- to determine which record keeping systems should be used by governmental bodies;
- to authorize the disposal of public records or their transfer into archival custody; and
- to determine the conditions -
  - according to which records may be microfilmed or electronically reproduced;
  - according to which electronic records systems should be managed.

The **National Archives and Records Service of South Africa Regulations**[1] was published in terms of section 18 of the National Archives and Records Service Act. Part V: Management of Records contains the specific parameters within which the governmental bodies should operate regarding the management of their records.

The Public Finance Management Act (Act. No. 1 of 1999) and Municipal Finance Management Act (Act. No. 56 of 2003)

The purpose of these Acts are to regulate financial management in the public service and to prevent corruption, by ensuring that all governmental bodies manage their financial and other resources properly.

The Promotion of Access to Information Act (Act. No. 2 of 2000)

The purpose of the Act is to promote transparency, accountability and effective governance by empowering and educating the public
- to understand and exercise their rights;
- to understand the functions and operation of public bodies; and
- to effectively scrutinize, and participate in, decision-making by public bodies that affects their rights.

1 Regulation 158 of 20 November 2002.

In this Act the definition of a record is similar to that in the National Archives and Records Service of South Africa Act namely "recorded information regardless of form or medium". Governmental bodies cannot refuse access on grounds that a record is in an electronic form (including an e-mail). This implies that an electronic record (including an e-mail) like any other record should be managed in such a manner that it is available, accessible, and rich in contextual information. By implication electronic records (including e-mails) should be managed in proper record keeping systems and the disposal of electronic records (including e-mails) should be documented and executed with the necessary authority.

The Promotion of Administrative Justice Act (Act. No. 3 of 2000)

The purpose of the Act is to ensure that administrative action is lawful, reasonable and fair and properly documented.

The Promotion of Administrative Justice Act imposes a duty on the state to ensure that administrative action is lawful, reasonable and procedurally fair. Everyone whose rights have been adversely affected by administrative action has the right to be given written reasons for such an action. If an administrator to whom a request was made fails to furnish adequate reasons for an administrative action, because the history of that action was documented in e-mail messages or records that were destroyed, it could be presumed that the administrative action was taken without good reason. The administrator then runs the risk of legal action being taken against him/her or his/her organization. Relating this back to the management of records - unauthorized destruction of records (including e-mails) could be considered a deliberate action to conceal the reasons for administrative actions. Any destruction of public records should be done in accordance with a written disposal authority issued by the National Archives and Records Service or its provincial equivalents.

The Electronic Communications and Transactions Act (Act. No. 25 of 2002)

The purpose of the Act is to legalize electronic communications and transactions, and to build trust in electronic records.

According to the Electronic Communications and Transactions Act data messages are legally admissible records, provided that their authenticity and reliability as true evidence of a transaction can be proven beyond any doubt. The evidential weight of electronic records (including e-mails) depends amongst others on the reliability of the manner in which the originator and the receiver managed the messages. Should bodies not have a properly enforced records management and e-mail policy and a reliable and secure record keeping system, bodies run the risk that the evidential weight of their electronic records (including e-mails) is being diminished.

Efficient records management practices are imperative if a body wants to give effect to the provisions of these Acts.

Besides the above mentioned acts a number of other laws compel governmental bodies to manage information and records so that they are readily available and accessible when needed. The legislation and standards mentioned above are generally applicable to all governmental bodies. There are also non-generic laws that applies to specific governance clusters and governmental bodies and although not mentioned specifically

these should also be kept in mind when reading this document.[2]

1.2 Benchmark

The strategies described in this document are based on two fundamental pre-requisites. The first is the need to understand the concept of "record" and the second is to have in place a strategy that addresses the management of records regardless of their physical form. The management of electronic records must be addressed within the broader context of the policies, standards and practices that deal with the management of all forms of recorded information, even though specific types of media may be handled differently.

The National Archives and Records Service endorses the South African national standard SANS 15489: *Information and documentation – Records management – Part 1: General and Part 2: Guidelines* as the required benchmarking tool for records management and, in terms of its statutory mandate, requires governmental bodies to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner. To this end the National Archives and Records Service requires governmental bodies to implement and maintain Integrated Document and Records Management Systems, which have built in records management functionality. Should governmental bodies consider deploying Enterprise Content Management Solutions or Smart Enterprise Suites, an Integrated Document and Records Management System should be a core component of these solutions.

Until a specific South African standard for electronic records management software is available the National Archives and Records Service also endorses the US DoD 5015.2 *Design Criteria Standard for Electronic Records Management Software Applications* and the UK National Archives' *Functional Requirements for Electronic Records Management Systems*. (See the bibliography for links to both standards) as benchmarking tools. Certification against these standards would ensure that electronic records management applications have the records management functionality required by the National Archives and Records Service. However, if the business needs of a governmental body require the use of an Integrated Document and Records Management System product suite of which the records management functionality is not certified against these standards, the National Archives and Records Service requires that they use the National Archives and Records Service's draft *Functional Specification for Integrated Document and Records Management Solutions*[3] as part of the specification in their requests for tenders. When using the draft functional specification, governmental bodies should however ensure that the records management requirements of the National Archives and Records Service are integrated with their own business requirements. The draft functional specification contains generic requirements and should not be considered sufficient to replace the need for a proper investigation into the unique business requirements of an office.

The National Archives and Records Service also recommends compliance with the National Intelligence Agency's *Minimum Information Security Standard*[4] and the

2 The company Mostert, Goodburn and Opperman recently did extensive research about records retention requirements in legislation. For more information contact Wim Mostert tel.: 011 802 2278, cell.: 082 378 9720, e-mail: wim@mostert.co.za

3 The draft functional specification is currently under revision. Copies of the original draft can be obtained from Louisa Venter of the National Archives and Records Service, Tel.: 012 323 5300; e-mail: Louisa.Venter@dac.gov.za.

4 To obtain copies of this standard contact the National Intelligence Agency, Private Bag X87, PRETORIA, 0001, tel. 012 427 4000, fax 012 427 4651.

Department of Public Service and Administration's *Draft Information Security Policies*[5].

The National Archives and Records Service also endorses the following national standards with a view that they would guide governmental bodies in creating authoritative and reliable records:

- SANS 15801: *Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability*; and
- SANS 23081: *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*.
- the National Intelligence Agencies' *Minimum Information Security Standard* and the Department of Public Service and Administration's *Draft Information Security Policies*[6], and
- SANS 17799: *Information technology – security techniques – Code of practice for information security management*.[7]

1.3 Objective of this publication

While the National Archives and Records Service of South Africa Act, 1996 assigns responsibility for determining the conditions subject to which electronic systems should be managed to the National Archivist, the heads of governmental bodies are accountable for the implementation of the National Archives and Records Service's requirements.

This publication aims to provide guidance to heads of governmental bodies regarding the management of electronic records and systems. The publication entitled *Electronic records and the law: What governmental bodies need to know* serves as an introduction to the National Archives and Records Service's policy for managing electronic records. It briefly defines the concept of electronic records, the legal implications pertaining to these records, the National Archives and Records Service's strategy for electronic records management, and the obligations of governmental bodies. *Managing electronic records in governmental bodies: Policy, principles and requirements* supersedes the *Guide to the management of electronic records in governmental bodies* of which First and Second Editions were published in 1999 and 2000 respectively and *Managing electronic records in governmental bodies: Policy Guidelines* version 1.1 (April 2003) and version 1.2 (April 2004). These guidelines contain a substantial amount of new information, particularly regarding the benchmarking of the National Archives and Records Service's requirements, the definition of electronic records, authenticity of electronic records, integrated management of records in all formats and the responsibilities of governmental bodies as well as new information regarding the management of electronic records without the benefit of Integrated Document and Records Management Systems.

The management of electronic records is a complex matter for which it is not possible to provide a simple set of guidelines applicable to all cases. However, the guidelines set out in this publication provide an approach that is applicable to most electronic records, and can be refined to suit particular cases.

---

5 Department of Public Service and Administration, *Draft Information Security Policies. Securing Information in the Digital Age.* http://www.info.gov.za/otherdocs/2001/infosecure.pdf

6 Department of Public Service and Administration, *Draft Information Security Policies. Securing Information in the Digital Age.* http://www.info.gov.za/otherdocs/2001/infosecure.pdf

7 This code of practice could be used by governmental bodies that are not subject to the *Minimum Information Security Standard* to guide the design of information security implementation. Governmental bodies that are subject to the *Minimum Information Security Standard* should consult with the National Intelligence Agency before they use this code. To obtain copies of all these standards contact the South African Bureau of Standards' Sales Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria; Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Telefax: (012) 428-6928; E-mail: sales@sabs.co.za.

1.4 Intended audience

The policies, principles and requirements in this document are applicable to all governmental bodies viz. any legislative, executive, judicial or administrative organ of state (including a statutory body) at the national level of government, and until provincial archival legislation takes effect, also all provincial administrations and local authorities. As soon as archival legislation comes into force in a specific province, such provincial offices and local authorities will receive specific guidelines from the relevant provincial archives service. The guidelines issued by the provincial archives services will not be inconsistent with these guidelines. Should a provincial archives service however prefer to continue using these guidelines, they should be read in conjunction with that province's specific archives and records management legislation.

2. THE NATIONAL ARCHIVES AND RECORDS SERVICE'S ELECTRONIC RECORDS MANAGEMENT STRATEGY

While its practical experience in the field is still limited, the National Archives and Records Service has adopted a strategy underpinned by a legal framework explicitly provided for in the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended). The Act specifies in sections 13(2)(b)(ii) and 13(2)(b)(iii) that the National Archivist must determine the conditions subject to which records may be reproduced electronically as well as the conditions with regard to the way electronic records systems must be managed.

The National Archives and Records Service's electronic records management programme is aligned with the regulatory requirements of the State Information Technology Agency (SITA), the Department of Public Service and Administration (DPSA) and the Government IT Officers' Council (GITOC) and is built on the following four-pronged strategy:

- Archival involvement in the design and maintenance of electronic records management systems. Archivists cannot, as they can in the paper environment, rely on their capacity to pick up the pieces when records are no longer required by their creators. The National Archives and Records Service of South Africa Act allows the National Archives and Records Service to insist that mechanisms and procedures be put in place to ensure that archival records are identified while still functional and then preserved appropriately. To this end the National Archives and Records Service requires that
  - electronic records should be managed according to the principles contained in this document;
  - electronic correspondence systems should be managed with **electronic records management applications** as part of an Integrated Document and Records Management System that manages records in all formats in an integrated manner;
  - electronic records should be managed as part of the broader records management strategy of a governmental body; and
  - structured and legacy systems should be managed with a **schedule for electronic records systems** as an instrument for obtaining disposal authority and use as a disposal schedule.

- The earliest possible transfer into archival custody of electronic records with enduring value. In terms of the National Archives and Records Service of South Africa Act, 1996, governmental bodies are only obliged to transfer archival records into archival custody when they reach 20 years of age. The National Archivist is however empowered to determine shorter transfer periods when appropriate. This shortened transfer period applies to electronic records.

- The identification of archival electronic records which should remain in the custody of the creating body. Circumstances in which this approach might be considered include the following: where the cost of transfer into archival custody is prohibitive; where technical considerations like data complexity and software copyright raise insuperable barriers; where the creating body, because of its facilities and/or the nature of the record, is best positioned to provide archival user services; or where statutory provisions exist which prevent transfer to archival custody. The National Archives and Records Service of South Africa Act, as amended specifically empowers the National Archivist to make such an arrangement with creating bodies.

  Should archival electronic records be earmarked for preservation by a governmental body, the National Archives and Records Service would require that such a body

creates a trusted digital repository that conforms to the *Open Archival Information System Reference Model*[8], in which

- data can be maintained in the long term without being damaged, lost or altered;
- data can be retrieved comprehensively; and
- that captures sufficient contextual information to ensure that the data can be understood by the user over time.

The management of a trusted digital repository should take the guidelines in SANS ARP 077 – *Document Management Applications - Long term preservation of electronic document-based information*[9] into account.

The National Archives and Records Service would also require that the governmental body capture the necessary preservation metadata to ensure that the authenticity of the archival records can be proven beyond any doubt. Preservation metadata should record information regarding:

- the custody history of the archival electronic records;
- the authenticity of the archival electronic records, e.g. whether the records and/or the metadata was changed;
- preservation activity e.g. conversion and migration actions;
- the technical environment e.g. hardware, operating system and software applications that created and stored the records;
- rights management, e.g. information about security classification, access restrictions and intellectual property rights.

- The identification of non-archival electronic records that can be disposed of as part of an offices' normal administrative practice. Most electronic systems, for which disposal authority has been applied to date, do not possess archival value, while systems that might have archival value are seldom reported. To attempt to streamline matters, two general disposal authorities authorising the destruction of ephemeral electronic records have been prepared. (See Annexures D and E). These general disposal authorities enable governmental bodies to dispose of electronic records that do not have archival value without specifically applying for disposal authority, so that the focus can be placed more appropriately.

8 ISO 14721 may be considered for adoption as a South African national standard during 2006/2007.

9 This recommended practise is based on ISO 18492 – *Document Management Applications - Long term preservation of electronic document-based information*. To obtain copies of this standard contact the South African Bureau of Standards Sales' Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria; Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Telefax: (012) 428-6928; E-mail: sales@sabs.co.za.

3. WHAT IS AN ELECTRONIC RECORD?

3.1 Definition

The National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) defines a **record** as recorded information regardless of form or medium. Examples of **form** are correspondence files, maps, plans, registers, etc. Examples of **media** are paper, microfilm or electronic format. **Public records** are those created or received in the course of official business and which are kept as evidence of a governmental body's functions, activities and transactions.

Electronic records means information which is generated electronically and stored by means of computer technology, while an **electronic records system** is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and metadata (descriptive, background and technical information regarding the information stored electronically.)

Electronic records can either exist in structured applications, which hold transactional records (i.e. Persal, Logis etc.) or in unstructured applications (i.e. electronic records generated on individual PC's and in e-mail systems).

The introduction of computers has raised difficult questions regarding record status. Traditionally records have been defined as physical objects such as paper files, tapes, disks, etc. Such traditional definitions are, however, problematic when it comes to dealing with electronic records. For instance, a disk can contain records. However, if the disk cannot be read, the record effectively no longer exists. With electronic records, therefore, the physical object or disk is not the record. Defining electronic records in terms of physical objects is not useful and specific programming or planning is required to ensure that the essential characteristics of the record are maintained.

Three properties are necessary to ensure the maintenance of the essential characteristics of a record, namely **content, structure and context**. These properties are fused in a single physical paper document. Visible to our eyes, we can read the text or content of the document. We can also see its physical structure: the document that is a ledger or cashbook will have a different format to a letter. Finally, we can easily deduce the context. A letter, for example, will show from whom and to whom it was written, the date it was written and the date it was received stamped on it, and its heading, file number and position in the file will all contribute to the context in which it was written and received.

In an electronic system, the properties of content (the information a record contains), structure (the appearance and physical layout or type) and context (the intended use, purpose and recipients, etc) may be physically separate. An electronic database may contain content in the form of data, but the information on its structure (such as the record format) and context (what other records it relates to) may be kept separately in software, technical documentation and directories. The problem is that content on its own does not constitute a record as it is not sufficient to guarantee authenticity or reliability for legal purposes or operational continuity, and without context it is difficult to interpret the full meaning of a document. An example of such a situation would be a database containing correspondence without any form of subject classification system or meaningful reference numbers, or links between related documents, which is searched in a hit-or-miss method by arbitrary keywords only. As technology has developed, the problem of content, context and structure not being integrated has become more acute. Some systems are designed to maintain different types of information as separate entities, and the software then creates a temporary record in answer to a specific query

bringing together information that is kept in different physical entities.

Unless archival considerations are built into an electronic system to ensure the maintenance of the essential characteristics of records, it may not in fact contain records, but merely information or data. Precisely for this reason the National Archives and Records Service endorses the use of and compliance to international standards to ensure that authoritative and reliable records are created and preserved.

3.2 Documents, records, content and digital assets

The debate about the difference between “documents” and “records” has been raging for more than a decade now, without a conclusion being reached. Adding “content” and “digital assets” to the equation has complicated matters even further.

For the purposes of the National Archives and Records Service Act, the following applies: The Oxford Dictionary defines a document as “a piece of written, printed or electronic matter that provides information or evidence or that serves as an official record”, while SANS 15489: *Information and documentation – Records management – Part 1: General and Part 2: Guidelines* defines a document as recorded information an object which can be treated as a unit. The National Archives and Records Service Act defines a record as “recorded information regardless of form or medium” and in practice a record is also defined as “evidence of a transaction”. With this in mind, and from the National Archives and Records Service’s perspective every electronic document generated has the potential to be a public record and should therefore be managed properly throughout its life-cycle.

Content is the data or information inside a record or according to the Oxford Dictionary “the material dealt with in a speech, literary work, etc as distinct from its style and form”. Content is the reason behind creation of a record. Without informational content a record has no reason to exist.

Digital assets constitute visually rich recorded information like images, logos, audio, video, 3-dimensional drawings, graphics etc. In other words records that are not text-based.

One could go further and say records are either text-based (documents) or visually rich (digital assets) and they all contain informational content.

The National Archives and Records Service’s view is that all the foregoing are records. They constitute recorded information regardless of form or medium. These terms are sometimes used interchangeably in this document.

The National Archives and Records Service is of the opinion that the question should rather be whether the document, digital asset or content is an official record or not. The National Archives and Records Service distinguishes between transitory records, i.e. records with a fleeting life-span that do not become part of the official record keeping system and can be disposed of in terms of General Disposal Authority AT2 and official records, i.e. the official evidence or account of the business operations of a governmental body that are known as public records.

Both transitory records and official records regardless of format or medium should be managed properly. They should be managed according to sound records management principles throughout their entire life-cycle from the moment they are created until they are no longer needed to ensure that they are and remain authentic and reliable.

3.3 Records life-cycle versus records continuum

The life-cycle concept is a comparison with the life of a biological organism, that is born, lives and ultimately dies. In the same way, a record is created, is used while it still has value and then it is disposed of.

Efficient life-cycle management of records is a key concept in records management. Without proper life-cycle management records clog up expensive space and it becomes impossible to retrieve important administrative, financial and legal information. If governmental bodies do not control records through the earlier stages of their life-cycle, records that have low administrative value are kept for too long and those of archival value cannot be identified and safeguarded.

Closely related to this is the concept of the records management continuum which suggests that four actions recur throughout the records life-cycle, namely

- the creation of records;
- placing records within a logical, documented system that governs their arrangement and facilitates their retrieval throughout their life-cycle;
- their maintenance and use; and
- their appraisal for continuing value, recorded in disposal authorities and given effect when they are no longer needed.

When managing records the life-cycle concept and the records continuum are combined in a seamless process. From the National Archives and Records Service's perspective proper life-cycle/continuum management requires that the electronic records should be managed from the moment they are created to their archival phase by:

- placing them in logical, documented record keeping systems to enable their retrieval and use;
- managing the disposal process;
- managing the systematic migration of records across new software and hardware platforms to ensure that they remain accessible;
- preserving the security, authenticity and integrity of records to enable their permanent preservation and admissibility as evidence in court;
- maintaining the relationships between records and the processes that created them;
- associating the contextual and structural data within a document to enable it to be a proper and reliable record; and
- constructing and managing proper metadata and audit trails to ensure the legal admissibility of the records.

The policy, principles and requirements that follow are provided in an attempt to ensure that records management processes are integrated into business processes to enable electronic records to be managed continuously throughout their entire life-cycle.

4. WHY SHOULD ELECTRONIC RECORDS BE MANAGED AND PRESERVED?

As records creators, most public servants have no real mandate, and very little incentive, to concern themselves with the care and management of records after they are done with them. Records managers/archivists however have a mandate to preserve the records for the remainder of their life-cycle. Records managers are concerned with a core set of tasks, e.g. classifying records, storing them in a logical fashion, tracking their location, retrieving them when needed for business reasons and destroying them or moving them into archival custody when no longer needed. Flowing from this, just some of the things that have to be applied to electronic records are:

- For all records, it must be clear how long they have to be retained, and whether they are to be destroyed or archived;
- Records of a sensitive or other special nature must be clearly identified and protected;
- Appropriate access control must be maintained for as long as the organisation needs the records;
- There must be a means whereby electronic records can be grouped or otherwise organised for formal disposal.

In short, governmental bodies need a practical means whereby the responsibility for electronic records can pass from the originator, to the people responsible for the corporate memory of the body and then into the archival phase without jeopardising the integrity and reliability of the records.

Government envisages a society where information is managed as a strategic resource, a culture of sharing and re-using of information exists and where the public has access to credible information. Government also envisages the implementation of e-government as the best way to enable the public to gain access to information and to transact with government. This is only possible if governmental bodies capture accurate and reliable records and if they manage their records in an integrated manner. By classifying records and by establishing retention periods in advance, it is more likely that the public will gain access to the right information at the right time and less likely that records will be inadvertently destroyed while they might still be needed for functional, legal or historical purposes or that access to information that should have been protected might be provided. This would be a serious contravention of the requirements of the envisaged data protection legislation.

Records management is the basis for sharing and re-using of information as well as for providing access to understandable records. Sound records management principles assist governmental bodies to file records in order to enable them to retrieve the records easily when they are needed. It also helps governmental bodies to know

- which records to provide access to and which not;
- which records to destroy, and when to destroy them.

5. ELECTRONIC RECORDS MANAGEMENT PRINCIPLES

The following principles apply to the management of records in electronic systems.

5.1. Classification systems

To support the continuing conduct of business and provide accountability, governmental bodies should create and maintain authentic, reliable and usable records. They should protect the integrity of the records by capturing them into record keeping systems that routinely capture all records, organise the records in a way that reflects the functions of the office, protect the records from alteration and/or unauthorised disposal, and provide ready access to the information contained in the records.

Records can only be interpreted if the underlying relationship between the records is understood. To provide the underlying relationships it is crucial that the records captured into the record keeping system should be classified intelligently by organising them into categories/subjects through which users can navigate to find individual records. Classification refers to the process whereby electronic records stored in the electronic repository are assigned subjects in the classification system that matches the records subject. If this is done consistently for all electronic records, the disposal and retention decisions will be properly applied to the right records, and they will be archived/destroyed at the right times. The staff will also spend less time looking for information and more time actively acting on the information.

To ensure that authentic and reliable records are created and maintained, the records should be captured into the managed environment of the classification system **at creation.**

The functional subject file plan principles prescribed by the National Archives and Records Service organise documents into **categories that reflect the functions/business of a body.**

A file plan is a visual representation of the functions/activities/transactions performed and the records generated by an office during the conduct of business. It is a conceptual model of a business classification schema represented as a hierarchical structure consisting of headings and folders to indicate where and when records should be created during the conducting of the business of an office. In other words the file plan links the records to their business context. Consequently a file plan should be a complete and comprehensive representation of all the functions/activities/transactions performed and records created by an office. A file plan is also a hierarchical representation of the metadata attributes that link an individual record to the specific functions/activities/ transactions that generated the record. For more information about metadata, see par. 5.1.5.

Disposal instructions with retention periods are determined for each unique subject in a file plan. The file plan with the disposal instructions and the retention periods attached is called a disposal schedule/disposal authority.

Guidelines regarding the drafting of a file plan and the procedures to have it formally approved by the National Archives and Records Service are available in the *Records Management Policy Manual*.[10]

10 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za. Alternatively hard copies can be obtained from the Records Management Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

5.2 Appraisal and disposal

While all records need to be appraised timeously by archivists to identify those records that have archival value and thereby promote a systematic disposal programme, it is crucial for the appraisal of electronic records to take place at an early stage. Conceivably, a terminated system of paper-based correspondence files can be appraised after the lapse of many years, because their content, structure and context will have been maintained as part of the records themselves. In contrast, it could be very difficult to appraise a terminated electronic system, as sufficient information on its functioning may not have been retained and it may not even be able to be accessed, owing to having used hardware and software which have become obsolete.

Since the cost of storing digital information is lower than the cost of storing paper-based records governmental bodies may be of the opinion that appraisal and disposal are not necessary in the electronic environment. Storing ever-increasing amounts of electronic records may not have huge cost implications in the short term but the long-term implications of degrading software performance and impeded access to critical information is a concern.

Meaningful information and records retention policies are even more critical in the electronic environment due to the volume of the records so created. Records should only be retained for as long as they have value for business, legal or historical purposes. Retaining unneeded information has direct and indirect costs. Direct costs are for example, additional disk space, bandwidth, hardware, software and migration while indirect costs are for example, the staff necessary to maintain the systems and the cost of the time it takes to retrieve records, as well as the back-up and disaster recovery cost.

However, this does not imply that records can be deleted at the discretion of the users. Appropriate appraisal scheduling and disposal procedures should be applied to electronic records. If not, records needed for litigation or investigation purposes or to comply with an access to information request, may be inadvertently destroyed. Such actions can be seen as obstruction of justice. Governmental bodies should obtain a written disposal authority from the National Archivist and for those records that are deemed non-archival, document their retention decisions. Governmental bodies should also be aware that notwithstanding the provisions of any other Act of Parliament to the contrary (e.g. the Electronic Communications and Transactions Act, 2002) no electronic records may be deleted without a prior written disposal authority issued by the National Archivist. This should be strictly adhered to, by ensuring amongst others that destruction of original records after imaging is only done

a) in terms of a written disposal authority; and
b) if the authenticity of the images is supported by a detailed policy document and a reliable and auditable process based on dependable technology and properly documented processes.

The procedures for obtaining a disposal authority are contained in the *Records Management Policy Manual*.[11]

11 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za. Alternatively hard copies can be obtained from the Records Management Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

5.2.1 Transfer

One of the purposes of appraisal is to identify, early in the records life-cycle, which records have long-term archival value and should be preserved as part of the national archival heritage. Records so identified have to be transferred into archival custody.

To ensure that the authenticity of records can be proven after they have been transferred, it is necessary that the transferring institution as well as the new custodian establish controls over the transfer that would demonstrate an unbroken chain of custody. The controls would include establishing, implementing and monitoring procedures for registering the records' export; verifying the authority for export; examining the records to determine whether they correspond to the records that are designated in the disposal authority governing their export; and formally importing the records on to the new platform.

The assessment of the authenticity of the creator's records should be verified. This includes verifying that the metadata and audit trail data relating to the identity and integrity of the records have been carried forward with them along with any relevant documentation.

It is recommended that the following controls should be implemented by the new custodian: access privileges concerning the access, use, and reproduction of records; procedures to prevent, discover, and correct loss or corruption of records, as well as procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change. The privileges and procedures should be effectively implemented and regularly monitored. If authentication of the records is required, the custodian should establish specific rules regarding who is authorized to authenticate them and the means of authentication that will be used.

5.2.2 Destruction

The sound management of the destruction process is equally important. Should destruction actions not be documented properly, any destruction of records could be seen as deliberate obstruction of justice.

The necessary controls should be in place to ensure that it can be proven that destruction of records was carried out in terms of a documented process. These would include documenting in the records management policies that no records may be destroyed without a written disposal authority being issued, obtaining a disposal authority from the National Archives and Records Service and keeping it on record, determining retention periods and documenting the reasons behind the retention periods, documenting when and how destruction should be carried out, documenting the names of officials responsible for authorising destruction processes, ensuring that destruction certificates are compiled and kept on record, and documenting destruction actions in audit trial data.

It is also necessary to document in policy and procedures in which cases destruction holds should be placed on records, who should authorise a destruction hold and who is responsible for reviewing a destruction hold.

Having these controls in place would ensure that the legality of destruction processes can be proven beyond doubt.

5.3 Accessibility

Records which are created by using the hardware and software technologies of today should remain available, usable, understandable and authentic over a long period of time.

In terms of the National Archives and Records Service of South Africa Act governmental bodies are only obliged to transfer archival records into archival custody when they reach 20 years of age. However, archival electronic records cannot be left for 20 years before preservation actions are taken because technology changes so rapidly that the storage media outlast the software and devices needed to read the content on the storage media. Furthermore, and even more critically, digital longevity is also dependent on the formats in which the records were generated. New releases of software do not necessarily enable access to older formats, and as a consequence the records generated in obsolete formats may become inaccessible. Steps have to be taken to ensure that the records themselves are adapted or migrated to be compatible with the new formats, storage media and systems as technological change takes place.

To enable electronic records to be used over time, they must remain readable by computer and intelligible to humans. This however, does not mean that obsolete hardware and software should be preserved along with the records to ensure access to electronic records. Rather, steps have to be taken to ensure that the records themselves are adapted or migrated to be compatible with the new systems as technological change takes place.

5.3.1 File formats

A file format is encoding that makes electronic objects readable by translating the object to a human readable form with format software. Accessibility of records occurs at format level. Format is thus fundamental to all accessibility and preservation actions.

Since the accessibility of electronic records occurs at format level, it is very difficult to keep electronic records accessible and to preserve them over time without managing file formats properly. Too many digital formats exist and many formats are obsolete already. Furthermore, file formats are not necessarily compatible backwards.

Since most records are created using specific, proprietary software applications a long-term view is required to ensure that the risk of format obsolescence is managed timeously. Non-proprietary formats are few in number and each has its limitations e.g. records converted to ASCII format or rich text format lose structure and functions. At this stage PDF seems to be the better choice because an archival version known as PDF/A was recently published as an International Standard. This does however not mean that PDF is problem free. PDF has a problem with backward compatibility with newer versions struggling to render older versions correctly.[12] XML also currently seems to be a format of choice since it is hardware and software independent and a text based, self describing, human readable mark up language. However, there is no guarantee that these formats will last into the future. Proper attention to file format obsolescence requires an up-front commitment of time and money to ensure that records remain accessible.

Migration of records is only part of the solution. Migration transforms today's formats

12 This is one of the reasons behind the standardisation of an archival PDF-format contained in ISO 19005-1: *Document Management Applications – Electronic document file format for long term preservation – Part 1: use of PDF 1.4 (PDF/A-1)*.

supported by specific software platforms to new formats for new software platforms. Governmental bodies need to make informed decisions about format migration. It is important that they know which formats are best for accessibility and preservation at a specific time. It is also important that they know something about the durability of the formats that they are working with to enable them to make informed decisions about format migration. It may for example not be necessary to migrate to new formats immediately when they become available, but only a few years down the line, because the risks inherent in new formats may be the same as the risks inherent in the current formats. Governmental bodies may only need to convert records to a software independent format to ensure that they remain accessible, for example converting from MS Word to PDF.[13] It may also be that there is a need to convert records before they are migrated to ensure that they remain accessible. Governmental bodies should consider the risks involved before a specific action is decided upon. Migration strategies are also format dependent and there is no guarantee that the newly chosen format will last.

It is recommended that governmental bodies set up a format watch strategy. Format watch can be done by using the functionality of existing file format registries, like the UK National Archives' PRONOM file format registry.[14] Information on other file format registries that are available internationally is available on the Global Digital Format Registry[15], the Format Registry Demonstrator[16] and the Inform Methodology[17]. The purpose of a file format registry is to preserve information about the durability of file formats, to document the specification of obsolete, current and new formats and to document reliable migration paths to new formats. Having a format watch strategy in place would provide governmental bodies with the ability to determine when format conversion or migration should be done.

It is also recommended that governmental bodies limit their use of proprietary file formats. Proprietary formats are controlled and supported by a single software developer or can only be read by a limited number of other programmes. It is preferable to use non-proprietary formats that are supported by more than one developer and can be read by many other software systems.

5.3.2 Storage media

Even though longevity of storage media is not the most important issue in the management of electronic records, it is necessary to know that records cannot be accessed if storage media cannot be read. There are two factors that influence the readability of storage media, namely

- physical care; and
- technological advancement.

When identifying records that must be preserved indefinitely, the special requirements regarding the medium in which these records must be preserved to ensure accessibility in future, can be set at an early stage. Electronic storage media are inherently unstable. The life expectancy of the information stored on these media is influenced by various environmental factors, including temperature, humidity, oxidation, dust and magnetic fields, and they are extremely sensitive to physical damage through careless storage, handling and use. Nevertheless, WORM magnetic tape or cassette, CD-WORM (preferably executable CD-WORM) and DVD-WORM can be used for the storage of

13 The National Archives and Records Service is investigating the applicability of PDF/A as a long-term storage format.
14 http://www.national.archives.gov.uk.
15 http://hul.harvard.edu/gdfr/.
16 http://tom.library.upem.edu/fred/.
17 http://www.dlib.org/dlib/november04/stanescu/stanescu.html.

electronic records that have been identified as archival in nature, on condition that the media are cared for properly.

Governmental bodies need to know how to take care of the media to ensure that information is not lost while it is still possible to read the media with existing technologies. They should also take into account that different media have different requirements regarding their proper care to ensure the preservation of electronic records contained on the media. A few common sense do's and don'ts must be observed when handling and caring for computer files and magnetic media. Additionally, special handling is needed to ensure the long-term preservation of electronic records. The first requirement is that file custodians know specifically which files are permanent, what is to be done with them, and when. This is even more important if computer files appraised as being archival are maintained in decentralised locations.

Hence it is recommended that governmental bodies establish a media watch strategy to continuously monitor whether the storage media on which records are held are in danger of becoming obsolete, and to monitor whether the storage media in their custody are degrading so that timely corrective actions can be taken. The strategy should contain procedures for both media refreshment and migration. Media refreshment entails writing the records to the same media type to ensure continued accessibility. This should be done at regular intervals to ensure the prevention of inaccessibility of data because of the degradation of the storage media. Manufacturers of storage media normally recommend a refreshment period. That recommended period should not be exceeded. Normally data should be copied to new or re-certified tapes at least once every 5-10 years and more frequently for optical storage media to prevent physical loss of data.

5.3.3 Migration

Electronic records need to be migrated to new hardware and software platforms constantly to enable them to remain accessible. Migration of data from one storage medium or software standard to another when changes in technology occur is essential. Migration involves the transfer of electronic records from one hardware or software configuration or generation to subsequent configurations or generations, preserving their integrity and retaining their accessibility. In order to preserve their integrity records must retain their reliability, completeness, authenticity and context. The requirement that records should remain authentic, places a huge responsibility on governmental bodies to ensure that format and media migration are properly managed and documented.

Migration strategies have to be planned for during the design phase of the electronic records system. If added at a later stage it may be

- that the format in which the records were captured does not lend itself to data interchange amongst different types of storage media and software applications;
- that records are lost in the migration process and that there is no proper recording of what was lost;
- that the necessary metadata could not be attached during the migration process because the links between the documents and the metadata were lost or never properly managed in the first place; and
- that the audit trail information was lost thus compromising the integrity of the records.

Ideally, migration should be carried out without the loss of any information. However, loss of some information may be inevitable because of the incompatibilities between the original hardware and software platforms and the new ones and because certain formats of records are better suited for specific migration strategies. The adoption of internationally recognised data and document standards and the use of open standards

will simplify the migration process.

The preservation of electronic records can be very costly in the long run if all records generated electronically have to be migrated continuously. The appraisal of electronic records at an early stage thus becomes more essential. By identifying those records that need to be kept accessible for long periods of time and limiting the migration process to only those records, the cost of migration can be kept at a minimum.

5.4 Long term preservation

There is a wide range of possible digital preservation options currently under investigation. (See in this regard the investigations into migration, emulation, encapsulation, XML etc., which are conducted in the Digital Preservation Test bed,[18] the Interpares project,[19] the Cedars project[20] and the San Diego Supercomputer Centre's PERM Project[21]. The International Standards Organisation is in the process of formulating a standard for the long-term preservation of electronic records.

The National Archives and Records Service is benchmarking its requirements against international best practice. Until these investigations lead to a best proven method of digital preservation, the National Archives and Records Service requires governmental bodies to migrate records through hardware and software changes to ensure that they remain accessible. The National Archives and Records Service, rather than settle for one digital preservation strategy, may in the end determine a range of suitable digital preservation strategies, and may require governmental bodies to implement strategies suitable to specific records and systems. (See Annexure B).

Until such time that a proper strategy has been determined, the National Archives and Records Service recommends that governmental bodies take note of the requirements about accessibility and authenticity and that they put the necessary strategies in place to ensure that records remain accessible.

5.5 Metadata

According to SANS 15489 metadata is "data describing the context, content and structure of records and their management through time"[22] and SANS 23081 elaborates by saying "metadata are structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition of records through time and with and across access domains …. Metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them and the policies that govern them."[23]

In short metadata is descriptive data that gives context to electronic documents. Without the necessary descriptive metadata attached a document cannot be considered to be a record. Descriptive metadata gives information about where a document comes from, who the creator was, when it was created, where it is located, etc. Metadata is also information describing data and their systems; that is the background information that describes how and when and by whom a particular set of data or a record was created, collected or received and how it is formatted. It also includes documentation on migration procedures and actions.

---

18 http://www.digitaleduurzaamheid.nl.
19 http://is.gceis.ucla.edu/us-interpares/index.html.
20 http://www.leeds.ac.uk/cedars/guideto/dpstrategies/dpstrategies.html.
21 http://www.npaci.edu/online/V6.2/perm.html.
22 SANS 15489 - *Information and documentation – Records Management – Part 1: General*, p.3
23 SANS 23081 – *Information and Documentation – Records management processes – Metadata for records- part 1: Principles*, p. 1.

Metadata defines the record at its point of capture and relates the record to its business context. During the existence of records or their aggregates, new layers of metadata will be added, because of new uses in other business or usage contexts. This means that as the metadata continue to accrue over time information relating to the context, the records management processes and the business processes in which the records are used will change".[24]

Metadata ensures the authenticity, reliability, trustworthiness, usability and integrity of records over time for as long as the records are needed. Metadata enables the management and understanding of records. Metadata itself also needs to be managed, to ensure that they are unalterable and thus trustworthy and reliable. Governmental bodies should ensure that only creators/users with the necessary authorisation have access to the metadata database to allow for documented and auditable changes to be done when necessary.

Capturing metadata:

a) protects records as evidence and ensures their accessibility, and usability through time;
b) facilitates the ability to understand the records;
c) supports and ensures the evidential value of records;
d) helps to ensure the authenticity, reliability and integrity of records;
e) supports and manages access, privacy and rights;
f) supports efficient retrieval;
g) supports interoperability strategies by enabling authoritative capture of records created in diverse technical and business environments and their sustainability for as long as required;
h) provides logical links between records and the context of their creation, and maintains them in a structured, reliable and meaningful way;
i) supports the identification of the technological environment in which digital records were created and the management of the technological environment in which they are maintained in order that authentic records can be reproduced as long as they are needed; and
j) supports efficient and successful migration of records from one environment or computer to another or any other preservation strategy.[25]

It is recommended that governmental bodies apply the principles in SANS 23081 *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*[26] when decisions regarding the capturing and management of metadata are taken.

5.5.1 Metadata schema

Metadata is only of value if all the users understand the usefulness of capturing metadata and if they have a common understanding of the precise meaning and use of each metadata element. Users should understand that metadata

- helps a governmental body to meet legal and regulatory requirements by proving authenticity;
- meets records management requirements by providing contextual information and

24 SANS 23081 – *Information and Documentation – Records management processes – Metadata for records- Part 1: Principles*, pp. 1-4.
25 SANS 23081 – *Information and Documentation – Records management processes – Metadata for records- Part 1: Principles*, pp. 2-3.
26 To obtain copies of this standard contact the South African Bureau of Standards Sales' Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria; Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Telefax: (012) 428-6928; E-mail: sales@sabs.co.za.

regulating retention and disposal; and
- enables retrieval of records.

It is therefore necessary to explain the value and use of metadata in a metadata schema. A metadata schema is a semantic and logically structured definition of record keeping metadata.

There are a number of international studies under way to determine which metadata should be kept to ensure long-term accessibility of records and a number of metadata schemas exist. These metadata schemas are not necessarily applicable to the South African environment. Governmental bodies should therefore ensure that they capture the minimum mandatory metadata as described in the National Archives and Records Service's minimum mandatory metadata set[27] and should ensure that they capture as many other metadata elements as are necessary to ensure the continued integrity of the records.

As a result the National Archives and Records Service's minimum mandatory metadata set should be used as the starting point for each governmental body to design and document its own metadata schema.

The International Standards Organisation (ISO) is drafting guidelines on how to design metadata schemas as part of the ISO 23081 set of standards. The new part should become available as an ISO standard by May 2007, after which it would be adopted as a South African national standard.

5.5.2 Types of metadata

According to SANS 23081[28] the following types of metadata are important in the records management environment:

a) Metadata about the record. This includes metadata about
- the identity of the record
  - unique identifier
  - record name
  - record structure
  - data and time of creation
  - relationship with other records
- the identity of the creator
  - the author
  - the organisation
- access and security restrictions

b) Metadata about policy, mandates and business rules. This includes metadata about why (policy and mandate) records were created and how (business rules) they were created.

c) Metadata about business processes. This includes metadata about the functions and activities that created the records and to which the records relate.

d) Metadata about records management processes. This includes metadata about file plans, disposal authorities and retention periods, as well as about the authorised individuals who were given rights to execute the records management process and the date and time such processes were performed.

---

27 *Managing electronic records in governmental bodies: Metadata requirements*, April 2006 http://www.national.archives.gov.za/rms/..

28 SANS 23081: *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*, pp 12-18.

Metadata should be collected at the time of records capture to ensure accessibility and long-term preservation and after records capture where it accrues on an ongoing basis to describe the linkage between the record, the business processes it relates to and the context it was generated in.

5.6 Version control

Version control is crucial in the electronic environment. Electronic records can be located in various places at the same time e.g. in a centralized database, in shared network filing spaces, on local hard drives, in e-mail systems in the inbox, outbox and deleted items, and on a variety of storage media. This makes it more difficult to manage the creation, revision and deletion of records and to identify the authoritative record. If the creation of records is not managed properly someone may accidentally use the wrong version of an electronic record or records which should have been kept may accidentally be destroyed.

If multiple copies of the same record exist, governmental bodies have to establish procedures that would identify the authoritative record, to ensure that it is protected and preserved.

5.7 Authenticity

Authenticity refers to the degree of confidence that a user can have that the record that he has access to, is the original authentic record. Annexure I contains a description of the characteristics of authentic records.

Information contained in records is a means of ensuring accountability and it may need to be produced as evidence in courts of law. Section 15 of the Electronic Communications and Transactions Act provides for legal recognition of electronic evidence, but only in so far as the integrity, authenticity and reliability of the evidence can be proven. To protect the authenticity, reliability, integrity, accuracy, adequacy and completeness of records, and to ensure their legal admissibility, the records must be protected against alterations by users and system administrators. All events that affect the reliability of records must be tracked and that audit trail must be kept as an unalterable record. It is also essential that the system logs a history of all changes that were done on a record including the date of the change and the identification of the person who has taken the action. It should log changes to the records and to the metadata to ensure that the records remain reliable.

Since the Electronic Communications and Transactions Act does not stipulate the specific requirements that would enable one to prove the integrity and reliability of records, the National Archives and Records Service assisted Standards South Africa with the adoption of SANS 15801: *Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability*[29] as a South African national standard. The National Archives and Records Service endorses this standard with a view that it would guide governmental bodies with the implementation of authenticity requirements. This standard describes the recommended processes and documentation that should be in place to ensure that the authenticity of records generated and stored in electronic systems can be proven.

29 To obtain copies of this standard contact the South African Bureau of Standards' Sales Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria; Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Telefax: (012) 428-6928; E-mail: sales@sabs.co.za.

5.7.1 Audit and history trail

In accounting, an audit trail is the sequence of paperwork that validates or invalidates accounting entries. In computing, the term is also used for an electronic or paper log used to track computer activity. For example, a corporate employee may have access to a section of a network in a corporation such as billing but be unauthorized to access all other sections. If that employee attempts to access an unauthorized section by typing in passwords, this improper activity is recorded in the audit trail.

Audit trails are also used to record customer activity in e-commerce. The customer's initial contact is recorded in an audit trail as well as each subsequent action such as payment and delivery of the product or service. The customer's audit trail is then used to respond properly to any inquiries or complaints. A company may also use an audit trail to provide a basis for account reconciliation, to provide a historical report to plan and support budgets, and to provide a record of sales in case of a tax audit.

Audit trails are also used to investigate cyber crimes. In order for investigators to expose a hacker's identity, they can follow the trail the hacker left in cyberspace. Sometimes hackers unknowingly provide audit trails through their Internet Service Providers' activity logs or through chat room logs.

An audit trail provides a historical record of all significant actions that are associated with a record. Audit trail data should as far as possible be system generated, because it is easy to authenticate. According to SANS 15801[30] audit trail information can be split into two categories, namely

- information about the stored record; and
- information about the system that stored the record.

Audit trail files can grow exponentially and it may not be necessary to keep all audit trail data for as long as the records it relates to. It is recommended that governmental bodies determine beforehand which audit trail data is critical to prove authenticity. The choice of actual data to be stored in the audit trail will depend upon the application and the system, as well as on the specific needs of the governmental body. It is recommended that each governmental body should document the types of audit trail data to be captured, as well as the process whereby the audit trail will be captured in the Records Management Policy.

The National Archives and Records Service recommends that as a minimum requirement audit trail information should be captured for

- the file plan
- groups of electronic folders
- individual electronic folders
- electronic volumes
- electronic records
- metadata associated with any of the above.

and that the following events should be captured:

- the type of action which is being carried out, for example
    - re-location of an electronic record to another electronic folder, identifying both source and destination folders
    - re-location of an electronic folder to a different series, identifying both source and destination series

30 SANS 15801*: Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability* p. 35.

  - re-allocation of a disposal schedule to an object, identifying both previous and reallocated schedules
  - placing of a disposal hold on a folder
  - the date and time of a change made to any metadata associated with electronic folders or electronic records
  - changes made to the allocation of access control markings to an electronic folder, electronic record or user
  - export actions carried out on an electronic folder
  - attempts to edit a record
- the user carrying out the action
- the date and time of the event

It must at all times be possible to prove that the system was tamper free at the time the records were created and stored. It is therefore imperative that the system should log all attempts to access it, and that it captures the identity of a user and the time edits were made.

Equally important is that it must be able to be proved that records were not tampered with in a migration process. Details of any move of records from one storage medium to another should be documented in the audit trail. Format migration of records should also be documented in the audit trail.

5.7.1.1 Managing audit trail data as records

Audit trail data is fundamental to prove the authenticity of records hence it must only be able to be accessed by authorised personnel and by auditors. The Records Management Policy should describe who has access and for what purposes. Access procedures to explain how the audit trail can be accessed and how to interpret the data should be formulated and documented in the systems procedure manual.

Audit trail data should be captured immediately after the event that it is documenting and the date and time stamp should be as accurate as possible.

Audit trail data should be stored for at least as long as the information/records it relates to. Should it be possible to prove that the audit trail data has been compromised, the reliability and trustworthiness of the records to which it relates would be questioned. Audit trail data should therefore preferably be stored on WORM media.

5.7.2 Digital certificates and digital signatures

The advent of e-government is changing the way governmental bodies transact with their clients and with each other. Traditionally records of transactions were created in paper and authenticated with a signature in ink. Because of this tradition to prove authenticity with a signature governmental bodies are of the opinion that the best way to protect the authenticity of electronic records is by using digital certificates and digital signatures.

A digital certificate contains a person's name, a serial number, expiration dates and a copy of a person's digital signature as well as the digital signature of the certificate-issuing authority and is used to establish a person's credentials when doing business or other transactions. A digital signature is an electronic signature that can be used to authenticate the identity of a sender of a message or a signatory of a document, and is used to ensure that the content of a document or message is unchanged. The Electronic Communications and Transactions Act, 2002 provides that where a law requires a signature, a governmental body should investigate whether such a signature should be

an advanced electronic signature.

Very few laws require the use of a signature, and no law forces the use of an advanced electronic signature. Authenticity of records can also be proven with due regard of the process by which they were generated. Any technology can, theoretically, authenticate the owner of the specific process. The document generated by that process could be considered legally admissible, if the parties involved could demonstrate the trustworthiness of the process that created and preserved the record. Even if a governmental body implements digital signature or electronic signature technologies, it does not automatically imply that records so signed are legally admissible. The trustworthiness of the processes surrounding the creation, storage, use and management of the signature authentication software would still play a role in the determination of the authenticity and reliability of a record. Governmental bodies should take note of the recommendations in SANS 15801[31] regarding the processes that should be in place to support authenticity.

Governmental bodies should also realize that the use of digital and electronic signature technologies poses practical challenges regarding the long-term preservation of the records and that the body's electronic records management strategy should cover these issues. Governmental bodies should

- create and maintain documentation of the systems used to create records that contain electronic signatures;
- ensure that the records that contain electronic signatures are created and maintained in a secure environment to protect the records from unauthorised deletion and destruction;
- document, implement, maintain and promote the use of standard operating procedures for the creation, use, management and preservation of records that contain electronic signatures;
- manage and preserve records containing electronic signatures for as long as they are required, keeping in mind that the digital signature and the fact of its verification or rejection is part of the contextual information of a record, and should be retained at least for the lifespan of the record it pertains to. Other contextual information that should be retained with the record is documentation that identifies and authenticates particular user(s) as the source of a specific electronically-signed record, as well as documentation that is used to link a verified identity to the public key that is used to verify the signature in a public key infrastructure.

It is advisable that before a decision is taken regarding the use of digital signatures or not, a governmental body

- should document its processes that generate records;
- investigate whether a process would be sufficient prove of authenticity; and
- investigate if there is a specific legal requirement for the use of digital signatures.

They should evaluate the risk associated with electronic transactions. The higher the risk (e.g. rand value, political risk, damage to credibility, etc) the higher the need for a more secure authentication mechanism.

Governmental bodies should also give consideration to the following issues when investigating the use of these technologies:

- technology obsolescence: The speed with which hardware and software becomes outdated makes it difficult to preserve and provide access to older electronic records.

31 SANS 15801 – *Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability*. To obtain copies of this standard contact the South African Bureau of Standards' Sales Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria; Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Telefax: (012) 428-6928; E-mail: sales@sabs.co.za

If governmental bodies use two different technologies to create and sign records, they are adding another layer of technology that should be converted and migrated over time. The physical and logical format of the record and the relationship between the individual data-elements comprising the record should remain intact. This implies that the physical and logical structure of the signature as well as its relationship to the context and content of the record should also remain intact. Since this is very difficult to achieve without migrating the signature technology across hardware and software changes, along with the records it requires careful planning because the migration process may cause signatures to be invalidated. Also consider the fact that the different technologies may "age" at different times. Migration planning should take this into account.

- third party involvement: As creator of records a governmental body may use digital signatures to authenticate records, and may do its utmost to ensure that the process surrounding the creation of authentic records is secure, but what about the certification authority? Is the certification authority managing its records and documentation in a secure manner? Could the authenticity of a governmental body's records and processes be compromised by the service provider?

5.8 Back-up and disaster recovery

Back-up and disaster recovery plans and strategies allow a governmental body to rebuild its electronic information and to continue operations despite significant network failure or other disasters. Back-up systems are not designed for records management purposes and should not be used as a substitute for good records management practices.

However, since those systems are designed for business continuity purposes and they do allow for back-up copies of records to be maintained, it is imperative that each governmental body should have a proper back-up and disaster recovery programme in place.

Governmental bodies should remember that the purpose of a back-up and disaster recovery procedure is to rebuild **authentic and reliable** records. It is therefore vital that back-up data should include the associated metadata and audit trails of all records so that the authenticity of recovered records is not compromised. Back-up strategies should be documented properly and should be monitored and audited to verify their reliability. Back-up data should be stored in a secure environment. The system technical manual should contain sufficient information about the back-up data to ensure that it can be rebuilt and interpreted correctly. A back-up procedures manual should include procedures for checking that file integrity has not been compromised and the frequent testing of back-up media to prevent data degradation.

Back-up and all the file recovery activities as well as problems experienced should be captured in the system's audit trail.

6. MANAGING ELECTRONIC RECORDS RESIDING IN DIFFERENT TYPES OF SYSTEMS

Sound records management principles should be applied to both structured and unstructured records. Structured records are records that are kept in a structured form in columns and rows in a database. Unstructured records are those recorded objects that are not kept in rows and columns in a database like text-based or visually rich records (audio, video, etc). The term unstructured can also apply to records that are not kept in the governmental body's formal record keeping systems, like e-mail, records created on individual PC's hard drives, records stored in shared network drives, etc. Structured systems are normally managed in a more formal way according to database management principles and procedures while unstructured records can very easily be forgotten and not be managed according to sound records management principles, thus compromising their integrity and legal admissibility. Hence, while it is necessary to manage records in structured systems, it is even more necessary to have proper systems to manage records in unstructured systems because they are created in such an undisciplined manner.

6.1 Structured systems

6.1.1 General

Regarding structured systems, the National Archives and Records Service requires that they be managed in such a manner that the authenticity and reliability of the records contained in those systems can be proven beyond any doubt. The information contained in these systems also constitutes public records that form part of the corporate memory governmental bodies and therefore needs to be managed according to the same principles by which all other records are managed. All the information contained in paragraphs 5.2-5.8 above is also applicable to structured systems. Although the proper management of all structured systems is equally important, specific attention should be given to:

6.1.2 Data warehouses

Due to the volatile nature of the information captured in these systems specific attention should be given to their proper management.

Data warehouses are central repositories that capture data from diverse online transaction processing sources for analysis and user queries. Data warehouses are mostly used actively in customer relationship management environments. Data warehouses are dynamic in nature and change frequently.

Governmental bodies can be held accountable for the information users have obtained from such systems. It is therefore imperative that governmental bodies should apply version control to such systems, and that they ensure that records are captured of all queries and the results of those specific queries. The absence of records of what information this system carried as well as how the systems were interrogated and what the results of the interrogations were, could lead to governmental bodies being held accountable for how the information was interpreted and used.

6.1.3 Geographic Information Systems

Geographic Information Systems capture geographical information in the form of scanned and digitized map images. These types of systems enable a user to envision geographic aspects of a body of data and are amongst others used for weather forecasting, sales analysis, population forecasting, land use planning etc. Geographic

Information System databases are dynamic in nature and change frequently.

While some of the information captured on these types of databases may exist in paper format, most of the dynamic assembly of information takes place online, and the record of a specific instance of information assembly only exists in real time while the user is accessing it. Different users can also require different assemblies of information with totally dissimilar results, which makes it extremely difficult to manage these systems or the records generated while interrogating these systems.

Governmental bodies can be held accountable for the information users have obtained from such systems. It therefore is imperative that governmental bodies should apply version control to both types of systems, and that they ensure that records are captured of all queries and the results of those specific queries. The absence of records of what information these systems carried as well as how the systems were interrogated and what the results of the interrogations were, could lead to governmental bodies being held accountable for how the information was interpreted and used.

Geospatial records in these systems are at risk of becoming inaccessible if they are not managed properly. The authenticity and reliability of these records are of utmost importance, since a lot of government decisions that have a direct impact on citizens and the environment they live in, are based on the information in these systems.

The management and preservation of records generated in Geographic Information Systems is very complex and cannot be handled without doing proper planning and putting the necessary policies and procedures in place to ensure that authentic records are generated and preserved in the long term.

The records management principles in paragraphs 5 apply to the management of geospatial data.

According to the Centre for International Earth Science Information Network's (CIESIN) Guide to Managing Geospatial Electronic Records[32] it is possible to manage digital geospatial objects as records within an electronic records management application or even in a digital asset management system. A Data Model for Managing and Preserving Geospatial Electronic Records[33] is available on the CIESIN website.

6.2 Unstructured systems

6.2.1 General

Records residing in unstructured systems should be maintained and retrieved in a manner which ensures that they retain their authenticity and reliability as evidence of transactions. The most sensible way to do this is to **use an electronic records management application**. The purpose of an electronic records management application is to manage all unstructured electronic records within an organisation including scanned images, word documents, e-mail, web-based activities, etc. These systems have an added benefit in that they also manage records in other formats to ensure that all records are managed in an integrated manner.

In the paper-based environment, officials usually create and preserve records in a uniform manner according to a file plan used in the particular governmental body. The records are also physically kept in a uniform manner in a registry that is shared by the governmental body as a whole. Generally in the electronic environment, and especially

32 http://www.ciesin.columbia.edu/ger/GuidetoManagingGERv1tinal.pdf.
33 http://www.ciesin.columbia.edu/ger/DataModelv1-200-50620.pdf.

where personal computers are used, there tends not to be any form of regulation of record creation and preservation. In a networked environment, records can be located in centralised databases, in a shared network filing space and on the hard drive of an individual's PC. The ability to keep information in several places makes it more difficult to control the creation, revision, distribution and deletion of records. The same records can also exist in paper-based form. As a result, it is imperative that governmental bodies should manage their records in a much more disciplined manner than they have in the past. Failure to do so could seriously impede effective access for on-going functional purposes as well as long-term retention and preservation. It makes little sense to organise paper records without doing the same for electronic records.

Flowing from this, the National Archives and Records Service requires that records generated by governmental bodies are

- managed according to the records management principles that are discussed in par 5; and that
- records in all formats and media are managed in an integrated manner.

6.2.2 Managing records in Integrated Document and Records Management Systems

The National Archives and Records Service requires governmental bodies to manage records contained in unstructured systems with an Integrated Document and Records Management System that consists amongst others of electronic document management functionality that supports the immediate operational requirements of an office by helping governmental bodies to exploit their information resources more effectively, and electronic records management functionality that supports the medium to long-term information requirements of an office by capturing electronic records and managing them according to records management principles.

Integrated Document and Records Management Systems should provide as a minimum the following records management functionality:

- managing a functional subject file plan according to which records are filed;
- managing e-mail as records;
- managing websites as records;
- maintaining the relationships between records and files, and between file series and the file plan;
- identifying records that are due for disposal and managing the disposal process;
- associating the contextual and structural data within a document;
- constructing and managing audit trails;
- managing record version control;
- managing the integrity and reliability of records once they have been declared as such; and
- managing records in all formats in an integrated manner.

Annexure A contains details regarding the records management functionality that is required by the National Archives and Records Service.

6.2.3 Managing electronic records without the benefit of an Integrated Document and Records Management System

Although the ideal is that all governmental bodies should implement and maintain Integrated Document and Records Management Systems, not many governmental bodies have the capacity to implement fully automated Integrated Document and Records Management Systems. This does not however mean that they should not manage their electronic records. If these records are created to aid in decision-making and to perform transactions that support the governmental bodies' activities,

governmental bodies are responsible for their proper management.

In the absence of an Integrated Document and Records Management System, heads of governmental bodies should take note of the recommendations in SANS 15801: *Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability* to ensure that they create authoritative records.

Heads of governmental bodies however should be aware that government is committed to e-government as a strategy for better service delivery to the public, and that the public sector is expected to participate fully in the planned e-government gateway. Governmental bodies will have to implement Integrated Document and Records Management Systems to enable them to do so. Only the use of an effective Integrated Document and Records Management System will ensure that authentic and reliable evidence of transactions that take place via the gateway would be able to be captured and maintained.

6.2.3.1 Records maintained on individual PC's and network drives

The National Archives and Records Service requires that governmental bodies should, as a matter of policy, ensure that the records that are created on individual PC's are saved to a shared workspace so that the information they contain can be shared and re-used and so that proper retention and disposal rules can be applied after a written disposal authority has been obtained from the National Archivist. It is possible to set up a shared workspace with a directory structure that corresponds with the paper-based file plan. It is also possible to establish naming conventions for individual documents and to develop retention and disposal procedures for these records that correlate with the disposal procedures of the paper-based file plans.

This method of work will however require:

- properly documented and disseminated records capturing and records management policies, procedures and guidelines;
- that the staff buy in to the idea and are committed to use the shared workspace; and
- that the staff are properly trained in the concept of records capturing and records management in the shared workspace, because their role as users will change from that of records creators to playing a more active role in records management.

The National Archives and Records Service's staff does not yet have expertise to advise client offices on the management of records in shared workspaces. The National Archives of Canada does however have a very good guideline for the management of records in shared workspaces. The publication Managing Shared Directories and Files that is available on the website http://www.archives.ca can be used as a guideline for setting up and managing shared workspaces.

6.2.3.2 Managing records in document management systems

Governmental bodies should not deploy stand-alone document management systems, since these systems

- do not protect authentic archival records for long-term preservation from creation until they are transferred into archival custody. It is crucial to manage and maintain records within the context of a file plan to ensure that they carry evidential weight from the moment they are created until they are disposed of and to ensure the long-term preservation of properly contextualized authentic and reliable archival records. Just from a practical perspective, should the users accidentally forget to declare the documents as official records, the documents would still be properly contextualized and the chance that they could be inadvertently deleted is diminished, since proper

disposal rules are built around the file plan.
- do not allow the implementation of systematic disposal programmes from creation until transfer into archival custody. Exactly for this reason there is an emerging trend world-wide to merge document management systems and records management systems to ensure that archival and retention requirements are met from the moment the records are created.

Should it be necessary to procure a document management system for business critical reasons or to do a technology roll-out in a phased approach, governmental bodies should ensure up front that the document management system that they procure
- would be able to integrate with a records management application when the resources become available to upgrade the technology; or
- would be able to be developed to include the necessary records management functionality when resources become available to upgrade the technology; and
- that they procure at least one electronic records management administrator licence to enable the records management functions to be automated.

If the document management system has the functionality to create an electronic file plan, the governmental body should ensure that the file plan structure correlates with the paper-based file plan. Should the document management system not have such functionality, all records created should be classified/indexed against an approved file plan that corresponds with the paper-based file plan. This is necessary to ensure that the records are not divorced from the other record keeping systems, and that the same disposal rules apply.

Governmental bodies should ensure that disposal authority is obtained from the National Archives and Records Service and that the retention and disposal rules are applied to records created and stored in such systems. Governmental bodies should also ensure that the records are protected against unauthorised alterations and deletion, so as to ensure their legal admissibility and/or compliance with the National Archives and Records Service Act, 1996 and the Promotion of Access to Information Act, 2000.

6.2.3.3 Managing records in imaging and scanning systems

Governmental bodies should not deploy standalone imaging and scanning systems without taking all the records management consequences into account. Even though the Electronic Communications and Transactions Act provides for electronic images to carry evidential weight, it only does so if it can be demonstrated that the records created in such systems were created in a trustworthy manner and there was no room to tamper with the records in the scanning process. The recommendations in SANS 15801[34] should be taken into account.

If the imaging and scanning system has the functionality to create a file plan structure, that structure should correspond with the paper-based file plan. Should the system not be able to create a file plan structure, the records should be indexed against the paper-based file plan to ensure that the same disposal rules apply.

When procuring an imaging and scanning system governmental bodies should ensure up front that the system that they procure
- would be able to integrate with a records management application when the resources become available to upgrade the technology; or
- would be able to be developed to include the necessary records management functionality when resources become available to upgrade the technology.

34 SANS 23081 – *Information and Documentation – Records management processes – Metadata for records- Part 1: Principles*, pp. 2-3.

6.2.3.4 Managing records in digital asset management systems

Some governmental bodies implement digital asset management systems to manage visually-rich media types like images, logos and line art, audio, video, animation, CAD drawings, etc., because they provide a mechanism for content retrieval functionality that most document and records management solutions do not have.

These systems are however deployed in such a manner that they isolate these records from the broader record keeping practices and systems in a client office.

Although the National Archives and Records Service does not have any objection to the use of such systems it is a concern that the management of records is not sufficiently addressed by these systems especially if they store the only instance of a record that may ever exist.

Digital asset management systems should support:
- the management of record as required by the National Archives and Records Service as indicated in par 5.;
- the capturing of metadata as required in the National Archives and Records Service's minimum mandatory metadata set[35];
- the capturing of a sufficiently detailed audit trail to ensure authenticity of records and to keep the audit trail as a record for as long as the records are required;
- integration into the Integrated Records and Document Management System or built in records management functionality to ensure that authentic archival electronic records are created and preserved.

6.2.3.5 Managing records with file and document tracking systems

Many governmental bodies wish to improve service delivery and record keeping practices but only have the capacity to implement file and document tracking systems to automate registry functions.

Tracking systems are used to bar-code paper-based records, to store them in a central location and to track their movement and usage.

The National Archives and Records Service does not have any objections to the use of such systems and in fact considers this a good place to start making the staff aware of the benefits of using better records management controls. Governmental bodies should keep in mind that such systems should be deployed within the records management framework set by the National Archives and Records Service Act, 1996. Having a file tracking system in place does not absolve the governmental body from its responsibility to implement and maintain an approved file plan and to manage its paper-based records according to the principles contained in the *Records Management Policy Manual*.[36]

When procuring file tracking systems, governmental bodies should ensure up front that the system that they procure
- would be able to integrate with a records management application when the resources become available to upgrade the technology; or
- would be able to be developed to include the necessary records management

35 NARS *Managing electronic records in governmental bodies: Metadata requirements,* April 2006 http://www.national.archives.gov.za/rms/.

36 The *Records Management Policy Manual* is available on the National Archives and Records Service website http://www.national.archives.gov.za. Alternatively hardcopies can be obtained from the Records Management Division Tel. (012) 323 5300, Fax 086 682 5055, e-mail: rm@dac.gov.za.

functionality when resources become available to upgrade the technology.

Governmental bodies should also be aware that
- the tracking records generated by these systems may be considered to be an audit trail for the paper-based records and should thus be managed in such a way that they cannot be tampered with; and that
- the file tracking systems should also allow for the capturing of metadata for paper-based records according to the National Archives and Records Service's requirements as set out in the minimum mandatory metadata set.[37]

6.2.3.6 Managing records with digital filing systems

Many governmental bodies wish to improve service delivery and record keeping practices but only have the capacity to implement digital filing systems.

Digital filing systems are used to scan paper-based records with the intention to route them to speed up service delivery. The paper-based records are bar-coded and stored in a central location. They are considered the legally admissible records. These systems can also capture born-digital records from other applications like MS Word and keep them in a secure environment for easy access. However, maintaining the scanned images and electronic records as legally admissible records **is not** the objective of these systems.

The National Archives and Records Service does not have any objections to the use of such systems and in fact considers this a good place to start making the staff aware of the benefits of using better records management controls. Governmental bodies should keep in mind that such systems should be deployed within the records management framework set by the National Archives and Records Service Act, 1996. Having a digital filing systems in place does not absolve the governmental body from its responsibility to implement and maintain an approved file plan and to manage its records according to the principles contained in the *Records Management Policy Manual*.[38]

When procuring digital filing systems, governmental bodies should ensure up front that the system that they procure
- would be able to integrate with a records management application when the resources become available to upgrade the technology; or
- would be able to be developed to include the necessary records management functionality when resources become available to upgrade the technology.

Governmental bodies should also be aware that
- even though not the intention, the scanned images created in these systems as well as the electronic records captured into these systems may in future be imported into fully fledged Integrated Document and Records Management Systems. Their legal admissibility may thus become and issue in the future. The principles in contained in par 5 and the guidelines in par 6.2.2.3 above apply.
- the tracking records generated by these systems may be considered to be an audit trail for the paper-based records and should thus be managed in such a way that they cannot be tampered with; and that
- the digital filing systems should also allow for the capturing of metadata for paper-based and electronic records according to the National Archives and Records

37 NARS *Managing electronic records in governmental bodies: Metadata requirements,* April 2006 http://www.national.archives.gov.za/rms/.

38 The *Records Management Policy Manual* is available on the National Archives and Records Service website http://www.national.archives.gov.za. Alternatively hardcopies can be obtained from the Records Management Division Tel. (012) 323 5300, Fax 086 682 5055, e-mail: rm@dac.gov.za.

Service's requirements as set out in the minimum mandatory metadata set.[39]

6.2.4 Managing records contained in e-mail systems

6.2.4.1 General

The use of e-mail as a means of communication is increasing on a daily basis. E-mail is no longer used as an unofficial communication medium e.g. to replace telephone calls, but is increasingly used to conduct business transactions and to convey information of an official nature. However, users are unaware that e-mails should be managed according to the same sound record keeping practices as any other records created or received in the pursuance of official business. E-mail may be subject to promotion of access to information requests, but users may have an inappropriate expectation of privacy and informality not realizing that the e-mails are actually public records. Messages sent or received in the performance of the functions of an office (as well as their attached metadata) are public records that must be retained for as long as they are needed for official purposes.

Examples of messages sent by e-mail that are public records include:
- policies and directives
- correspondence or memoranda related to official business
- work schedules and assignments
- agendas and minutes of meetings
- drafts of documents that are circulated for comment or approval
- any document that initiates, authorizes, or completes an official business transaction
- final reports or recommendations.

Some examples of messages that are not public records are:
- personal messages and announcements not related to official business
- copies or extracts of documents distributed for convenience of reference
- phone message slips
- announcements of social events, such as retirement parties or holiday celebrations
- spam
- unsolicited e-mail

E-mails are deleted at the discretion of the user or system administrators who are purging systems to save storage space. With no control over the systematic disposal of e-mails governmental bodies run the risk of losing records that are critical to continued service delivery and that should be kept as part of the corporate memory of the body.

E-mails are not kept in open repositories or shared domains, which makes access to the corporate knowledge-base and the sharing of information very difficult. This tendency also contributes to the abundance of e-mails floating around, because the only way to share information contained in e-mails is to forward them to other people. Furthermore, if e-mails, like other public records, are not classified and maintained in corporate record keeping systems, it will result in diminished evidential weight in legal proceedings and it will make it very difficult to retrieve them in context.

In terms of the National Archives and Records Service Act, the definition of a record is "recorded information regardless of form or medium". E-mail is considered a type (form) of record as well as the channel (medium) through which the communication is transmitted. E-mail messages should always be treated as potential official records. If

39 NARS *Managing electronic records in governmental bodies: Metadata requirements,* April 2006 http://www.national.archives.gov.za/rms/.

not valuable information will be lost. E-mail records should be managed according to the basic principles that apply to records in any medium.

6.2.4.2 Approaches to managing e-mail

There are a number of approaches to managing e-mail records. Whichever method is chosen, all users should be aware of the policies, procedures, and tools for managing e-mail messages and they should be capable of applying them consistently to all records.

When managing electronic messages, the following specific requirements should be kept in mind:

- The e-mail message must include transmission data as well as the message itself and all the attachments to the message. The transmission data identifies the sender and the recipient(s) and the date and time the message was sent and/or received. This data provides essential context for the message. This is equivalent to correspondence on paper, where the record includes information identifying the sender and recipient and the date of the letter, not just the message. Any attachments containing information necessary for decision-making or to understand the intention or the context of a message should also be kept as part of the record.
- When e-mail is sent to a distribution list, information identifying all parties on the list must be retained for as long as the message is retained.
- If the e-mail system uses codes, aliases, nicknames, or anything other than the real name of senders or recipients, their real identities need to be retained as part of the record.
- If a message is sent to a distribution list and the recipients reply to the message, different records are generated that should be filed as separate records. The system normally uses the subject line to name messages when they are filed into the file plan. To prevent filing of messages with the same name into the electronic repository the system should provide the facility to add an additional file name to the e-mails to enable them to be distinguished from each other. Each message should be identified as a unique entity.

The following are possible approaches to managing e-mail:

6.2.4.2.1 Managing e-mail within an Integrated Document and Records Management System

The ideal is that records in all formats should be managed with an Integrated Document and Records Management System (IDRMS) that amongst others

- manages a corporate file plan according to which records including e-mail are filed;
- Protects the authenticity of e-mail in the same way it protects the authenticity of all other records in the system; and
- That manages the disposal of e-mail in the same way it manages the disposal of all other records in the system.

However, the National Archives and Records Service realizes that not all governmental bodies can afford to procure an Integrated Document and Records Management System and that they still have a need to manage their e-mail properly.

The National Archives and Records Service also allows the following approaches to managing e-mail, provided that they are implemented within the broader framework of the National Archives and Records Service Act.

6.2.4.2.2 Managing e-mail within the e-mail system

There are three types of folders within an e-mail system namely:
- personal folders of which access is limited to the specific user;
- public folders that are equivalent to a corporate work space; and
- shared folders that can be set up for a specific unit or project team, where messages within a specific division or unit can be stored and shared.

The aim of managing messages in the e-mail system is to encourage users to store messages in one of the three folder areas. The purpose would be to take corporate control of the e-mail records by allowing official records to be moved from individual in boxes to a corporate environment. This type of strategy is however, very labour intensive and very dependent on the co-operation of the users in regularly moving relevant messages from the in boxes box to shared or public folders.

Personal e-messages can be moved from individual e-mail boxes to personal folders that limit access to the specific individual users. However, to prevent the e-mail system from being overflowed with e-mail messages, users should be limited to the amount of "personal" e-mail space they can occupy.

Official messages can be stored in the shared folders and the public folders by requiring users to drag and drop them there. A directory structure for both the public folder and the shared folders can be set up according to the structure of the paper-based file plan. This would allow for the setting of appropriate access restrictions on folder level and the retention rules that apply to the paper-based file plan will also apply to the e-mail. It is also possible to set the system up to store read only copies of the e-mail. This would only work properly if the records manager has corporate control over the public and shared folders to
- monitor the allocation of appropriate metadata and proper file names; and
- ensure that disposal actions are carried out on a regular basis.

Governmental bodies should remember that moving records to public and shared folders does not remove them from the e-mail system. The problem regarding the volume of e-mail records would thus not be solved if disposal actions are not carried out regularly.

Even though this is not the ideal solution in the long term, this approach will provide valuable groundwork for the move to an electronic system by creating awareness about the importance of e-mail records.

6.2.4.2.3 Managing e-mail on a shared drive

Governmental bodies could set up a file plan directory structure according to the paper-based file plan for the management of e-mails on a shared network drive. However, governmental bodies should take note of the fact that placing the e-mails in a shared file plan structure would not necessarily ensure that they are non-editable except if the system is configured to store read only versions of the e-mails. The e-mails would also be accessible by everyone who has access to the folders except if the system is configured to limit access according to user role. The same disposal rules that would apply to the subject folders in a paper-based file plan would apply to the subject folders in the electronic directory structure. To ensure that the records have evidential weight in a court of law, the authenticity and reliability of the e-mails should be guaranteed by configuring the systems to capture a proper audit trail.

This method of work is not the most perfect way to manage e-mails, but it is better than not managing them at all. Governmental bodies should note that this method of work

can be labour intensive and that it will require:

- properly documented and disseminated records capturing and records management policies, procedures and guidelines;
- that the staff buy in to the idea and are committed to use the shared workspace;
- that the staff are properly trained in the concept of records capturing and records management in the shared workspace, because their role as users will change from that of records creators to playing a more active role in records management; and
- that the records manager is committed to managing the records in these directory structures according to the documented policies and procedures.

6.2.4.2.4 Managing e-mail within an e-mail archiving system

E-mail archiving is a process whereby the system, based on predefined rules, automatically extracts e-mail messages, attachments and information about the e-mail as it is received or sent and then indexes and stores the messages so that they are secure, tamperproof and retrievable, and so that they can be disposed of based on established policies to comply with legal and regulatory requirements.

However, the implementation of these systems is done without the necessary records management principles being applied to the management of e-mails. E-mail archiving solutions are deployed to facilitate compliance with legal and regulatory requirements and to enforce e-mail retention and privacy policies. However the use of these solutions must also fit with the required records management practices in terms of the National Archives and Records Service Act.

An e-mail archiving solution should not become an e-mail dumping site; because it would still take time to search for a particular e-mail. E-mail inside an archiving solution should still be managed properly to ensure that messages are contextualized and retained for as long as they are needed.

The National Archives and Records Service does not have any objection to the use of e-mail archiving systems as long as they are deployed within the framework of the records management principles set by the National Archives and Records Service Act. As a minimum requirement e-mail archiving systems should support

- the management of records as required by National Archives and Records Service as discussed in par 5.
- filing of e-mails against the file plan to prevent e-mails from being isolated from record keeping systems
- disposal in terms of disposal authorities issued by the National Archives and Records Service
- the capturing of metadata as required in the National Archives and Records Service's minimum mandatory metadata set[40]
- the capturing of a sufficiently detailed audit trail to ensure authenticity of e-mails and keeping the audit trails for as long as the records are required
- basic minimum records management functionality or integration into the Integrated Document and Records Management System
- managing attachments as records in their own right by capturing proper metadata and audit trails
- integration into the technology watch and migration strategy.

40 NARS *Managing electronic records in governmental bodies: Metadata requirements*, April 2006. http://www.national.archives.gov.za/rms/.

6.2.4.2.5 Print-to paper

If a governmental body decides to print e-mails to paper it should be realised that this option is not necessarily the best, since the hard copies would carry less evidential weight. This is especially true if a governmental body does not have a properly enforced policy that obliges all staff to file hard copies of their e-mails as part of the normal administrative practice of the office. Born digital records are best kept in their digital format in a secure and non-editable environment with a secure and non-editable audit and history trail to ensure that they carry evidential weight. The following should be kept in mind to prevent unnecessary duplication of e-mail messages on the paper-based files:

- if an e-mail message is sent and no reply is expected, print and file the message;
- if an e-mail is received and no reply is necessary, print and file the message;
- if an e-mail message is sent and a reply is expected, keep the e-mail until the matter is finalised. As soon as the matter is finalised, print all related messages and file them. A good option would be to require the recipient always to attach the original message text to the replies. In this way all messages sent and received on the same matter are kept together;
- if an e-mail is received and a reply is expected, keep the e-mail until the matter is finalised. As soon as the matter is finalised print and file the message. A good option would be to reply to the message and to attach the original message text to the replies. In this way all messages sent and received on the same matter are kept together;
- if a message is sent to a distribution list and the recipients reply to the message, different records are generated, which should each be kept until the individual matters are finalised and then be printed and filed separately.

6.2.5 Managing Websites and web-based activities as records

6.2.5.1 General

A website is a collection of information, records, or databases that is provided to a user community through a web interface. Web-based activities refer to the interactive communication of information and/or the conduct of business activities through web technologies.

Websites comes in many different forms, each of which poses a different challenge when it comes to the management of the site as a record. Websites can be:

- **Static**
  This is the most basic form of website. It consists of a collection of static documents sitting in folders on a database. The documents are hyperlinked, and the only activity on the site is the movement between the hyperlinked documents. These sites are relatively easy to preserve. Snapshots of the sites can be taken or the entire site can be written to a CD. Version control can be applied when the site changes.

- **Dynamic**
  On a dynamic website users can make requests, through the use of an e-form, for data contained in a database on the server that will be assembled on the fly according to what is requested. Dynamic websites are linked to the Internet and can query all available resources to answer a specific query. These types of websites are more difficult to manage as records.

- **Interactive**
  These websites are dynamic sites which are also used as a user interface to provide web-enabled services to the public. These sites are the most difficult to manage as

records.

Governmental bodies increasingly use web technology to communicate with internal and external stakeholders. Websites are often the main entry point to other electronic systems in operation. Websites are not static anymore, but contain large dynamic collections of information and content. While some of the records published to websites often exist in paper format in proper record keeping systems, it does happen that records are created in the online environment, which are not captured in record keeping systems. Governmental bodies are responsible for the creation of authentic, reliable and accurate records of all web-based activities to enable them to be accountable to the public to which the services are provided.

Governmental bodies can be held accountable for the information they publish on their websites even long after the website has been updated/changed, as well as for the transactions conducted via the website. At a given time websites may contain information on:

- the structure and organisation of the body concerned;
- the legislation it administers or under which it operates;
- the functions for which it is responsible;
- its current policies, guidelines, advice and publications;
- its current products and services;
- instructions for the access and use of those products and services and for the interpretation of the information posted to the websites;
- the functionality to transact with the governmental body to obtain products and services.

Websites document both the structures and public face of governmental bodies. It is necessary for governmental bodies to document their websites accurately over time so that they can reliably establish the content their websites carried at any particular point of time. If websites are not managed appropriately governmental bodies could be required to:

- carry the cost of legal action when being sued for not being able to provide accurate information on the content of a website at a specific time;
- operational cost when vital information is lost;
- administration costs when information has to be searched for and replicated; and
- historical costs when the archival records containing the corporate memory are lost.

It is even more imperative that records should be created of all transactions conducted using this functionality. In the absence of a record of transactions, there is no evidence of these transactions ever having occurred. This can lead to a transaction being deemed by a court of law not to have taken place.

Records management principles should be applied to the management of websites to:

- ensure that the requirement to capture and manage records of business transactions is met. Governmental bodies publish records to websites and remove them at will without realizing that those records should be kept as evidence and should thus meet all the requirements for creating and managing authentic records;
- ensure that web content and web transactions are captured as authentic and reliable records that carry evidential weight;
- ensure that authentic records so created are sustained for as long as they are needed; and
- ensure that web-based records and activities that are part of the national archival heritage are protected and preserved.

6.2.5.2 Authenticity of web records

As in the case of all other records governmental bodies should ensure that trustworthy records of web-based activities are created, by maintaining the content, context and structure of the site. Content, context and structure are defined as follows:

> Content: The actual HTML pages as well as the linked additional content files referenced therein or content created by end users interacting with the website. Maintenance of these web content records is necessary to support all of the characteristics of trustworthiness: reliability, authenticity, integrity, and usability.
>
> Context: Administrative and technical records necessary for or produced during the management of a website. Maintenance of these records provides a context for web operations, which attests to the reliability, authenticity, and integrity of an body's website.
>
> Structure: For those websites (or portions) that have been appraised as permanent and for high risk temporary sites, a site map indicating the arrangement of a website's content pages and software configuration files of content management systems. Maintenance of this record provides a structure for content records and thereby enables the integrity and usability of both current and preserved versions of an agency website.[41]

6.2.5.3 Approaches to managing web records

6.2.5.3.1 Managing web records within an Integrated Document and Records Management System

Due to the nature of websites it is recommended that the website should link to the repository of the Integrated Document and Records Management System and that it should extract its information from the repository. This would prevent multiple copies of the same document existing in various places. The appropriate metadata for each individual record could then be captured before it is published to the website. Metadata regarding the posting of the record to the website (e.g. date of posting, format it was published in, authorizations for postings and removal from website) could then be captured and linked to the record. Besides the metadata regarding every record that is posted to the website appropriate metadata about the website itself could then also be captured at the time that the website is extracted to the repository.

It should be possible to extract a precise copy of the site to the electronic repository to create a record of the public face of the website. This should be done the first time the website becomes active and thereafter each time a change/update is done. If the website changes on a daily basis a governmental body should decide how frequently version control should be applied, taking into account its accountability requirements.

The links in the extracted copy of the website should remain active. If a record that was linked to the specific website was disposed of according to a disposal authority, the link to the metadata of that document should be maintained to indicate what happened to the specific document.

A historical log should be kept all actions taken on the website after it has been extracted to the electronic repository.

Records of web-based activities should also be extracted to the Integrated Document

41 NARA, *Guidance on Managing Web Records*, pp. 9-10.

and Records Management System. Single transactions between the website and the user should be captured at the time of the transaction. The following should be captured:

- Date and time of the transaction;
- The IP or domain address of the user;
- The user profile;
- The query or other action performed;
- The resources provided to the user with the relevant metadata attached;
- If an e-form was used, information regarding the specific version of the e-form that was used for that specific transaction.

The National Archives and Records Service does not yet have the expertise to advise client offices on the technology behind the proper management of web-based record keeping. The National Archives of Australia does however have a comprehensive guideline for archiving web resources. The publication Archiving Web Resources: Guidelines for keeping records of web-based activity in the Commonwealth Government can be accessed on http://www.naa.gov.au. This will give governmental bodies an idea how to go about managing websites as records.

The principles in paragraph 5 are also applicable to websites.

6.2.5.3.2 Web content management systems

Many governmental bodies rely on web content management systems to manage their websites. Web content management systems are systems used to manage the content of a website and consist of a set of integrated modules that support creation, modification, workflow, storage, publishing, removal and management of web content. Most of these systems include publishing, format management, revision control, indexing search and retrieval functionality. These systems seldom have sufficient records management functionality. The National Archives and Records Service therefore requires that web content management systems should be implemented within the broader records management framework as set out in par 5 of these guidelines.

It is essential that the records manager plays an active role in the management of web records to ensure that the National Archives and Records Service's records management requirements are met and that archival web records are identified and safeguarded early on in their life cycle.

As a minimum requirement web content management systems should support:

- the management of record as required by the National Archives and Records Service as discussed in par 5;
- the capturing of metadata as required in the National Archives and Records Service's document Managing electronic records in governmental bodies: Metadata requirements[42];
- the capturing of a sufficiently detailed audit trail to ensure authenticity of records;
- keeping the audit trail especially if the web content management system generated the only instance of a record for as long as the records are required;
- integration into the Integrated Records and Document Management System or built-in records management functionality to ensure that authentic archival electronic records are created and preserved;
- the rendering of all content elements/records especially archival content/records that

42 NARS *Managing electronic records in governmental bodies: Metadata requirements*, April 2006. http://www.national.archives.gov.za/rms/.

are created, managed or delivered through the web content management system into PDF format (for document type content) or TIFF (for graphic type content).

7. AUTOMATED CORRESPONDENCE SYSTEMS IMPLEMENTED WITHOUT TAKING RECORDS MANAGEMENT REQUIREMENTS INTO CONSIDERATION

Many governmental bodies have implemented electronic systems to automate correspondence processes, without taking the National Archives and Records Service's requirements for the management of electronic records into account.

The National Archives and Records Service is aware that the investment made in these systems is of such a nature that it cannot be required of governmental bodies to stop using them and to implement new systems. This does however not mean that the National Archives and Records Service's records management requirements should not be addressed.

Heads of governmental bodies are still obliged to ensure that electronic records generated in these systems are managed according to sound records management principles.

Records created and stored in such environments carry the inherent risk that they would not be accepted as evidence in courts of law, because it is impossible to prove their authenticity and reliability. Governmental bodies should keep in mind that the Electronic Communications and Transactions Act provides for legal recognition of electronic records only in so far as the integrity, authenticity and reliability of the evidence can be proven.

Hence the National Archives and Records Service urges governmental bodies to give consideration to-

a) integrating existing non-compliant systems with an US DoD or UK National Archives certified out-of-the-box electronic records management application if there is systems available that would provide seamless integration with the existing systems; or
b) developing the necessary records management functionality into the existing non-compliant system according to the functionality specified in the National Archives and Records Service's Draft Functional Specification for Integrated Document and Records Management Solutions[43]. When using the draft functional specification, governmental bodies should however ensure that the records management requirements of the National Archives and Records Service are integrated with their own business requirements. The draft functional specification contains generic requirements and should not be considered sufficient to replace the need for a proper investigation into the unique business requirements of an office. Should this method be chosen governmental bodies should keep in mind that the customized functionality would most probably have to be rebuilt every time an upgrade to a new release of the original software is done.

Whichever method is chosen the National Archives and Records Service would have to certify that the necessary records management functionality is available to enable a governmental body to comply with the National Archives and Records Service's electronic records management requirements.

43 The draft functional specification is currently under revision. Copies of the original draft can be obtained from Louisa Venter of the National Archives and Records Service, Tel.: 012 323 5300; e-mail: Louisa.venter@dac.gov.za.

8. THE RESPONSIBILITIES OF GOVERNMENTAL BODIES REGARDING THE MANAGEMENT OF ELECTRONIC RECORDS

The heads of governmental bodies have to shape the electronic records management culture within their organisations. They can play a role in defining its explicit rules and implicit etiquette, and they should be perceived as promoters of the sound management of electronic records. This goal can be reached by ensuring that the institution's electronic records management strategy is understood throughout the organisation. Taking into account the records management principles contained in par 5 governmental bodies should:

8.1 Notify the National Archives and Records Service of the intention to introduce electronic records systems

By contacting the National Archives and Records Service beforehand, governmental bodies can ensure that they work together with the National Archives and Records Service to make certain that electronic records are created, maintained and preserved according to the National Archives and Records Service's requirements. This would also ensure that governmental bodies build records management requirements into their business processes so that they become part of the normal operation of the body. The requirements are amongst others that:

- the subject classification requirements should be addressed before the records are created to ensure their proper contextualisation. See par 5.1.

- the disposal requirements for electronic records should be built into the systems during the planning phase of the systems to prevent records from being kept for unnecessarily long periods of time. This is especially necessary in the electronic environment where a system's performance can be adversely affected when data/records that are no longer needed for functional and legal purposes are retained unnecessarily. The implementation of electronic records systems usually leads to the destruction of paper-based records, which needs to be done in terms of a proper disposal authority issued by the National Archivist. Most offices are under the impression that they can destroy the paper-based records automatically if an electronic copy thereof is made especially since the Electronic Communications and Transactions Act, 2002 allows for an electronic version of a record to be considered the legally admissible copy. This is not a correct assumption. The National Archivist can still determine that the paper-based records are the archival records and that they should be retained permanently. See par 5.2.

- the requirements regarding the medium for the long-term storage and the format for long-term accessibility of archival records should be built into electronic systems in the planning phase of such systems to prevent records from becoming inaccessible. See par 5.3 and 5.4.

- descriptive and background information (metadata) and sufficient audit trail data needed to ensure that records are authentic and reliable, should be built into the system to ensure that understandable and reliable records are created. See par 5.5 and 5.7.1.

- the management of e-mail and web records should be addressed to ensure that authentic and reliable records are created. See par 6.3 and 6.4.

8.2 Do a proper preliminary study

The implementation of technology should never happen in isolation from the broader records management environment, since such implementations have an enormous impact on all records management practices of an office. The deployment of technology solutions changes the way records are created, managed and stored. When IT implementations fail, it has serious implications for the record keeping and records management practices of governmental bodies. This is a great concern for the National Archives and Records Service that has to protect the memory of the nation for centuries to come. As a result, the National Archives and Records Service requires that governmental bodies plan their technology implementations properly and access the impact that it would have on the record keeping and records management practices before they embark on such implementations.

The National Archives and Records Service is convinced that a properly planned approach to the roll-out of technology solutions would contribute to the success of the projects and would contribute to an overall records management improvement programme that would integrate records management into the normal business practices of a body.

The National Archives and Records Service recommends that the following should be investigated before a governmental body procures and attempts to implement technology solutions:

8.2.1. The environment within which the governmental body exists

The role of the governmental body, its structure and the administrative, legal, business, regulatory and socio-political environments in which it operates are major factors affecting its record keeping practices and service delivery obligations.

Doing an institutional analysis will provide:

- an understanding of the organisation and the administrative, legal, business and social contexts in which it operates;
- an understanding of the organisation's record keeping strengths and weaknesses;
- an understanding of the records that need to be sustained over the long term;
- a sound basis for defining the scope of the organisation's record keeping project and presenting a business case for managerial support; and
- information about the requirements of the body's stakeholders.

The information gathered during an institutional analysis is an essential basis for the compilation of a functional subject file plan and the preparation of a records disposal authority as well as for deciding what metadata and audit trail data should be captured to ensure legal and regulatory compliance.

8.2.2 The business of the governmental body

In 1998 the Public Service Review Commission (PSRC) remarked in their report that "many of the processes and procedures through which services are provided are still based to a large extent on [the] rule-based bureaucratic norms ….. and serve the bureaucratic needs of the public service rather than the needs of consumers and clients"[44]. The PSRC in chapter 6 of their report recommended that a business process

44 *Developing a Culture of Good Governance. Report of the Presidential Review Commission on the Reform and Transformation of the Public Service in South Africa*, 27 February 1998, Chapter 3 [http://www.gov.za/reports/prc98/chp2.htm].

re-engineering should be done to ensure an alignment between the business objectives and the actual service delivery of governmental bodies.[45]

Understanding the business of a governmental body serves a dual purpose:

- Records are created within the business context of a governmental body, and are kept as evidence of business activity, i.e. they have an evidential purpose. Every decision a governmental body makes, and everything a governmental body does, involves the use of information. The manner in which a governmental body creates, classifies, stores and manages its records contributes to the success or failure of the governmental body. It is necessary to understand the business processes, why and when records are generated and how they should be managed to ensure that they do have evidential weight. This is why an analysis of the business processes is necessary to enable the drafting of a file plan, and to gain an understanding of why records are created and why and for how long they should be retained.
- When a governmental body envisages the automation of its service delivery, business process mapping/modelling is required **before** processes can be designed in the workflow. The processes should also be optimised and approved by the governmental body to avoid the automation of ineffective processes that would in turn prevent the creation of authoritative records. Re-engineering the processes would contribute to the improvement of service delivery.

8.2.3 The records requirements of the governmental body

Records are the reflection of an organization's activities and the environment in which it operates. It is essential for governmental bodies to know which records they should create to enable them to conduct their business in an orderly manner, to comply to legal requirements and to mitigate risk. It is also essential for them to know what records a body hold to enable them to:

- respond to requests for information;
- prevent access to information that should not be made available due to protection of privacy legislation.

The analysis should also include an investigation into the current record keeping practices. A records audit will

a) identify each record type, records series and system,
b) help to identify any problems with the current record keeping practices;
c) assist with the design of a file plan; and to
d) assist with the production of a retention schedule;
e) help to determine what is required to install and maintain the records management programme (space, equipment, personnel, etc).

In order to meet records management objectives and users' needs, having regard to the likely availability of resources, a records audit needs to include the following:

i) what records are held and the activities to which they relate;
ii) an inventory of record containers (cabinets, shelves, etc);
iii) records documentation (file lists, indexes, etc);
iv) amount of records;
v) where copies of records exist;
vi) date range of the records;
vii) frequency of consultation of the records;
viii) tracking systems for the records;

---

45 *Developing a Culture of Good Governance. Report of the Presidential Review Commission on the Reform and Transformation of the Public Service in South Africa,* 27 February 1998, Chapter 6 [http://www.gov.za/reports/prc98/chp2.htm].

ix) current records management system and competence levels of records management staff;
x) record keeping costs;
xi) identification of records that should be sustained for the long term.

This analysis should also assist with determining the most appropriate policies, procedures, standards and tools that are necessary to support sound records management practices.

8.2.4 The impact on the human resources

The implementation of technology and service delivery improvement is very much a cultural issue in a governmental body. There should be sufficient understanding of how the implementation of an electronic system would impact on the training, skills level and work processes and procedures of the staff. Any electronic system can only be as good as the people that are using the system.

An investigation should be done to determine:
- The influence of ineffective record keeping on the staff and their service delivery;
- The skills level of the staff;
- How the staff would deal with a new record keeping system;
- How the staff would cope with technology when it is introduced;
- How the staff would deal with electronic service delivery;
- The training and change management activities that are necessary to create a record keeping culture.

The job functions of existing staff may be impacted by records management projects and will definitely be impacted by the roll out of technology. Governmental bodies need to determine if it would be necessary to re-skill and redeploy staff.

ARP 076: *Electronic Imaging – Human and organisational issues for successful electronic image management implementations* contains very good guidelines with regards to the issues that should be investigated.[46] It also contains change management guidelines.

8.2.5 The IT infrastructure

The roll-out of the technology is very much dependent on the IT infrastructure of the body. The deployment of an Integrated Document and Records Management System requires specific infrastructure specifications. An analysis will indicate:
a) Inadequacies of workstations, which may require upgrading before deployment;
b) Limitations of server specifications;
c) Network limitations which may influence response times;
d) Components that must or can be reused in the system;
e) Technology direction that was decided by the governmental body (i.e. open-source).

The solution decided on together with strategic decisions made by the governmental body will dictate the eventual architecture of the system.

If a governmental body needs to upgrade its existing infrastructure to enable it to deploy an electronic system, it should not hamper the implementation and maintenance of

46 This recommended practice is based on ISO 14105: *Electronic Imaging – Human and organisational issues for successful electronic image management implementations.* To obtain copies of this standard contact the South African Bureau of Standards' Sales Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria; Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Telefax: (012) 428-6928; E-mail: sales@sabs.co.za.

sound records management practices, since the implementation of a records management programme is not reliant on the availability of technology.

8.3 Design an electronic records management strategy

With a broader understanding of the body in mind, heads of governmental bodies should design a strategy for managing electronic records. The purpose of the strategy is to ensure that electronic records are trustworthy, complete and accessible. The strategy should be aligned with the governmental body's legal mandates and should provide a framework for the body's public accountability obligations.

The strategy should integrate –

- the legal and regulatory framework that applies to the governmental body;
- the needs of all stakeholders (internal and external);
- the preferred processes, procedures and technologies;
- short-term functional/operational needs and the long-term storage and access needs;
- the management of e-mail and web content;
- the physical care and intellectual control of the records.

The strategy should reflect the relationship between the body's business operations and electronic records management as well as between these and the management of records in other formats should the body still have processes that generate records in other formats.

8.4 Establish records management policies and procedures

An organization keeps information resources to support its operations, as well as to fulfill legal and other obligations.

All information resources, whether they are in paper-based, electronic or other format, should be managed by the organisation in terms of the broad policy guidelines contained in the National Archives and Records Service Act of South Africa, 1996 as amended. It is essential for each organisation to establish its own records management policy to integrate its own unique processes and procedures with the records management requirements of the National Archives and Records Service of South Africa Act. The policy should not only be in line with the Act, but should also link up with the organisation's overall mandate and mission objectives. It should specifically address the management of electronic records and should take into account the unique characteristics of the specific electronic applications that are in use by the specific office.

The policy would however not be of much use if the body does not design and maintain suitable supportive processes.

8.5 Assign responsibility for electronic records management

Organisational units (or specific staff members) should be identified for involvement in the management of electronic records. These units should, together with the responsible Information Technology staff, accept responsibility for the intellectual control and physical management of all electronic records.

People create and use records. They are a key factor in successful record keeping and records management. The organisation needs to ensure that the staff of the organisation is properly skilled to capture and manage records.

Specific leadership responsibility and accountability for records management should be

assigned to the records manager. The records manager should also be responsible for the management of records generated and stored in electronic systems. The records manager must thus have a basic understanding of the concepts of database management, file/document tracking, imaging and scanning, electronic document management, workflow and electronic records management to enable him/her to properly control records created in an electronic environment.

The management of electronic records should not be left to the IT manager alone, because he/she is involved with the technical management of the IT Systems and may not have time to apply records management principles to the records generated in these systems.

Specific roles and responsibilities regarding records management metadata should be defined and assigned throughout the organisation. It should be clear who is responsible for the capture of records metadata throughout the life-cycle of the record. Different users may be responsible for capturing metadata at different stages in a records life-cycle. It should also be clear who is responsible for the management of the metadata. Reliable and unaltered metadata is core to prove the authenticity of records. Specific accountability for the management of metadata should preferably be assigned to the records manager in co-operation with the IT manager. SANS 23081[47] recommends that

- Records management professionals should be responsible for the reliability, authenticity, usability and integrity of metadata associated with records, and for training users on capturing, managing and using metadata. Records management professionals should participate in the definition of metadata requirements, develop related policies and strategies, and monitor the process of metadata creation.
- All employees should be responsible and accountable for ensuring the accuracy and completeness of the records management metadata which they are capturing.
- Executives should be responsible for ensuring that internal controls are in place so that customers, auditors, courts, and other authorized users can rely on the information that the organization produces. Executives are responsible for supporting the use of records management metadata and related policies throughout the organization.
- Information technology personnel should be responsible for the reliability, usability and integrity of the systems used to capture and maintain metadata. They are responsible for ensuring that all records management metadata is linked to the related records and that these links are maintained.

8.6 Implement an Integrated Document and Records Management System for the management of unstructured records

The ideal is that if a governmental body contemplates using an automated system for the management of its records, such an office should implement an Integrated Document and Records Management System which contains an electronic records management application to manage the entire life-cycle of the records from the moment they are created until they are disposed of. Should a governmental body not be able to implement a fully fledged Integrated Document and Records Management System, it should take note of the requirements in par. 6.2 and 6.5.

However, governmental bodies should never assume that the implementation of the technology would magically solve all their records management and service delivery problems. In fact, the implementation of technology on top of existing records management and service delivery inadequacies could compound the problems to such an extent that service delivery could grind to a halt and the evidentiary weight of records

47 SANS 23081: *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*, pp 12-18.

could be seriously compromised.

The decision to implement any electronic system should be taken with care and should be planned and executed properly, more so, because technology in itself would not meet all the business requirements out-of-the-box.

Governmental bodies should not attempt to deploy technology without
- Doing a proper environmental analysis (see par 8); and
- Solving the records management and service delivery problems before the technology is deployed.

To assist governmental bodies to manage all their records according to sound records management principles it is required that they:

8.6.1 Implement an approved functional subject file plan

The following should receive attention:

Governmental bodies should
- compile and submit a functional subject file plan to the National Archivist for approval in terms of Section 13(2)(b)(i) of the National Archives and Records Service of South Africa Act (No 43 of 1996, as amended). This file plan must be used for the filing of electronic records as well as for the filing of records in paper-based and other formats; and since the file plan should always reflect the functions of the governmental body:
  - maintain the approved file plan by the reporting of amendments and additions to the file plan to the National Archivist for approval;
  - apply for the issuing of a disposal authority on the file plan.

8.6.2 Decongest records storage areas

Governmental bodies have huge amounts of paper-based records that were not filed against file plans, either because there is a serious lack of awareness of the benefits of sound records management practices, or because the necessary policies and controls to ensure that the staff comply with their records management obligations under the National Archives and Records Service Act are not in place.

It is impossible to share the information contained in these records. They are not managed properly and the information is irretrievable and not properly contextualised. Because these records are not kept in proper record keeping systems with proper security and access controls, their reliability as evidence of the business of an office is diminished. Records that do not carry evidential weight are a risk for proving accountability.

It is of critical importance to ensure that records are subject classified and that the relationships between the records are determined to contextualise individual pieces of information. It is also critically important that records that are no longer needed for operational, legal and historical purposes are identified and disposed of to maintain those records that are needed for the longer term economically. It would support operational efficiency if access to critical information is improved through the removal of unneeded records from congested storage areas.

The implementation of technology and specifically back scanning will not make these records and their resultant information retrieval and service delivery problems disappear. Active steps should be taken to back file the unfiled records and to decongest records storage areas.

8.6.2.1 Unfiled paper-based records

The National Archives and Records Service requires that all governmental bodies should file their paper-based records in an approved file plan. See Part 2 and Part 3 of the *Records Management Policy Manual*.[48] Should a governmental body have allowed its records systems to collapse to such an extent that records were not filed, the National Archives and Records Service requires governmental bodies to ensure that records are backfiled into appropriate systems.

The back filing of unfiled paper-based records cannot be done without having knowledge of the functions and procedures of a governmental body and without applying common sense. Some of the unfiled records are:

- exact duplicates of original records that are filed into existing file plan(s);
- drafts of originals that are filed on existing file plan(s);
- originals that were never filed into any existing file plan;
- reference copies of records that were published;
- copies of records that are available on the internet.

When conducting a back filing project, careful analysis is necessary to enable a distinction to be made between official records that should have been filed and transitory records and non-archival records that could have been destroyed in terms of General Disposal Authorities[49] issued by the National Archives and Records Service.

Only those records that are official in nature should be back filed according to the following principles:

- If approved file plan(s) exist for the period that the records were not filed, the unfiled records should be filed against that approved file plan(s).
- If no approved file plans exist for the period that the records were not filed the records should be classified into subject groups according to the functions of the office to enable subject-based lists to be compiled for appraisal purposes. Individual listing of each document according to the addressees is not acceptable.

8.6.2.2 Non-disposed paper-based records

The National Archives and Records Service requires all governmental bodies to implement systematic disposal programmes. See Part 4 of the *Records Management Policy Manual*.[50] Records that do not yet carry a disposal authority should be listed and disposal authority should be applied for.

Records that are already covered by a disposal authority should be disposed of when the retention periods have lapsed. The National Archives and Records Service has published a number of General Disposal Authorities on its website that can be used by governmental bodies to dispose of the records covered by those authorities.[51]

Should a governmental body be unsure if the records in its custody are covered by a disposal authority the National Archives and Records Service could be contacted to ascertain if disposal authorities exist.

---

48 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za. Alternatively hard copies can be obtained from the Records Management Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

49 See the National Archives and Records Service's website for an up to date list – http://www.national.archives.gov.za/rms/general_disposal_authorities.html.

50 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za Alternatively hard copies can be obtained from the RecordsManagement Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

51 See http://www.national.archives.gov.za/rms/general_disposal_authorities.htm.

Clearance actions should follow the issuing of the disposal authority. Clearance actions in terms of a disposal authority should be done as prescribed in the *Records Management Policy Manual*.[52]

8.6.2.3 Unstructured electronic records

In the paper-based environment, officials usually create and preserve records in a uniform manner according to a file plan used in the particular governmental body. The records are also physically kept in a uniform manner in a registry that is shared by the governmental body as a whole. Generally in the electronic environment, and especially where personal computers are used, there tends not to be any form of regulation of record creation and preservation. If these records are created to aid in decision-making and to perform transactions that support the governmental bodies' activities, governmental bodies are responsible for their proper management. If records generated in such an environment are not managed properly it can lead to the possible illegal destruction of records. This could seriously impede effective access for on-going functional purposes as well as long-term retention and preservation.

The National Archives and Records Service requires that governmental bodies should, as a matter of policy, ensure that the records that are created electronically are managed properly.

Records residing in unstructured environments should be maintained and retrieved in a manner which ensures that they retain their authenticity and reliability as evidence of transactions, and should also be disposed of when no longer needed functionally. However, it is not wise or appropriate to save all electronic records that currently exist on the staff's PC's into the new file plan in the electronic system when the system is deployed, because it is not archivally sound to merge records generated in different file plans with each other. Doing so would distort the provenance of the records, which would hamper the archival arrangement and description of the records according to international archival standards. Should records be back filed into the new file plan, it would also be issued with a disposal authority in terms of the new file plan. The danger of this is that records that could have been destroyed in terms of the disposal authorities issued for the previous file plans would now carry much longer retention periods than the paper-based versions that were filed on the previous file plans. The risk inherent in this is that during legal discovery actions, the best evidence rule will apply and governmental bodies would have to make available the still existing electronic copies of the records that should have been destroyed. Even copies existing on back-up media fall under the discovery rules. Governmental bodies would need to make the resources available to retrieve the records from the back-ups and would have to carry the cost of doing this, if the system is not able to identify all copies for disposal purposes.

The decongestion of unstructured electronic records cannot be done without having knowledge of the functions and procedures of a governmental body and without applying common sense. When conducting a project careful analysis is necessary to enable a distinction to be made between official records that should have been filed against a file plan and transitory records that could have been disposed without filing them. Some of the records existing on the PC's of individuals are:

- exact duplicates of records that are filed into the paper-based file plan(s);
- drafts of originals filed on the paper-based file plans;
- originals that were never filed into the paper-based file plans;

52 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za Alternatively hard copies can be obtained from the Records Management Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

- reference copies of records that were published;
- copies of documents available on the internet;
- e-mails which were filed to the paper-based file plans;
- e-mails that were not filed to the paper-based file plans;
- e-mails which are not official in nature.

Exact duplicates of records that are filed into the existing file plans, drafts of originals filed on the file plans, reference copies of records that were published, and e-mails that are not official in nature should be identified. These records can be destroyed in terms of General Disposal Authorities AK1[53] for the Destruction of Precise Duplicates and AT2 for the Destruction of Transitory Records (See Annexure E). Should the governmental body be able to identify them and destroy them they would need to keep a proper record of what was destroyed and when they were destroyed, should any legal action arise that requires these records to be produced.

The following possible solutions could be considered for official records that should have been filed:

- This first option is to mirror the previous paper-based file plans in the new electronic system as terminated file plans. The existing electronic records could then be filed against those file plans. However, there is a strong possibly that previous paper-based file plans did not make sufficient provision for all the functions of the governmental body. Filing against those file plans could necessitate belated revisions and additions to be made to the file plans. The benefit would be that the same disposal authority and retention periods could be applied.
- The second option is that the new file plan could be mirrored in the system as a terminated file plan and the records could be back filed into that file plan. The down side of this option is that during the appraisal process the governmental body would have to make sure that there is a correlation between the disposal instructions of the electronic records and the paper-based equivalents. This would also place a responsibility on the governmental body to ensure that the retention periods of the mirrored file plan correlate with the retention periods of the terminated file plans to enable the destruction of records that should have been destroyed long ago, had they been filed on the correct files.
- The third option is to maintain a directory structure based on the previous paper-based file plan on a shared corporate or “home” drive. The records could then be back filed into this file plan. The disposal rules of the paper-based file plan would apply to the records in this file plan. Access restrictions could be set up according to the requirements of the body. When all the records are back filed into the file plan on the shared drive, the drive could be turned to read-only to prevent staff from continuing to file to it. The records manager should be allowed to access the drive to execute disposal actions. The drive should be set up to capture an audit trail of all events affecting the records in the file plan.
- The fourth option is to print the records to paper, but this is not the most practical option. It would be labour intensive to scrutinise the paper-based files to ensure that there is no duplication of documents and that no incompatible versions are being filed. Furthermore, some documents may contain embedded links that will no longer work.

Whichever of the above methods is decided on in agreement between the governmental body and the National Archives and Records Service, it would require that the decision and the reasoning behind the decision should be documented properly, especially in the finding aids of National Archives and Records Service.

53 See the National Archives and Records Service’s website for information about AK 1 http://www.national.archives.gov.za/rms/general_disposal_authorities.html.

8.7 Ensure that records are trustworthy evidence of transactions

Heads of governmental bodies should ensure that records are authentic and reliable evidence of transactions. They should ensure that proper metadata and audit trail data is captured to prove the authenticity and reliability of the records.

8.7.1 Metadata

8.7.1.1 Design a metadata schema

The value of metadata should be understood to enable users to capture metadata judiciously. It is therefore necessary to explain the value and use of metadata in a documented metadata schema.

To be effective, metadata needs to be precise and comprehensible. All users should understand what it means. Each governmental body should document the metadata schema that they are using to explain the precise meaning of each metadata element and, if there are choices to be made, to create the choice lists (drop down lists) from which the users are allowed a choice. Choice lists are environment specific and will differ from one governmental body to another.

The National Archives and Records Service formulated a generic minimum mandatory metadata set[54] that covers only the minimum metadata necessary for the long term retrieval of records. Governmental bodies should use this generic metadata set as the starting point to design their own site and record specific metadata schemas.

The design of a metadata schema requires a partnership between records creators, custodians and users, the information technology staff, the legal staff and the records management staff.

8.7.1.2 Promote the use of metadata and educate the users

Most public servants rely on metadata to find information, but are unaware of the fact that it even exists. Governmental bodies should create an awareness of the purpose, creation and usefulness of metadata. The successful implementation of a metadata schema is very dependent on the co-operation of the users.

8.7.1.3 Implement the metadata schema

Creating and maintaining metadata to sustain authentic records over time requires attention, resources and staff. The capturing of metadata is not a once-off action. Metadata should be captured at creation and should be updated and maintained as a record moves through its life-cycle and records management processes are applied to it to ensure that the record remains authentic evidence of the transactions it relates to.

The records manager should be mandated to monitor the creation of metadata and to take corrective actions when required.

54 NARS *Managing electronic records in governmental bodies: Metadata requirements*, April 2006. http://www.national.archives.gov.za/rms.

8.7.2 Audit trail

8.7.2.1 Risk analysis

Heads of governmental bodies should commission a thorough study of the risks involved in not being able to prove the authenticity and reliability of records created in the execution of the body's daily operations.

The results of the risk analysis will indicate the type of audit data that should be captured, as well as the depth to which the audit trail should be captured and retained. For low risk records it may not be necessary to capture and retain all access events, while for high risk records (e.g. those records that are more likely to become the subject of litigation, an access to information request or an administrative justice case) it may be necessary to capture all access events as well as minute detail about who edited what under which authority, and to retain these for the life-cycle of the record.

8.7.2.2 Formulate an audit trail policy

With the results of the risk analysis at hand governmental bodies can make informed decisions about the audit trail data that should be captured. These decisions should be documented in the electronic records management policy.

The policy should document the types of audit trail data that should be captured and should indicate who may access the audit trail data and under which circumstances it may be accessed.

8.7.2.3 Manage audit trail data as records

Audit trail data should be managed as unalterable records to protect its authenticity as well as the authenticity of the records it pertains to. It should not be possible to alter or delete audit trail data without the facts of such events also being captured as records.

Heads of governmental bodies should effect the necessary policies and procedures are to guarantee that audit trail data is tamper free, and they should, within the framework of the access policy, ensure that audit trail data is accessible and interpretable by authorized individuals.

Since audit trail data is also considered to be records, it is necessary to formalize the need to destroy some audit trail data in a written disposal authority. Audit trail data increases exponentially every day each time a record is captured. Sometimes it is necessary to purge systems to ensure optimal performance. Purging should not be done without taking the long-term consequences into account. System Administrators should have proper guidelines as to what audit trail data may be purged and how they should document such actions.

8.8 Formulate an electronic records preservation plan

The value of the information governmental bodies generates justifies their investment in information technology. There is little point in investing large sums of money in technology if the use-value of the information created, stored and exchanged cannot be preserved. For the short term this is not necessarily a problem, but if records are to be maintained in an accessible form for as long as they are required, it does pose a problem. The challenge to preserve the trustworthiness and accessibility of the records is to do it in an efficient and cost effective way.

Even though the long-term preservation of archival records ultimately would be the responsibility of the National Archives and Records Service, it does not mean that governmental bodies need not address preservation issues.

For as long as the records are in the custody of the governmental body, the governmental body is responsible for their care and preservation. This implies that governmental bodies should draft a preservation plan as part of their electronic records management strategy and that they should implement the plan early on in the life-cycle of the records, before the records become inaccessible. Formulating a preservation plan is core to the management of the accessibility of records as long as they are needed.

Governmental bodies should preserve and care for any item forming part of an electronic records system in such a manner as to ensure that it is not exposed to harm or unauthorised access and under such specific conditions as the National Archivist may prescribe. Preservation planning requires that governmental bodies:

8.8.1 Understand the value of the records

Governmental bodies should conduct a needs analysis to enable them to build an understanding of the value of the information they generate. All information does not have equal value. Some has legal and evidentiary value and therefore demands proper management. Some information has long-term historical value that requires a long-term preservation plan. Needless to say, most information created by a governmental body supports the body's mandate.

Furthermore, governmental bodies should take informed decisions about the retention of the records after the National Archives and Records Service has issued written disposal authorities for the records. They need to know for how long they need to keep the records and why. They also need to know if there are any requirements about the medium in which the records should be kept – a legal requirement may for instance be that records should be kept in paper medium to ensure admissibility as in the case of wills.

They also need to know what the legal requirements about access are. Access to some records may be guided by statute. Privacy and data protection, intellectual property, etc. may be regulated by law. It is essential that the records management staff, the information technology staff and the legal staff are involved in this process, because they would all look at the issue from different angles.

With this information at hand, a governmental body would be able to make informed decisions about the preservation options they need to deploy.

8.8.2 Establish a technology watch programme

Heads of governmental bodies should ensure that the long-term accessibility of records is managed pro-actively to guarantee that authentic records are maintained for as long as they are required. A technology watch programme should be established to monitor the current software and hardware environment and to notify the body timeously when file formats or storage media are in danger of becoming obsolete. This programme should establish the necessary procedures for handling such eventualities. A technology watch programme will consist of:

8.8.2.1 Format watch strategy

Since access to records is dependent on the readability of the format in which they were created governmental bodies should formulate a format watch strategy. The purpose of

the strategy would be to

- provide the body with timely notification that formats are in danger of becoming obsolete;
- provide the body with a suggested format migration path;
- allow the body to take timely conversion and migration actions to prevent records formats from becoming inaccessible.

8.8.2.2 Media watch strategy

Access requirements normally determine the most appropriate storage options for records. Normally records that are accessed frequently would be kept on a server or a hard drive, while records that are accessed less frequently would be stored near-line on media such as optical disks in juke boxes or tapes in automated tape libraries while records that are seldom accessed are stored off-line on removable media. Whatever the choice of media, the dependency on the media to access the records should be considered – hence governmental bodies should formulate a media watch strategy. The purpose of the strategy would be to -

- provide the body with a timely notification that storage media is in danger of becoming obsolete;
- provide the body with a timely notification that data is degrading;
- provide the body with a timely notification that media is degrading;
- allow the body to take timely maintenance and migration actions, to prevent records from becoming inaccessible.

8.8.3 Migration strategy

There are several approaches to ensure that records remain useful over time. Not all approaches are very practical and all of them have their own set of limitations.

One approach is to maintain a “museum” of computer hardware and software, but there are no guarantees that the technology will work when needed. Emulation uses emulator programmes to simulate the behaviour, look and feel of other programmes, thus preserving the functionality of the records in their original formats. The cost of emulation is very high and there are no guarantees that it will work. Encapsulation involves combining the object that should be preserved with all the necessary information about how to interpret it. However, the file sizes of encapsulated objects are very large, the format specifications must still be determined, and the encapsulated record must still be migrated over time.

Migration and conversion seem to provide the most useful techniques at this stage. Migration involves the process of moving records to new hardware and software platforms as the technology evolves, while conversion is the process of changing files from one format to the other – mostly from proprietary to non-proprietary formats. This approach should be planned properly and special attention should be given to converting and migrating the attached metadata and audit trial data at the same time to ensure authenticity.

In order to prevent loss of information and loss of functionality and to ensure legal admissibility and validity for audit purposes a migration programme should involve:

- establishing formal policies for migration to substantiate why specific options for migration were chosen and how they were used;
- assigning responsibility for migration to a specific person or unit;
- assessing the impact of migration strategies on the integrity and utility of records (including testing the approach on a sample of records before implementing it);
- establishing and implementing an appropriate quality control procedure for migration;

- documenting migration procedures and actions by preparing thorough and complete documentation of any measures taken to convert records to new formats (documentation should include the organisation's migration policy, the reasons for selecting the specific migration option, the results of any tests or evaluation of the impact of the method used, the specific methods used and any known changes to the records that resulted from conversion and/or reformatting as well as details about the old and new file formats). These records themselves should be authentic and reliable.

Maintenance of electronic storage media as well as migration to new software and hardware platforms requires a continued commitment from an office. Governmental bodies need to budget for the expense as well as for the use of the human resources required to maintain electronic records in a readable format. If the necessary procedures are established beforehand, the use of resources can be planned to fit into the long-term strategies of the office.

8.9. Ensure electronic records are accessible

Certain basic records management principles apply to any record, whether in a filing cabinet or on a computer disk. Records are valuable only if they can be found when needed for action or reference. Proper classification, labelling, indexing, and preservation actions are necessary to ensure that electronic records are available and accessible throughout their useful life.

8.9.1 Classifying against a file plan

The easiest way to ensure that records are accessible is to file them in a file plan containing subjects connected to the business operations/functions of the office.

However, there are some types of records, especially those existing in business applications other than correspondence systems, like customer relationship management systems, financial systems, procurement systems, etc. that cannot be indexed against a file plan.

Governmental bodies should ensure that their records management policy clearly indicates to the users in which cases indexing against the file plan are required, and in which cases not. For example, the National Archives and Records Service requires indexing against the file plan when the following systems are used:

- enterprise content management systems;
- integrated document and records management systems;
- document management systems;
- e-mail archiving systems;
- imaging and scanning systems;
- digital asset management systems; and
- also when there are only standalone PC's and PC's connected to network drives.

The National Archives and Records Service does not require indexing against the file plan in for example the following cases:

- Geographical Information Systems;
- Personnel management systems, like Persal;
- Procurement management systems, like Logis, etc.

It is advisable that governmental bodies discuss the matter with the National Archives and Records Service if they are uncertain about when filing against the file plan is required and when not.

8.9.2 Indexing

Indexing is another term for capturing metadata. Indexing is normally done by different users in different stages of a records life-cycle. The main purpose of indexing in the short term is to be able to make unique identification of records possible to enable the retrieval of records that were filed. For the long term, however, the purpose of indexing is to capture appropriate metadata to ensure that records are authoritative. Governmental bodies should therefore ensure that the users know the importance of indexing.

Users should be allocated specific responsibility for indexing. It is important that indexing of individual records is done with care to enable the records to be retrieved in the shortest possible time.

8.9.3 File naming conventions

A file on a computer is what we would normally call a document. A file name is the name of an individual document on a computer and is the main method of retrieving electronic records. In most governmental bodies naming individual electronic records is left to the discretion of the creators. It may however be a good practice to establish a file naming convention to ensure that all electronic records are equally retrievable by all users in the shortest possible time, especially as the volume of records grows.

Each individual record should carry a unique logical file name and should be able to outlast the creator who originally named it. Governmental bodies should remember that records are not only created for short term functional use by their creators, but are created as evidence of the business of the body. Records become part of the corporate memory to be shared in the medium term and part of the national archival heritage in the long term.

A file naming convention would foster collaboration based on a mutual understanding of how to name files, especially in an environment where a file plan is not used. Records that are logically named are easier to manage, e.g. very few people will understand the file name MERPG.pdf but if named Managing Electronic Records Policy Guidelines.pdf, users will immediately know what the document is.

Rules for naming documents should be kept simple and clear, so that they can easily be introduced and followed. The value of file naming conventions lies in the use of a few simple rules that take away the burden of decision and encourage consistent practice. Naming rules should follow the same logic and consistency across different types of items, following the same pattern for similar situations – so that, once learned, the user can reasonably predict how the rules will apply in a new situation.

Conventions for naming electronic documents should be co-ordinated with those for naming folders, so that a document title does not contain unnecessary general information already present in the folder in which it is filed: for example the name of a project or organisational division.

The use of file naming conventions should be addressed in the electronic records management policy.

8.9.4 Ensure that electronic storage media are identifiable

Labels are essential to identify electronic media. Labels on a diskette's jacket (external labels) should include the originating office name, title, beginning and ending dates, what software was used to create the records (e.g., LOTUS 1-2-3 or MSWord), and on

what equipment it was produced. Labels on a computer magnetic tape should include the volume/serial number, the name of the office that created the data, and data set name(s). Identification of any access restrictions should be included on any external label.

8.10 Establish proper records storage facilities

Governmental bodies are required to keep records of their business activities to enable them to be accountable to the public and the state. Governmental bodies cannot give effect to this mandate if they do not provide adequately for the physical care of records. Records should be stored, handled and accessed in such a way that it meets daily operational requirements as well as long-term preservation needs.

Governmental bodies tend not to plan for records storage when office space is acquired. Such planning is essential to meet their records retention and accountability requirements. The *Records Management Policy Manual* contains information about the storage conditions recommended for electronic records.[55]

8.11 Manage e-mail as records

8.11.1 Formulate an e-mail policy

Each governmental body needs to establish a policy for the capturing of records of e-mail communications. Its own unique functions and environment should inform this policy. The policy should be endorsed by senior management and should be communicated throughout the organisation as part of the overall records management policy.

The policy should inform e-mail users that official records communicated through e-mail systems must be identified, managed, protected, and retained for as long as is needed for ongoing operations, audits, legal proceedings, research, or any other anticipated purpose. The policy should also explain how the governmental body would implement a records management programme that includes the management of e-mail records. The policy should cover the following records management aspects:

- how the e-mail should be filed against the corporate file plan;
- how and what metadata should be captured;
- how the disposal of the e-mails would be managed;
- where official records will be kept, such as in a central repository associated with a departmental network or LAN or in decentralised electronic or paper-based filing systems;
- procedures for security, backup and purging to protect records from alteration, loss, or inappropriate destruction.

Due to the volume of e-mails received on a daily basis it is very difficult to have a central authority that can decide which e-mails are records and should be kept. These decisions are left to the discretion of the users. However, without proper guidance about which records to keep, it will be difficult for the users to make sound decisions. It is recommended that the e-mail policy should contain details about which e-mails to consider for retention and that the e-mail procedures contain detailed diagrammatic decision tables to guide user actions. See Annexure K for examples.

For an example of an e-mail policy written from a records management perspective see

55 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za Alternatively hard copies can be obtained from the Records Management Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

Annexure J.

8.11.2 Determine retention periods

Retention periods for records communicated through e-mail systems, like other records, are derived from the functional needs of the office and any additional legal and audit needs. Generally, records transmitted through e-mail systems will have the same retention periods as records in other formats that are related to the same function or activity.

8.11.3 Develop procedures for e-mail management

Governmental bodies should develop e-mail management procedures to support the e-mail management policy. It is not sufficient to obligate users to manage e-mail without explaining how to do it.

The e-mail procedures should include guidance on how to create official e-mails that would be authentic and reliable and contain sufficient proof that official transactions were conducted. The procedures could include guidance about:

a) Proper subject line

Subject lines are very important, since they indicate to a recipient what the message is all about. If subject lines are not used appropriately the recipients may not realize the importance of the message and choose to read it later or not at all. Users should allocate useful subject lines to e-mails. If a user receives a message with a senseless subject line and needs to reply to or forward it, the subject line should be changed to properly cover the subject of the e-mail before sending it off.

b) Auto-signatures

Sometimes the staff receive e-mails from people that they don't know and that do not identify themselves or their place of business properly, because the e-mail addresses are not specific e.g. Peter.Baker@hotmail.com versus Peter.Baker@communication.gov.ky. At least for the latter one would be able to deduce from the domain name that Peter Baker is at the Department of Communications of the Cayman Islands. For the former one would not know where he is from, except if there is some other identifying information in the e-mail message. Auto-signatures are a way to provide recipients with alternative ways to contact the sender.

An auto-signature should as a minimum requirement contain the following identifying information of the sender

- name
- position
- section name
- name of the organization
- phone number
- fax number

c) Creating and replying to messages

These could contain rules for

- addressing to main recipients and to c.c. recipients;
- message length and use of attachments;
- managing dialogues;
- use of categories and labelling.

d) Message length and attachments

There are two broad approaches to the use of e-mail for formal business, namely:

- using the e-mail purely as a covering note for sending an attached document, so that only the document needs be saved; or
- composing longer text messages, which contain the text directly; the message itself is kept as a record.

The former approach requires management of the native document over time, and is unwieldy in many situations. The latter has the advantage that the message is plain-text based, and is easier for the user to produce.

The most appropriate form to use will vary according to the nature of the communication, but it is often better to encourage direct use of e-mail where appropriate, rather than extensive use of attachments – and this format is easier to maintain over time. Where use of attachments is preferred users should be encouraged to capture the appropriate metadata for the attachment separately from that of the e-mail.

e) Managing dialogues

E-mail messaging is an unstructured medium which will tend to become disorderly and tangled unless guided by disciplined procedures. Confused e-mail threads and much repetition of previous message text in dialogues will produce confused and repetitious records. Disjointed replies and the use of embedded messages are also sources of poor structure that are difficult to manage. Users should receive clear guidance on how to conduct e-mail discussions in an orderly fashion and at the same time protect the authenticity of the discussion.

f) Managing the InBox

User guidance on managing a personal mailbox should cover:

- the benefits of structuring any personal folders within the individual mailbox to be consistent with folder structures used to store documents in both public and shared drives. This will help to integrate different filing structures at the logical level, and is a useful step towards integration at the physical level; as well as introducing personal information management disciplines.
- The need to delete messages and working copies, where these have been saved into a corporate file space and are no longer of local interest. This will help to ensure that in the longer term, duplicate copies of information items are destroyed and to reduce the likelihood of alternate versions arising.
- The potential for automatically routing incoming and outgoing mail to nominated folders, using the Inbox Assistant, where standard types of message can be pre-determined according to characteristics recognisable to MS Outlook. This can help to build structured sets of records, but should only be used with records that can reliably be identified by metadata characteristics.

g) Filing messages

The basic rules for responsibility in filing an e-mail message would for example be:

- the sender files a message sent within the organisation;
- the recipient files a message sent from outside the organisation;
- recipients marked as c.c. do not need to file the message, except if they reply to the message in which case they will then be considered the sender of the reply.

8.12 Manage websites and web-based activities as records

Websites may contain records or be records in their own right. These records should be managed as part of the overall electronic records management strategy.

Websites should be managed according to the basic principles that apply to records in any medium. The management and retention of websites are subject to the National Archives and Records Service of South Africa Act (Act No 43 of 1996, as amended), and its regulations. SANS 15489[56] outlines the need for organisations to develop strategies to ensure that "full and accurate" records are captured into records classification systems and that these records should be retained for as long as required for legal, accountability and historical purposes. The National Archives and Records Service endorses this standard and advises that governmental bodies should apply the guidelines contained in the standard to capture and maintain records of web-based activities. Governmental bodies should carry out the following managerial activities:

8.12.1 Risk assessment

Governmental bodies need to assess the risk associated with the improper management of websites and web-based activities as records. They need to determine

- The current state of record keeping in the governmental body;
- The purpose of the website;
- The evidential and informational value of the website;
- The nature and importance of the materials posted to the site;
- The audience of the site;
- How frequently the information on the site changes;
- The review dates of all information published to the site;
- The likelihood of it being requested to account for the content of its current, recent and older websites, whether by litigation, promotion of access to information requests, or otherwise;
- Its current ability to prove/disprove the existence of particular content at a given time.

Resulting from the risk assessment, governmental bodies need to determine what records to capture of their websites in their specific legal, business and social context. The necessary policy requirements associated with managing websites should then be drafted to ensure that these records are kept. Governmental bodies should document the results of the risk assessment. Websites are not static; therefore the potential risk level should routinely be investigated and documented.

8.12.2 Web content management policy

Each governmental body needs to establish a policy for the capturing of records of web-based activities. A web content management policy should address website planning, development and maintenance. The emphasis should be on records management rather than on technology. The body's own unique functions, environment and accountability requirements should inform this policy. The legal requirements for capturing authentic and reliable records and the need to sustain them over time would inform the web content management policy. The involvement of stakeholders is imperative in the design of the policy. Content creators, technical experts, internal users, records management staff and legal staff all have a role to play in the design and implementation of the policy to ensure the trustworthiness of the web records.

---

56 SANS 15489 - *Information and documentation – Records management – Part 1: General* and *Part 2: Guidelines.*

From a records management perspective elements to include in the policy are:

a) Identification of records
   Is the website a record in its own right?
   Does it contain unique records or do the records exist elsewhere?
   Does it create unique instances of records e.g. if it is interactive?
b) Completeness of records
   Define what would constitute a complete record in web terms.
c) Version control
   Describe how frequently the site should be updated and how to create versions.
d) Integration with other records systems
   Define how the web records integrate with other records systems, especially the file plan and related disposal schedules.
e) Metadata
   Define the web metadata to be captured.
f) Snapshots
   If the entire website is a record, define how and how frequently to take snapshots.

The policy should be endorsed by senior management and should be communicated throughout the organisation as part of the overall records management policy.

8.13 Establish a systematic disposal programme

8.13.1 Apply for the appraisal of all other records systems

In order to manage electronic records systems other than the correspondence system efficiently and determine retention periods, a governmental body must compile a comprehensive inventory/catalogue (See Annexure H) of all electronic records systems containing a brief description of the purpose of each system. The general disposal authorities for the disposal of ephemeral electronic and related records (Annexure D) and transitory records (Annexure E) that authorise the destruction or erasure of certain categories of electronic records can then be applied by the governmental body to dispose of non-archival systems.

The inventory/catalogue must be submitted to the National Archives to appraise the remaining electronic systems. The National Archives will require the office to compile detailed descriptions of the archival systems for the issuing of a disposal authority as well as for archival management and retrieval purposes. The schedule must be compiled according to the elements required in the schedule of electronic records systems (Annexure C).

The precise manner of how electronic records should be scheduled can be negotiated with the National Archives and Records Service. In some cases it may only be necessary to provide an explanation of the purpose of the system and the technology used. In other cases the National Archives and Records Service may request that systems be described in comprehensive fashion. Descriptions should then include an explanation of the data sets and files included in the system; the hard copy input and output; the processing, subset, and special format files created and used in the system; and the documentation that describes and defines the system and the data in it, as well as migration information.

The information in electronic records systems, including those operated for a governmental body by a contractor, have to be scheduled in the inventory (see Annexure H for an example of the inventory) as soon as possible, preferably before implementation of the system.

8.13.2 Transfer archival electronic records into archival custody

Should a disposal authority require the deposit of specific electronic records into archival custody, such transfers should be made as soon as possible to ensure their proper maintenance and preservation. These electronic records would be maintained permanently for subsequent use by the original body, other bodies, other organisations, researchers, and the general public.

Certain technical documentation is required to accompany computer files. Technical documentation would include the electronic records management strategy, and policy related to the management of the specific system, as well as the system technical manual and systems procedures manual, and the metadata schema (if it exists separately from the policies and manuals). Technical documentation should be sufficient to support the use of computer files for secondary analysis. If a transfer is made on tape/disk the custodian would also need specific information on how the tape/disk was written, identification and definition of all data sets transferred, record layouts specifying relative positions, lengths and definitions of all data elements, and code books for all unique codes used in the records. This is necessary to ensure that the new custodian would have possession of all the information that is necessary to prove the authenticity of the records within the relevant context.

Before transferring electronic records into archival custody it is necessary for a governmental body to arrange for the transfer with the archives repository. Any transfer problems can then be resolved beforehand. If records are identified as archival, the National Archives and Records Service will specify certain requirements regarding the format of the records. If the technology is too advanced for the archives repository to manage, the governmental body will be required to undertake archival preservation. The governmental body is responsible for all costs regarding transfer and archival preservation.

If electronic records of enduring value are to be transferred or copied from one governmental body to another, such a transfer must be authorised by the National Archives and Records Service in accordance with the National Archives and Records Service of South Africa Act.

When electronic records of enduring value are retained in the physical possession of a governmental body, the National Archives and Records Service will audit the extent to which such records are being kept in an accessible state. Subject to certain exceptions, the National Archives and Records Service is entitled to full and free access, at all reasonable times, to all government records in the custody of a governmental body. Where this involves electronic records the National Archives and Records Service will seek the assistance of appropriate staff of the governmental body to ensure that archival records are being kept in an accessible way, and that the governmental body is maintaining the metadata, systems documentation and contextual information necessary to preserve evidential values.

8.13.3 Erase electronic and related records only in accordance with a disposal authority issued by the National Archivist

No deletion/erasure of electronic records should be done without the assurance that the records are no longer required, that no work is outstanding and that no litigation or investigation or request which would involve the records in question in terms of the Promotion of Access to Information Act, 2000 is pending. Erasure should also be done in such a manner that ensures protection of any information requiring special security provisions.

When records are deleted/destroyed a destruction certificate should be submitted to the National Archives and Records Service. See Annexure 15 of the *Records Management Policy Manual*.[57]

8.14 Manage Data Warehouses and Geographic Information Systems as records

Governmental bodies should assess the risk associated with the improper management of and disposal of records from these systems and resulting from the risk assessment determine:

- how version control should be applied to these systems and
- how records of queries and the results of those queries should be captured and
- what metadata should be captured for each record?

The results of the risk assessment and recommendations should be documented.

Governmental bodies should, if possible, ensure that these systems integrate with the Integrated Document and Records Management System to enable reliable records of transactions to be captured. If this is not possible, the governmental body should put other methods in place to ensure that the authenticity of the records is guaranteed.

Specific recommendations about the management of Data Warehouses as records are not possible at this stage, but the following applies to records in Geographic Information Systems:

8.14.1 Geographic Information Systems

Governmental bodies should ensure that the management of records created in these systems is part of the overall electronic records management strategy and should ensure that policies and procedures are in place for the management of records created in these systems.

8.14.1.1 Formulate and implement a Geographic Information Systems Management policy

The policy should communicate the importance of this information as an asset that should be managed properly. The policy should address

- data management, including acquisition, selection and intellectual property rights;
- preservation, including appraisal and long-term preservation;
- authenticity and reliability;
- how version control should be applied to these systems;
- how records of queries and the results of those queries should be captured; and
- what metadata should be captured for each record.

8.14.1.2 Assign responsibility for the management of geospatial records

Specific functionaries should be identified to take responsibility for managing geospatial records. The functionaries so identified should receive specific records management and digital preservation related training.

57 The *Records Management Policy Manual* is available on the National Archives and Records Service's website http://www.national.archives.gov.za Alternatively hard copies can be obtained from the Records Management Division, Tel.: (012) 323 5300, Fax: 086 682 5055, e-mail: rm@dac.gov.za.

8.14.1.3 Obtain and maintain facilities for the management and preservation of the geospatial records

Proper planning is necessary to ensure that the hardware and software necessary to store and manage the data is adequately maintained and migrated through technology changes. Geospatial records should be included in the Technology Watch Programme.

8.14.1.4 Design and implement a geospatial metadata schema

There are international standards available for geospatial metadata that primarily support retrieval and not necessarily records management and long-term preservation needs. For example the Content Standard for Geospatial Metadata.[58] Governmental bodies should ensure that they capture sufficient metadata to support the long-term preservation of the records, using the National Archives and Records Service's minimum mandatory metadata set[59] as the starting point.

8.14.1.5 Implement records management procedures to ensure the authenticity of the records

The application of records management principles and procedures is necessary for the effective life-cycle management of geospatial data and related records. Appropriate long-term planning for the management of these records is critical to ensure the integrity and authenticity of the records. Geospatial data, like all other records, is at risk to become inaccessible due to changes in application software, operating systems and hardware, as well as the inaccessibility of storage media. The authenticity of those records as evidence of business transactions could be compromised seriously, which could as a result thereof put the legal admissibility in jeopardy. Inappropriate management could also lead to the possible illegal destruction of records. To enhance their accountability, bodies should ensure that, even without the benefit of an Integrated Document and Records Management System, they exercise effective records management control over these records.

58 http://www.fgdc.gov/metadata/constant.html.
59 NARS *Managing electronic records in governmental bodies: Metadata requirements* , April 2006 http://www.national.archives.gov.za/rms/.

ANNEXURE A: Summary of the records management functionality for Integrated Document and Records Management Systems

This Annexure contains only the **records management functionality** required of an Integrated Document and Records Management System. Governmental bodies should take note that the technical requirements as well as the integration with messaging and calendaring applications, imaging and scanning applications, document management applications, workflow applications, search and retrieval applications, digital asset management applications, web content management applications and security applications are critical to the success of the system.

Governmental bodies that wish to invite tenders for Integrated Document and Records Management Systems could use the National Archives and Records Service's draft Functional Specification for Integrated Document and Records Management Solutions[60] as part of the specification for the request for a tender. When using the draft functional specification, governmental bodies should ensure that the records management requirements of the National Archives and Records Service are integrated with their own business requirements. The draft functional specification contains generic requirements and should not be considered sufficient to replace the need for a proper investigation into the unique business requirements of an office.

The National Archives and Records Service requires that Integrated Document and Records Management Systems should contain the following minimum records management functionality:

Storage of electronic records

In the paper-based environment records are stored in a dedicated, secure environment. The same should apply to electronic records. It is not very practical to store records on a LAN file server. Access to the documents on the file server is dependent on the security features of the host LAN. The protection it gives to the documents is only as good as the users' application of the security system. Furthermore, if the electronic records are stored on the LAN file server, they will have to compete for space with the system files etc. Electronic documents should at the very least have the same level of secure filing space as the paper-based records. A sound reliable repository requires a dedicated, stable, long-term storage space.

Where should one then store electronic records? The records can either be stored in network-attached storage devices such as CD/DVD-ROM towers/ jukeboxes, etc. or in separate storage area networks. Whichever method is chosen, the following should be kept in mind when constructing a storage system:

- Prevent data loss;
- Offer adequate capacity that can easily be increased as storage needs grow;
- Provide fast access to data without interruptions;
- Be prepared for equipment failures;
- Use cost-effective technologies.

To ensure that records remain accessible it is imperative that the records management application provides backwards access to at least one of its superseded repositories and

60 The draft functional specification is currently under revision. Copies of the original draft can be obtained from Louisa Venter of the National Archives and Records Service, Tel.: 012 323 5300; e-mail: Louisa.venter@dac.gov.za.

databases.

File plan management

Without a proper file plan in place, a governmental body will not be able to obtain a disposal authority from the National Archivist. This will prevent the timeous disposal of records, which will in the long run have a negative impact on the system's performance. Without a disposal authority in place all electronic records created will also have to be migrated across changes in technology to enable them to be readable over a long period of time, which does not make sense from a financial perspective.

Proper file plan management requires that there should be strict control over making additions to the file plan or deleting folders from the file plan structure. If folders are added randomly without proper consideration, folders can be added for existing subjects. This can cause confusion when documents are filed. Deleting folders is a disposal action, which should only be allocated to the records manager/systems administrator. The records management software chosen should not allow for end users to have this function. Revising the file plan is a function that should only be allocated to the records manager/systems administrator.

An integral functionality of a file plan is that it allows for files to be closed and new volumes/parts to be opened. The records management software should also provide the capability to implement cut-off instructions for records folders. The cutting off of a folder will allow for the calculation of the retention periods according to the disposal authority issued on the file plan. The software should ensure that only the most recently created volume/part within a folder is open at any one time. However, the records in the other closed parts should remain viewable and retrievable.

Document filing

In a paper-based filing system documents are filed in a file cover which is used to keep records of the same subject together in chronological order. The same concept applies to electronic records. They need to be filed in chronological order in subject folders to enable them to be retrieved in context.

The full co-operation of the users is necessary to consistently and regularly file documents into the file plan in the repository. Without this, there will be no records to manage. In most governmental bodies staff tends not to file records, even in paper-based form. Filing documents should be extremely fast, simple and non-intrusive, to enable them to buy into the concept.

Records management software that provides for embedded filing might be the best choice. Embedded filing happens for example when the user clicks the send button when sending e-mail and the user is automatically invited to file the message to the file plan in the repository. Preferably, the records management software that is chosen should provide the same embedded facility for all documents that are created electronically. If users are prompted as part of the normal procedure to file to the file plan in the repository when they save a document they might not even notice that they are managing records!

Document classification

This refers to the process of selecting the appropriate subject from the file plan and assigning the subject identifier to a specific document. This way all documents are associated with a subject in the file plan that reflects the business operations/functions

of the office.

Classifying documents according to subjects should preferably be an end user task. If the end users send documents to the repository without classifying them first, the systems administrator/records manager will have to review all documents sent to the repository and classify them in order to create proper records. Without being assigned subjects, documents that are supposed to be linked together and read in context will not be able to be retrieved as a single unit.

It is so that powerful retrieval tools exist whereby records can be retrieved by using key word searches. However, practical experience has shown that:
- if the correct key word is not used, records are not retrieved;
- the results of the key word retrieval are so enormous that it takes up a lot of time to page through everything to find the documents that belong together.

It does make sense to link documents that should be read together to the same folder. This provides an alternative search method, with more relevant results.

The following should also be considered:
- Classification of documents is required in order for disposal instructions and retention periods to be allocated;
- Classification according to subjects in the file plan links paper-based records to electronic equivalents. It is very important that the paper-based records and the electronic records be classified against the same file plan. This will ensure that records on a given subject in all media are managed against the same retention rules and that all records on a given subject are retrieved comprehensively.

Document search/retrieval

This is the primary reason why users would want to use an electronic system. Nobody likes to page through hundreds of irrelevant documents to find those that they are interested in. When the users realise that retrieval is easier and more reliable when they classify the paper-based and electronic records against the same file plan, they will be more inclined to file electronic records to the classification system in the repository.

Because users have high expectations of electronic retrieval systems, most records management software has the capability to do full text searches and some also have advanced search aids such as thesaurus assist, relevance ranking, concept searching, Boolean operators, metadata searching, etc.

The records management software chosen should preferably also allow for the paper holdings of the body and records in other formats to be recorded. This will enable the users to find records in all formats on a specific subject.

Metadata management

Preservation of metadata with the specific electronic document gives context to the document. Without the necessary context attached the electronic document will not be a record. It is no use to have the content but not to know where it comes from, who the creator was, when it was created or where it is located. The records management software chosen must prompt the users to preserve the metadata with the documents they create. It must also support automated capturing of as many metadata elements as possible, to minimise the amount of data entry performed by the users.

The National Archives and Records Service determined a set of minimum mandatory

metadata, the capture of which is necessary for the long term preservation of archival electronic records.[61]

Retention and disposal

A fundamental aspect of records management is the use of retention schedules to manage the disposal of records from operational systems. Disposal schedules define how long the records have to be kept by the system, and how they may be disposed of. The disposal instructions and retention periods are applied to each subject file within the file plan. This means that all documents within that subject file carry the same disposal instruction and retention period. It also means that the disposal instruction and retention period apply to records in all formats relating to a subject.

To ensure that the right records are destroyed at the right time the records management software that is chosen should not allow for automatic software-driven destruction to take place. It should rather allow for built in triggers to prompt the records manager that a disposal action should take place. Triggers can be based on an event, such as the closing of a file, the last action date or any other action that the user specifies. The rationale behind this is that it can happen that a retention period is too short, or that it is necessary for some reason to change the disposal instruction of a file. Human intervention should be mandatory before any destruction takes place. This will enable retention periods to be reviewed and the correctness of the destruction to be confirmed. It will also serve to ensure that there are proper disposal authorities in place, and that proper audit trails are in place before the physical destruction of records. It will also enable the reversal or alteration of the disposal instructions of records if necessary.

The system should alert the administrator if an electronic file that is due for destruction is referred to in a link from another file and must pause the destruction process to allow the administrator to review the retention periods of all related files, and require a confirmation by the administrator to proceed with or cancel the process.

Governmental bodies may need to move records from their system to other locations or systems to enable the permanent preservation of the documents for legal, administrative or research reasons or to use outside services for the medium term or long term management of the records. Sometimes they will also need to export the records, i.e. copying the records to another location or system while still retaining the original records, or to destroy the records. The system must be able to execute the transfer, export or destruction in a controlled manner. In all cases, the metadata and audit trails must be transferred, exported or destroyed at the same time as the records they relate to. The system must provide a well managed process to transfer records to another system or to a third party. It must be able to transfer or export a file such that the content and structure of its electronic records remain intact, all components of the record are exported as an integral unit, all links between the record and its metadata are retained, and all links between electronic records, volumes and files are retained. It must also include a copy of all the audit trail data associated with the records, volumes and files being transferred.

The system must report any failure during a transfer, export or deletion. The report must identify any records destined for transfer which have generated processing errors, and any files or records which are not successfully transferred, exported or deleted.

---

61 NARS *Managing electronic records in governmental bodies: Metadata requirements,* April 2006 http://www.national.archives.gov.za/rms/.

Where hybrid files are to be transferred, exported or destroyed, the system should require the administrator to confirm that the paper part of the same files has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.

The system should also enable the total destruction of series and individual files that are stored on re-writable media, by completely obliterating them so that they cannot be restored by use of specialist data recovery facilities.

Version Control

Governmental bodies should decide as a matter of policy at which stage documents should be filed as records in the repository. If draft documents are saved as new records in the records repository each time they are edited, it will become very cumbersome to identify and retrieve the final version (the record copy) of a document. Keeping unnecessary documents in the repository will also increase migration costs and will slow down the system.

The appropriate way to do version control is to keep draft versions of documents on the user's desktops or in the document management system and only to file final versions into the records repository. Editing of final versions should not be allowed. However where it is appropriate to retain various versions of a record as it passes through draft to finalisation, creating new and related versions of a record should be possible by making and editing copies of the final version and saving them as new records.

Archiving

Storage management is designed to ensure that data is moved through a defined hierarchy of storage devices and servers so that less frequently used objects are moved to lower cost storage to achieve a lower cost performance ratio. In storage management archiving is defined as the action of writing all the data/objects that are used infrequently to the least expensive, slowest storage medium where they are kept permanently in a storage repository for inactive data. The purpose of archiving is therefore to keep inactive records on the cheapest storage medium.

Records management enables governmental bodies to create, maintain, use, store and dispose of its records efficiently and cost effectively. It helps governmental bodies to conduct its business, deliver services and meet regulatory and accountability requirements. It also helps to control the amount of information created, received and stored. Furthermore it helps to maintain records economically and it promotes operational efficiency by improving access to critical information by removing unneeded records from current systems.

Storage management and records management complement each other in achieving cost effective public administration.

In records management terminology the terms archive/archiving are interpreted differently. The National Archives and Records Service Act defines archives as records in the custody of an archives repository. The purpose of having archives in an archive repository is to take into custody non-current records that were identified in a records appraisal as being part of the social and historical memory of government which should be kept as the national archival heritage. The goal of an archives repository in this case is to keep records of archival value for centuries to come and to make and keep them accessible for research purposes.

Electronic records can be archived in two ways:

- When records are archived with an electronic document management system the documents are moved from central magnetic disk storage to offline or less expensive storage media. The electronic document management system supports the ability to search document profiles as if they were online, and the documents can be retrieved from offline storage to online use.
- With an electronic records management system the records are physically removed from the repository entirely and they are transferred to an archives repository or to off-site storage and the governmental body gives up custodianship of the records.

The records management software chosen must include both possibilities and should preserve the format, profiles, and supporting contextual information (the metadata) of each document when it is archived.

Long term format

The electronic records management system must provide the functionality to store records in non-proprietary formats, or to convert records to such formats upon checking them into the electronic repository, because non-proprietary formats are better suited for migration than proprietary ones. The adoption of internationally recognised data interchange and document format standards will simplify the migration process. Data interchange is the ability to store files on the media using one type of computer and then to access the content of the storage media by using any other type of computer, while non-proprietary format implies that records created in a specific format should be able to be read by other software packages in the same way as the creators and users originally saw them. There are no guarantees that any of the formats that exist at present would be able to be read in a few years' time. However, the international community seems to be settling for PDF/A[62] and XML as the long-term formats. It may therefore be necessary to convert the data written in proprietary formats to standard hardware and software independent formats (e.g. PDF/A, TIFF, XML) to enable migration strategies to be put in place.

An option at this stage is to ensure that records are self-sufficient by adding encoding metadata to the record. This is done by adding simple textual encoding that describes the data to indicate its extent, syntactic meaning, semantic meaning, and relationship to other data in the record, and a reference to the specification of the standard format that was used. This will enable future users to extract information from the records even if they do not have the specific format the records were created in, because they will be able to obtain the specifications of the formats that were used.

Security

Access control

Organisations need to control access to their records, as records contain personal and operational information that should be protected against unauthorised access.

The electronic records management software must be able to control or limit access to records, files and metadata on user level as well as group level, in the document management system as well as in the records repository.

62 The National Archives and Records Service is currently investigating whether PDF/A is an acceptable long-term format. PDF/A was recently published as an international standard. ISO 19005-1 *Document management Applications - Electronic document file format for long-term preservation-Part 1: Use of PDF 1.4 (PDF/A-1)* is currently under consideration for adoption as a South African national standard.

Security classifications

In some environments e.g. the security establishment, there is a need to limit access by using a scheme of security categories and security clearances. These clearances take precedence over any access rights that might be granted using normal access control features. This is achieved by allocating to subjects, files and/or records one or more "security classification". Users can then be allocated one or more security clearance(s) that prevent access to all subjects/files/records at higher security classifications.

The system must allow security classifications to be assigned to records, and should support the review of security classifications.

Backup and disaster recovery

For disaster recovery purposes the system must be provided with comprehensive controls to provide regular backup of the records and metadata; and to be able to recover rapidly any records if lost because of system failure, accident, security breach etc.

Regular automated backup and recovery can either be provided by the records management system or by integration with the utilities of an Electronic Document Management system (EDMS), or a Database Management System operating with the records management system.

Backup and recovery functions should be divided between the records administrators and IT staff.

Authenticity

Information contained in records is a means of ensuring accountability and it may need to be produced as evidence in courts of law. To protect the authenticity, reliability, integrity, accuracy, adequacy and completeness of records, and to ensure their legal admissibility, the records must be protected against alterations by users and system administrators.

The electronic records management software must be able to prevent changes to the content of records and must provide the functionality to record all events that affect the records to make it possible to track deliberate or accidental alterations of records. It is imperative that the system logs an audit trail of all actions that were taken against a record including the date of the action and the identification of the person who has taken the action. It should log changes to the records and to the metadata. The system should also be capable of preserving the audit logs as records in the electronic repository and must prevent them from being changed.

Audit trail

An audit trail is a record of actions taken on records within the electronic repository.

Records must be able to be deleted from the system. The electronic records management software must provide the functionality to record all events that affect the records to make it possible to track authorised and unauthorised deletion of records.

The National Archivist is the only authority who can authorise the legal destruction of

records in terms of a disposal authority. It must not be possible to destroy or delete records or their metadata information outside of the normal disposal function. It must also not be possible to hide records by deleting their metadata. All disposal actions should be logged to ensure that illegal destruction of records could be traced.

Proper records management also requires that files and their metadata should be transferred from one storage medium or location to another, as their activity decreases and/or their use changes. This transfer can be to either near-line, offline or into archival custody.

It must at all times be possible to trace the precise location of records by recording references to the new location of the records. The destruction and transfer audit log should be kept as part of the records of a fully documented disposal process and should be unalterable.

The records management software must keep an audit trail of:
- all the actions that are taken upon an electronic record, electronic file or file plan;
- the user initiating and/or carrying out the action;
- the date and time of the event.

The system must also provide an audit trail of all changes made to:
- groups of electronic files;
- individual electronic files;
- electronic volumes;
- electronic records;
- electronic documents
- metadata associated with any of the above, and
- of all changes made to administrative parameters, e.g. changes to access restrictions, etc.

Digital certificates and digital signatures

Governmental bodies should ensure that electronic records management applications are able to integrate with digital signature and digital certificate technology should it be necessary to use this method to ensure that a record cannot be tampered with to protect its integrity and reliability as evidence of a transaction.

Rendition

The electronic records management application should be able to render records to different formats.

The purpose of rendition is to provide electronic documents in formats that are software and hardware independent so that they can be read by any computer system accessing the information. Rendition is a functionality to display documents in a different format than that they were created in. E.g. a Word document (.doc) displayed as a PDF (.pdf) document or HTML (.html) document, etc. This provides a format that everyone can display and eliminates the need for all users to have the original application installed on their desktops.

Records stored in their native format can be rendered to another read only format when accessed. This functionality is especially useful to protect the original format from being altered.

Website management

A website is a record, which contains information regarding the structure and functions of an office, the legislation it administers, its current policies and guidelines and advice on how to apply the legislation and policies as well as information on products and services.

An office can be held accountable for the information published on its site. For evidential, legal and accountability reasons it is imperative to keep a record of what was available on the site and how it was presented at a given time.

Ideally a website and its content should be managed via an electronic records management application. All documents published to the website should be checked into the electronic repository before being published to the site. The website should link to the repository and extract its information from the repository. This should prevent multiple copies of the same documents existing in various places. A record of a website should be created by extracting a precise copy (that keeps the look and feel of the website and maintains the links in the website without duplicating documents that already exist in the repository) of the site to the repository.

Websites should be version controlled and an audit trail should be kept of all changes to the site to guarantee its authenticity and the legal admissibility of the site.

The electronic records management application should be able to manage websites as records.

Managing records in non-electronic formats

Although governmental bodies strive to create less paper or even "paper less" environments they always end up with some paper-based records being created.

The records management application should include paper management functionality to allow for integrated records management. It should track files and containers, update their current locations and report on free space within storage facilities.

The following features are examples of paper management functionality:

- Bar coding of files and boxes;
- Label printing
- Movement tracking;
- Online file requesting
- Charge-out/in file management;
- Location Auditing
- Destruction and transfer

The application should log all actions taken on paper-based records and should enable the audit log to be kept as an unalterable record.

The application should also be able to manage records in other non-electronic formats such as microfilm, sound cassettes, videocassettes, maps, plans, photographs, etc in the same manner.

The application should log disposal and transfer actions taken on non-electronic records and should enable the audit log to be kept as an unalterable record.

Quality assurance

Because of the inherent volatility of electronic records and the larger role played by end users the records manager should play an expanded role regarding the quality assurance of records to ensure their validity as evidence of the business transactions of the body and their legal admissibility.

The records manager must be able to monitor the percentage of documents that are being filed. He/she should be able to determine if there are staff who do not file electronic records and why not. He/she should also be able to determine the rate of accuracy in filing. This would enable him/her to determine if there is staff that needs assistance/training in filing techniques.

The records manager must also be able to determine if disposal instructions and retention periods are being applied thoroughly.

Managing e-mail records

Users must file e-mail messages to the file plan in the repository. Electronic records management software can either automatically capture all e-mail messages, in which case even personal e-mail messages will be captured, or the software can prompt the user to file the message when he clicks on send, close or save.

The records management software chosen must automatically capture the transfer metadata (information on the sender and the recipient(s) and the date and time the message was sent and/or received). This data provides essential context for the message.

This is equivalent to correspondence on paper, where the record includes information identifying the sender and recipient and the date of the letter, not just the message. The software should also preserve any attachments containing information necessary for decision-making or to understand the intent or the context of a message. The records management software must, however, provide the capability to edit the subject or title, author or originator, addressee(s) and other addressees(s) metadata fields prior to filing the e-mail.

Migration Strategy	Advantages	Disadvantages
1. Transfer to paper or microfilm: This is the oldest method of migration and has been used effectively for textual documents that may be retrieved and read, but that will not be altered and re-used.	• from a legal and a technological point of view, the methods for demonstrating the authenticity of printed or microfilmed documents are well established. • alterations to records are more difficult and are relatively easy to detect • transfer to film or paper eliminates the problems of software obsolescence	• much of the functionality for both rapid retrieval and reuse is lost • this method does not work well for many formats of material because of the limited options for manipulation, linkage and presentation • Hybrid solutions can mitigate some of these disadvantages: retain computerised indexes to records to ease retrieval/scan to reconvert printed materials to digital form, etc.
2. Store records in a 'software independent' format: This strategy involves transferring electronic records to a simple software independent' format prior to storage. It has been used extensively with numeric data files and with some textual materials (e.g. text files stored in ASCII)	• the need for special software for retrieval and reuse of the records is limited once records are formatted in software-independent form, simple copying is all that is needed during subsequent migrations	• special programs may need to be written to transfer the records into a software independent format if the original system does not have the ability to 'export' files in a neutral format (Exporting means to format data in such a way that it can be used by another application.) • information and functionality may be lost in conversion • cannot be used with many complex file formats (multi-media records, hypertext).

Migration Strategy	Advantages	Disadvantages
3. **Retain records in their native software environment:** One option is to retain electronic records for as long as possible in the hardware and software system that was used to create them. This may be the only strategy available for preserving records in very specialised formats that cannot be accessed without the original software. [This strategy is closely related to 7 as it assumes the software will be available].	• eliminates the need to reformat records • retains all of the functionality of retrieval, display and manipulation	• requires long-term maintenance of hard-ware and software that may become obsolete (if the records are retained by the originator, a business decision would be made to migrate them to a new system if ongoing access is required; if the records have been transferred to an archives, the archives will have to migrate them to a new systems before their native environment becomes obsolete)
4. Migrate records to a system that is compliant with open systems standards: This strategy is an alternative to storing electronic records in a software independent form. Instead it converts them to a format that complies with widely used international standards (open standards).	• even through widely adopted standards are subject to change, they are not likely to change as often as proprietary software	• the initial expense of conversion from proprietary to standard formats (ideally, organisations should create records in standard formats that support their export to other systems) • conversion can result in the loss of information and/or initial functionality (the impact of conversion must be evaluated and tested in advance and the conversion process must be carefully documented) • many so-called 'open standards' have evolved into variant versions used by particular software manufacturers that may not be compatible

Migration Strategy	Advantages	Disadvantages
5. Store records in more than one format: This can reduce the uncertainty of software Obsolescence and increase the options for future migration (e.g. textual documents may be kept in two different word processing formats). This may be a sensible approach if no open standards exist and where several software products are competing for market share. Many systems today provide the capability to export documents in two or more formats so that special conversion is not needed.	• the organisation has an alternative format should one of the software packages become obsolete • retains both functionality and integrity of records when a single format cannot support both functions (e.g. electronic records stored as both bit-mapped image files and as scanned text in ASCII code. The bit-mapped images provide a physical reproduction of the original document, but the bit-mapped image cannot be searched; the scanned ASCII text may not have sufficient structure and contextual information to stand alone as a reliable record, but can be used for access and retrieval. (The term bit-mapped refers to hardware and software that represent graphic images as bit maps. Bit maps are a representation, consisting of rows and columns of dots, of a graphics image in computer memory. They are often known as raster graphics.)	• Increases the cost of storage and maintenance
6. Create surrogates for the original records: If the software dependencies are so extensive that the record cannot be migrated to different systems it may be necessary to create a 'surrogate' of the original record. Surrogates are documents that represent the original but that do not reproduce its original structure or content (e.g. summaries or abstracts of documents might serve as surrogates for textual records). This strategy may be necessary when access, retrieval or display of records require maintenance of executable software. This strategy should only be used when other options have been considered and found too expensive to not be feasible from a technology stand-point.	• if surrogates are created in software-independent formats or in formats that comply with open system standards, the complexity and cost of future migration will be reduced	• unless the process is carefully controlled and fully documented, the integrity of the records will be lost • surrogates rarely retain the functionality and utility of the original documents and often result in loss of content as well • the authenticity and legal admissibility of the record is open to challenge

Migration Strategy	Advantages	Disadvantages
7. Save the software needed for access and retrieval: [This strategy is closely related to 3].	• as an interim measure, it could provide repositories with an option of retrieving obsolete document for some years into the future	• the technical complexity of preserving software; most software is written to work only with specific hardware. As a result, saving software also implies saving the hardware needed to run it.
8. Develop software emulators: An alternative to preserving software is the development of new programmes that can 'emulate' (i.e. replicate) the functionality of obsolete software. If this strategy is used, it is critical to have access to documentation of the original software system that explains the precise software requirements needed to open and retrieve a document and these must be written in a software-independent form.	• does not require access to the same hardware and/or software used originally for the initial application	• special programs have to be written to emulate the obsolete software • can be an expensive and complicated under-taking; bodies considering this approach will need access to highly competent software designers and programmers • not fully tested • copyright issues have not been resolved

ANNEXURE C: Example of a description for an archival electronic records system

A. General remarks

A1. Electronic records are subject to the same requirements provided in the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) that apply to other records.

A2. Each system is evaluated on its own merits and archiving procedures are determined accordingly.

A3. Ideally archival appraisal should take place during the design phase of electronic systems. Appropriate procedures for timely provision of archival copies can then be built into systems. Moreover archival involvement at an early stage can ensure that the contextual information required to give validity to the records is included, especially in correspondence systems (e.g. addressee, sender, reference number, subject, date, etc.)

A4. As governmental bodies apply electronic systems differently, it is necessary to liaise with the National Archives and Records Service on the precise manner of scheduling. Schedules for appraisal purposes can then be compiled according to the needs of a particular body.

A5. Preferably the information in each automated system should be described in comprehensive fashion. That is, the description should include an explanation of the data sets and files included in the system; the hard copy input and output; the processing, subset, and special format files created and used in the system; and the documentation that describes and defines the system and the data in it.

A6. The schedule must be compiled in duplicate.

A7. Where there is more than one electronic records system, a separate description must be prepared for each one.

A8. Systems should be numbered consecutively.

A9. The information required should be given in detail.

A10. Websites should also be scheduled if they are not managed via the Integrated Document and Records Management System.

B. Information that should be included in the schedule

A complete and accurate description of all a governmental body's electronic record keeping systems and websites should include the elements indicated below. Part D of this Annexure contains and example of a schedule.

B1. Name of the system/website: Indicate the commonly used name and acronym of the system. In the case of a website, also include the URL.

B2. Implementation date: Indicate the date on which the system/site was implemented.

B3. System control number: Specify the internal control number assigned to the system for reference, control, or cataloguing purposes. For example, the information systems inventory number.

B4. Governmental body's programme supported by the system: Show the governmental body's programme(s) or mission(s) to which the system/site relates. In the case of websites, also describe sub-sites that are linked to the main site.

B5. Cite any laws or directives authorising such programmes or missions.

B6. List the names, office addresses, and telephone numbers, and location of the programme personnel who can provide additional information about the programme and the system supporting it. In the case of a website also provide the particulars of the webmaster and or the web content manager.

B7. Purpose of the system/site: Indicate the reasons for the system/site and the requirements met by it. In the case of a website indicate if it is used interactively, creating dynamic and interactive sites.

B7.1 Data input and sources: Describe the primary data input sources and the providers of the data to the system/site. Also give the names of any other systems, either inside or outside the governmental body, from which this information system receives data.

B7.2. Major output: Show the system's main products and the frequency of their preparation. For example reports, tables, charts, graphic displays, catalogues, or correspondence - prepared weekly, monthly, or yearly. Also indicate whether the information is transferred to other systems.

B8. Information content: Indicate the main subject matter, date coverage, time span, geographic coverage, update cycle, and other major characteristics of the system. Also tell whether the system saves superseded information and whether it contains micro data or summary data. In the case of websites include:

- The content pages that comprise the site, inclusive of the HTML mark-up;
- A description of records generated when a user interacts with a site and indicate if these records are captured in a record keeping system; and
- If the agency chooses to document its site this way, lists of the URLs referenced by site's hyperlinks.

B9. Platforms: Indicate the hardware and software platform on which the system was operated. List the formats the records were captured in. Indicate if any of the formats are obsolete already. In the case of websites describe the:

- Records relating to the software applications used to operate the site; and
- COTS software configuration files used to operate the site and establish its look and feel, including server environment configuration specifications.

B10 Continuation of system: Indicate if information contained in the system was imported from a previous system and/or if the system was run on another platform previously. Also indicate if the system underwent any name changes and/or if the system was inherited from an antecedent organisation. Describe any information losses that have occurred in the process.

B11. Location of documentation (metadata see par 4.1.4) needed to read and understand the files: Indicate where the code books and file layouts are maintained. Indicate the office, room number, and name of the person having

custody of them. Full documentation must accompany electronic records to assist in their use and interpretation. The documentation should include a background description of the purpose of the system; extent and use of the system as well as record formats and other information needed to recreate the system. Technical documentation would include the electronic records management strategy, and policy related to the management of the specific system, as well as the system technical manual and systems procedures manual, the metadata schema (if it exists separate from the policies and manuals). The technical documentation of the records, sufficient to support their use for secondary analysis, must accompany the transfer. If a transfer is made on tape/disk the custodian would also need specific information on how the tape/disk was written, identification and definition of all data sets transferred, record layouts specifying relative positions, lengths and definitions of all data elements, and code books for all unique codes used in the records. This is necessary to ensure that the new custodian would have possession of all the information that is necessary to prove the authenticity of the records within relevant context. A transfer list in which individual cassettes and their contents are specified is also required. Restrictions on access and use: Indicate national security, privacy, or other restrictions. In the case of websites include:

- website design records,
- records that specify the body's web policies and procedures by addressing such matters as how records are selected for the site and when and how they may be removed,
- records documenting the use of copyrighted material on a site,
- records that document user access and when pages are placed on the site, updated, and/or removed,
- site maps that show the directory structure into which content pages are organized.

B12. Metadata schema: Metadata is critical to the understanding of the context of the records. Provide full detail about the metadata captured in the system and attach the metadata schema that describes the conceptual entities, their elements, their interrelationships and their rules.

B13. Audit trail: Audit trail data is critical to prove authenticity of records. Provide full details about the types of audit trail data, where and how it is stored and how to interpret it.

B14. Storage management: Describe the storage media the master copies, back-ups and any other copies will be kept on. Describe the storage environment in which these records will be kept. Describe how often the records will be spot checked to detect any deterioration in the storage media. Describe how often the storage media will be refreshed (i.e. writing to new media of the same kind). Describe the migration strategy in place for these records (i.e. strategies are used to ensure that the information remains accessible across technological development in hardware and software platforms). Describe how often migration to new technologies will be done.

B15. Back-up and disaster recovery: Describe any back ups that exist. Describe any disaster recovery actions that were performed and how they influenced the records in the system.

B16. Disposal authority: If disposal authority has already been granted on any item the appropriate disposal instructions as well as the number of the disposal authority should be given. (See par C for a definition of disposal instructions.)

Where input documents are filed on files in a filing system approved by the National Archivist, the file number should be indicated.

B17. Date prepared: Give the date the schedule was prepared.

C. Disposal instructions: Electronic records

It is important to note that the National Archives and Records Service, in consultation with the governmental body concerned, determines archival value. Arrangements to this effect should be made with the National Archivist. There are two basic disposal instructions, A (representing "archival") and D (representing "not archival"), with variations determined by retention period. For instance, A1 means transfer to the National Archives and Records Service one year after creation and D3 means destroy/delete three years after creation.

A: Three options are available:

(i) The transfer of archival electronic records to an appropriate archives repository for permanent preservation as soon as possible after creation, or at such time as specified by the National Archivist.

(ii) The transfer of electronic records with archival value to an appropriate archives repository for permanent preservation in a proven archival medium such as paper or microform.

(iii) The office of origin being required to preserve the archival electronic records and maintain their functionality permanently.

D: Records not to be transferred to the National Archives and Records Service. The governmental body, keeping aspects such as legal requirements, financial accountability, transparency and organisational functionality in mind, has to determine its own retention periods.

D. Example of a system description for a schedule for electronic records systems other than the correspondence system

DEPARTMENT OF FISHERIES

1. System name:
Quota Control System (QCS)

2. Implementation date
1999.03.15

3. System control number:
FISH2

4. Governmental body programme(s) supported by the system:
Communication Services
Communication channels throughout the Department of Fisheries
Publications Division
Legal Services

5. Relevant laws and directives
Fisheries Act of 1990 (Act No. 45 of 1990)
Directive 7 of 1992 (Disposal of records regarding deep sea fishing)

6. Responsible Unit
The Quota Control Unit

7. Purpose of the system
The system is used to register the fishing industry and to allocate quotas to each registered industry.
The system provides the following functionality:
Registering the individual industries;
Calculating and allocating quotas.
Printing of permits.
Printing of statistics and management information concerning each registered industry.

7.1 Data input and sources:
Form Fish 207 completed by applicant.
Supportive legal documents attached to Fish 207.
Relevant information is also received from several wildlife organisations, universities and similar departments in foreign countries.

7.2 Major output:
Permits
Quarterly and annual statistics.
Reports/articles regarding related topics.
Information is sporadically exchanged with similar bodies in other countries.

8. Information content:
Information regarding the fishing industry.
Relevant information regarding ichthyology, the fishing industry, halieutics, weather patterns, etc.

Content date coverage, time span: 1980 - present

Geographic coverage: Oceans around the globe; water masses in Southern Africa

Update cycle: Every two weeks

9. Platform
Mircrosoft Access 97
Windows 97

10. Continuation of system (where applicable)
Originally run in a XYZ Database. Migrated to [Microsoft Access] DEF on 01.09.19.

11. Location of documentation needed to read and understand the files:
The Information Systems Division of the Department of Fisheries maintains codebooks and file layouts. A system technical manual and a system procedures manual exist.

Contact person: Ms B Bass, Information Systems, Room 101

A file containing metadata and other relevant information on each transfer can also be found in the List of Separate Case Files at Registry.

Information regarding the transfer of the cartridges can be found on file 9/1/1/3/5/6 at Registry.

12. Metadata schema
A detailed description of the metadata that is captured in the system is contained in the systems procedures Manual.

13. Audit trail information
Details regarding the audit trail information that is captured is contained in par. 5 of the Electronic Records Management Policy.

The systems procedures manual contains information regarding how to safeguard access and interpret the audit information.

14. Storage management
Online database

Storage environment according to National Archives and Records Services' guidelines contained in Annexure F of the *Managing electronic records in governmental bodies: Policy, principles and requirements*.

Spot checking of media on an annual basis, etc

15. Back-up
Daily, weekly and monthly back-up done on WORM magnetic tape.

Back-ups are stored off-site at commercial records storage company ABC.

16. Disposal authority:
Correspondence filing system: 2-S1NA
Additional information on file 13/2/1/4.

17. Date prepared:
2004-11-14

ANNEXURE D: General disposal authority number AE1 for the destruction of ephemeral electronic and related records of all governmental bodies

1. AUTHORITY

This document grants authority to governmental bodies in terms of section 13(2)(a) of the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) to erase or destroy ephemeral electronic and related records of all governmental bodies when no longer needed.

2. RETENTION PERIODS

Each governmental body should determine appropriate retention periods for records that do not have enduring value in terms of disposal authorities issued by the National Archivist.

In determining retention periods, the governmental body's own requirements for access to information for efficient functioning should be taken into account, as well as its obligations to the public for accountability, e.g. in terms of the Promotion of Access to Information Act, 2000.

3. INTRODUCTION: EPHEMERAL ELECTRONIC AND RELATED RECORDS

Ephemeral electronic and related records are defined as those that are not regarded as having enduring value.

Authority to dispose of electronic records is in most cases linked to the approval of classification systems and the issuing of disposal authority on the basis of such systems. In the electronic environment there is therefore a need for a sound records management system to be in place. This is in fact a requirement in terms of section 13(2) of the National Archives and Records Service of South Africa Act (No. 43 of 1996).

Erasure or destruction in terms of disposal authorities issued by the National Archivist should take place in a controlled and systematic manner under central supervision within each governmental body.

The following electronic and related records can be erased/destroyed:

4. DESCRIPTIONS

4.1 <u>Word Processing Files</u>

Documents such as letters, messages, memoranda, reports, handbooks, directives, and manuals recorded on electronic media such as hard disks or diskettes:

4.1.1 When used to produce hard copy that is maintained in files of a classification system.

4.1.2 When maintained only in electronic form, and duplicate the information in and take the place of records that would otherwise be maintained in hard copy providing that the hard copy has been authorized for destruction in terms of this disposal authority or another disposal authority issued by the National Archives and Records Service of South Africa.

4.2 Administrative DataBases

Data bases that support administrative functions such as financing, provisioning of supplies and services, and staff (EXCEPT where these are the line functions of the body), and which contain information derived from hard copy records authorized for destruction by this disposal authority or another disposal authority issued by the National Archives and Records Service of South Africa, if the hard copy records are maintained in a classification system. The National Archives and Records Service approves classification systems for use by governmental bodies. Hard copy printouts from these databases that are made for short-term administrative purposes.

4.3 Schedules of Daily Activities

Calendars, appointment books, schedules, logs, diaries, and other records documenting meetings, appointments, telephone calls, trips, visits, and other activities by public servants while serving in an official capacity, created and maintained in hard copy or electronic form, EXCLUDING:

4.3.1 Records determined to be personal.

4.3.2 Records containing substantive information relating to official activities, the substance of which has not been incorporated into official files.

4.3.3 All records kept at ministerial level.

4.4 Tracking and control records

Logs, registers, and other records in hard copy or electronic form used to control or document the status of correspondence, reports, or other records that are authorized for destruction by this disposal authority or another disposal authority issued by the National Archives and Records Service of South Africa.

4.5 Finding Aids (or indexes)

Indexes, lists, registers, and other finding aids in hard copy or electronic form used only to provide access to records authorized for destruction in a disposal authority issued by the National Archives and Records Service of South Africa, EXCLUDING records containing abstracts or other information that can be used as an information source apart from the related records.

4.6 Files/Records created in central data processing facilities to create, use, and maintain master files

4.6.1 Electronic files or records created solely to test system performance, as well as hardcopy printouts and related documentation for the electronic files/records.

4.6.2 Electronic files or records used to create or update a master file, including, but not limited to, work files and intermediate input/output records.

4.6.3 Electronic files and hard-copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files [Excluding audit trail files that are necessary to demonstrate who created the record, when it was created, that it has not been altered since creation, and audit trail files that capture information regarding the identity of users who authorized transfer or

destruction, the date a record was destroyed/transferred, and the authority in terms of which the record was des-troyed/transferred], system usage files, and cost-back files used to access charges for system use.

4.7 Input/Source Records

4.7.1 Non-electronic documents or forms designed solely to create, update, or modify the records in an electronic medium and not required for audit or legal purposes (such as need for signatures) and not previously scheduled for permanent retention in a disposal authority issued by the National Archives and Records Service of South Africa.

4.7.2 Electronic records, except as indicated in 4.7.3 below, entered into the system during an update process and not required for audit or legal purposes.

4.7.3 Electronic records received from another department and used as input/source records by the receiving department, EXCLUDING records produced by another department under terms of an interdepartmental agreement, or records created by another department in response to the specific information needs of the receiving department.

4.7.4 Computer files or records containing uncalibrated and unvalidated digital or analogue data collected during observation or measurement activities or research and development programmes and used as input for a digital master file or data base once it has been calibrated and validated.

4.8 Master files relating to administrative functions except where an administrative function is a line function of the body concerned

4.8.1 Master files that replace, in whole or in part, administrative records scheduled for destruction in a disposal authority approved by the National Archives and Records Service of South Africa.

4.8.2 Master files that duplicate, in whole or in part, administrative records scheduled for destruction in a disposal authority approved by the National Archives and Records Service of South Africa.

4.9 Data Files consisting of summarized information

Records that contain summarized or aggregated information created by combining data elements or individual observations from a single master file or data base that may be destroyed in terms of a disposal authority issued by the National Archives and Records Service of South Africa, EXCLUDING data files that are created as disclosure-free files to allow public access to the data; and those created from a master file or data base that is unscheduled, that was scheduled as permanent but no longer exists, or can no longer be accessed. The latter data files may not be destroyed before securing the National Archives and Records Service of South Africa's approval.

4.10 Records consisting of extracted information

Electronic files consisting solely of records extracted from a single master file or data base that is disposable in terms of a disposal authority issued by the National Archives and Records Service of South Africa, EXCLUDING extracts that are: produced as disclosure-free files to allow public access to the data; or produced from a master file or data base that is unscheduled, or that was

scheduled as permanent but no longer exists, or can no longer be accessed; or produced by an extraction process which changes the informational content of the source master file or data base. The latter files may not be destroyed before securing the National Archives and Records Service of South Africa's approval.

4.11 Print Files

Electronic files extracted from master files or databases without changing them and used solely to produce hard-copy publications and/or printouts of tabulations, ledgers, registers, and reports.

4.12 Technical Reformat Files

Electronic files consisting of data copied from master files or data bases for the specific purpose of information interchange and written with varying technical specifications, EXCLUDING files created for transfer to the National Archives and Records Service of South Africa.

4.13 Security Back-up Files

Electronic files consisting of data identical in physical format to master files or databases and retained in case the master files or databases are damaged or inadvertently erased.

4.13.1 Files identical to records scheduled for transfer to the National Archives and Records Service of South Africa.

4.13.2 Files identical to records authorized for destruction in a disposal authority approved by the National Archives and Records Service of South Africa.

4.14 Special Purpose Programmes

Application software necessary solely to use or maintain a master file or data base authorized for destruction in a disposal authority issued by the National Archives and Records Service of South Africa, EXCLUDING special purpose software necessary to use or maintain any master files or data bases for which disposal authority has not yet been obtained from the National Archives and Records Service of South Africa or are scheduled for transfer to the National Archives and Records Service of South Africa in terms of a disposal authority.

4.15 Documentation regarding electronic systems

Data systems specifications, file specifications, code-books, record layouts, user guides, output specifications, and final reports (regardless of medium) relating to a master file or data base that has been authorized for destruction in a disposal authority issued by the National Archives and Records Service of South Africa, EXCLUDING documentation relating to any master file or data base for which disposal authority has not yet been obtained from the National Archives and Records Service of South Africa or are scheduled for transfer to the National Archives and Records Service of South Africa in terms of a disposal authority.

ANNEXURE E: General disposal authority number AT2 for the destruction of transitory records of all governmental bodies

1. AUTHORITY

This document grants authority to governmental bodies in terms of Section 13(2)(a) of the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) to destroy transitory records.

2. RETENTION PERIODS

Each governmental body should determine appropriate retention periods for records that do not have enduring value in terms of disposal authorities issued by the National Archivist.

In determining retention periods, the governmental body's own requirements for access to information for efficient functioning should be taken into account, as well as its obligations to the public for accountability, e.g. in terms of the Promotion of Access to Information Act, 2000.

3. DEFINITION

Transitory records are those records created by officials but not required by the governmental bodies for which they work to control, support or document the delivery of services, or to carry out operations, to make decisions, or to give account of the activities of government. Such records are needed by officials for only a limited time to facilitate the completion of routine actions or to prepare a subsequent record required by a governmental body for the above-mentioned reasons.

4. GUIDELINES FOR THE IDENTIFICATION OF TRANSITORY RECORDS

4.1 <u>Conventional paper-based records</u>

Transitory records may include:

(a) information in a form used only for casual communication;

(b) cryptic notes made during telephone conversations/meetings/ discussions and on which formal reports/minutes created thereafter are based or which are reproduced formally in such documents;

(c) officials' diaries;

(d) manuscripts of letters, or other documents prepared for word processing;

(e) annotated drafts where the additional information is found in subsequent versions, except where retention is necessary as evidence of approval or the evolution of the document;

(f) copies of documents kept only for reference or convenience purposes, e.g. copies of letters the originals of which have been filed.

(g) Copies of classified records received:

- where the office from which the record emanates states that it has disposal authority from the National Archivist for this category of record; and

- where the receiving office has not annotated the record in any way (i.e. it is purely a duplicate), and instructions based on the incoming document are kept separately.

(h) original faxes made on heat sensitive (thermal) paper after photocopies were made for record purposes.

4.2 Electronic records

Transitory records in electronic form may exist in a variety of forms and formats regardless of data processing environments, from large centrally managed mainframes to stand-alone personal computers. The examples described below are applicable regardless of the environment.

This authority should be applied to electronic records within the context of the standard operating practices that institutions apply for the effective and efficient administration of their automated information systems.

Electronic records that are transitory include:

4.2.1 Electronic input/source records

(a) Electronic input/source records entered into a system during an update process that are not required for audit or legal purposes. Such input/source records may be deleted once the data have been verified and entered into the master file or database, or when no longer needed to support reconstruction of or serve as back-up to a master file or database.

(b) Electronic input/source records copied from a master file for transmission to another location. If the master file is retained, the version at the transmitted location may be deleted when the action is completed.

4.2.2 Intermediate input/output records

Electronic records containing data that are manipulated, sorted and/or moved from one execution of a programme to another in the process of creating or updating a master file or database. Such records may be deleted in accordance with system design specifications.

4.2.3 Valid transaction files

Electronic records consisting of data that are used in the course of batch processing to create an updated master file. Such records may be deleted in accordance with system design specifications. N.B. This does not include Master files from one system that are used as transaction files in a second system.

4.2.4 System audit records

Electronic records generated during the creation or use of a master file or database that contain information on the operation of the system, except where

they are required to support the integrity of the master file or database. Such records may be deleted in accordance with system design specifications.

4.2.5 Test records

Electric records consisting of routine data used only for the purpose of testing system performance. Such records may be deleted in accordance with system design specifications.

4.2.6 Print files

Electronic files copied from a master file or database where the only purpose is to produce hardcopy publications and/or printouts of tabulations, ledgers, registers and reports. Such records may be deleted in accordance with system design specifications.

4.2.7 Electronic documents

- Documents that were not communicated beyond the official who created them, e.g. electronic diaries; notes upon which reports or minutes were based; word processing documents created solely to produce a hardcopy version and where a duplicate is maintained in hard-copy files.

- Working copies or drafts of documents which gave rise to a final version in which all comments on the working copy have been incorporated, except where retention is necessary as evidence of approval or the evolution of the document.
- Information in a form intended only for non-official communication, e.g. non-official e-mail messages.

- Copies of electronic documents, kept only for reference purposes or convenience, where the documents are retained elsewhere for functional purposes.

4.3 Photographic records

Photographic records that are transitory may include:

- process photography, containing negatives created solely as an intermediate stage in printing operations, and where such negatives are used to create lithographic or photo off-set plates; and

- outs, containing photographs which do not become part of a collection, and are discarded immediately after creation because of poor quality duplication or repetitiveness. "Outs" do not include photographic records which are included with a group of records or other photographs for even a short period of time which are then believed to have lost their usefulness and are identified for "weeding" from the group.

4.4 Moving image records

Moving image records that are transitory may include: Video recording material generated to prepare a video presentation or production that is not required to reconstitute the completed production, and which is not defined as original footage or printing elements for final production.

ANNEXURE F: Handling magnetic media

1. Types of magnetic media

The term 'magnetic media' is used to describe any record format where information is recorded and retrieved in the form of a magnetic signal.

The common types of magnetic media are:

- Magnetic disk. Magnetic disks include the hard disk found in a computer that stores programmes and files. Magnetic disks provide random access. Also included are:
  - Removable hard disk. These disks are encased in a plastic housing that allows them to be inserted and removed from a processor. In this way, a single processor can have access to the data on multiple hard drives.
  - Removable disk. Removable disks include the relatively small-capacity floppy disks a.k.a. stiffy disks, as well as the larger-capacity peripheral disks, such as the Iomega Zip disks.
  - Cartridge. Removable cartridges contain disks encased in a metal or plastic casing for easy insertion and removal.
- Magnetic tape. Magnetic tapes come in reel-to-reel, as well as cartridge format (encased in a housing for ease of use). The two main advantages of magnetic tapes are their relatively low cost and their large storage capacities (up to several gigabytes). Magnetic tapes provide sequential access to stored information, which is slower than the random access of magnetic disks. Magnetic tapes are a common choice for long-term storage or the transport of large volumes of information.
  - Worm Tape. Allows for non-editable data storage.
  - Digital audio tape (DAT). DATs are in a cartridge format a little larger than a credit card. The industry standard for DAT cartridge format is a digital data storage (DDS) cartridge. DDS cartridges provide sequential access.
  - Videotape. Videotape provides sequential access to video footage (e.g., feature films).

2. Composition of magnetic media

A magnetic tape consists of a carrier of plastic film coated with a matrix containing magnetisable particles. By weight, the matrix contains about 70-80% magnetic particles, with the rest of the layer consisting of a plastic or resin binder, and other ingredients such as lubricants and fungicides. Sometimes the tape is coated on the reverse side with an anti-static material to reduce the build-up of static charges and to improve the winding capability of the tape.

Magnetic hard disks have a metallic base, usually aluminium. The base is coated on both sides with a matrix similar to that on magnetic tape.

Disk packs, which have a wide application in computing, consist of a number of hard disks stacked together around a central spindle. They require a special recording and playback system with many pairs of read/write heads.

RAID's are a group of loosely assembled hard disks. They are connected to one controller board, which controls them as if they were a set of platters from one disk. To improve data reliability, the same data exist in more than one place on the disk. If one of the disks goes down, it will thus be possible to retrieve the data from another disk in the RAID.

Floppy disks and diskettes consist of a plastic base, with a magnetic matrix, on one or

both sides. They are enclosed in a rigid, plastic protective jacket that does not easily flex or bend. There is a slot in the jacket through which the read and write head has contact with the disk.

3. Deterioration of magnetic media

All materials degrade over time. We cannot control this inevitable deterioration, but we can control how fast it happens.

It is useful to know that certain materials are susceptible to deterioration in particular ways just because of their properties, and that other materials deteriorate as a result of particular environmental conditions.

For example:

- The tape carrier can become brittle and easily broken. Deterioration of the matrix on tapes and disks can result in it flaking off the base.
- The particles in the magnetic layer that retain the coded information can become unstable leading to a gradual loss of signal quality and eventually information loss.
- Print-through can occur when tapes are stored for long periods without being played or exercised – the signal from one loop of tape transfers to the adjacent loop, resulting in poor signal quality.
- Extreme fluctuations in, or high levels of, temperature and humidity may cause the magnetic layer to separate from the base layer, or cause adjacent layers in a reel of tape to 'block' together. High temperatures may also weaken the magnetic signal and ultimately cause the medium to become completely demagnetised.
- Tapes are particularly susceptible to mould because pockets of air trapped in the windings can create microclimates that will support mould growth.
- Exposure of the magnetic layer surface to dust particles, dirt, grease and chemical pollutants can promote moisture condensation and oxidative deterioration. These contaminants can also interfere with proper contact with the playback head resulting in a weakening of the recording or playback signal.
- Data on hard disks can be lost due to head crash, which causes the magnetic head to touch the surface of the disk and scrape away the magnetic data. This makes the entire disk unreadable.

4. Magnetic fields

Because magnetic media store information by the alignment of magnetic particles, even a small external magnetic field can cause information loss on a tape or disk if it is in close proximity for long enough. Magnetic fields can be generated by items such as fridge magnets, magnetic screwdrivers and most machines with electric motors.

The degree of risk depends on how close the media is to the source of the field, the strength of the field, and the duration of exposure. The effect of a magnetic field decreases with distance. This means that running a vacuum cleaner past the shelves will probably not cause any damage, whereas storing tapes or disks close to a large electrical generator could result in serious loss.

5. Handling and care of magnetic media

- Handle with care.

- Wear lint-free gloves, or ensure that hands are clean and dry.
- Open-reel tapes should be supported by the hub of the tape during handling and transportation.
- Disks should never be flexed, bent or picked up by the oval slot in their jackets or by the centre hole of the disk.
- Labelling should be in ink rather than pencil as graphite dust from the pencil could interfere with the reading of the disk or tape. Labels should not be written on once they are attached to a disk.
- Items should only be removed from their protective packaging for use and returned to their containers immediately after use.
- Cassettes and tapes should be wound to the end of one side after use. They should never be left stopped partway through for any length of time and the use of 'pause' mode should be avoided.
- Special care should be taken when moving magnetic media. Ensure that the media are not bumped or dropped, and items should be properly packed in custom-made transportation canisters. Freight and courier companies that specialise in the transportation of magnetic media should be consulted where large quantities or important material is to be moved.
- Do not touch the recording surfaces of floppy disks, do not fold or bend them, and do not write on the paper jacket.
- Keep food and drink away from storage media as well as equipment.
- Store disks and tapes in a vertical position in a storage container.
- Store diskettes under normal office conditions, taking care to avoid extreme fluctuations of temperature or humidity.
- The storage environment must be climatically controlled with a constant temperature of between 18 to 20 degrees Celsius (optimum 18 degrees), and a constant relative humidity of between 35 and 45 percent (optimum 40%).

6. Protective packaging

Paper or cardboard enclosures should never be used for the storage of magnetic media. These enclosures tend to generate dust that can be particularly damaging to magnetic media.

Tapes should be stored in cases made of non-magnetic material, preferably an inert plastic such as polypropylene. PVC plastic is unsuitable because it contains chlorides that may damage the tape. Cases should have fittings to hold the tapes in position by the hub. They should be strong enough to protect the cassettes from physical damage and close tightly to keep out dust particles.

Reels or cores used for winding tapes should be clean and free from cracks or sharp edges. There should be slots in the flanges of the reels to prevent bubbles of air from being trapped between the layers of tape on the reel. Reels should be made of aluminium or a stable plastic such as polypropylene (not PVC).

Floppy disks and diskettes should be stored in protective envelopes that are resistant to static electricity build-up and have a non-abrasive surface. Tyvek envelopes are widely available and are suitable for this purpose.

7. Storage

Areas intended for storage of magnetic media should be checked by qualified staff to ensure the absence of magnets or magnetic fields that exceed acceptable limits. Walls, floors and all storage equipment, electrical equipment and wiring within the area must be checked.

The area should be free from potential sources of dust, such as typewriters, paper shredders and printers. Carpets should not be used and measures should be taken to prevent dust entering from outside, e.g. installation of an air lock, or maintaining positive internal air pressure.

Magnetic media should preferably be stored in a vertical position in closed metal cabinets, to provide extra protection against heat and dust. However if there are adequate environmental controls, storage on open shelves and racks is acceptable. The storage equipment should:

- be sturdy
- allow for vertical storage of tapes and disks
- be electrically grounded.

8. Environment

Magnetic media should be stored at temperatures between 18-20 ºC and relative humidities between 35 – 45%. In these conditions the natural deterioration of the items can be slowed. In some instances deterioration can be slowed further by lower temperatures. It is important that these environmental levels are stable. Mould will start to grow at around 60% relative humidity. If the humidity fluctuates more than 10% in 24 hours or the temperature is too high, the items will be stressed, speeding up their deterioration.

Materials degrade quicker when exposed to ultraviolet light. Fluorescent tubes that are low in ultraviolet light should be used wherever possible in storage areas. Ultraviolet light can be easily measured with a light meter, and levels should not exceed 75µ W/lumen. Lights should be turned off whenever possible. Storage areas should not have windows, but if they do they should be covered with curtains or blinds.

Insects and rodents once attracted to a records storage area may start eating the records, so:

- do not eat in storage areas
- keep surfaces (floors, tops of shelves) clean

Magnetic media are particularly vulnerable to irreversible damage if exposed to dust, heat and moisture; therefore storage areas should be fitted with special alarm systems. Use of these systems can provide much earlier warnings of fire or high dust levels than conventional detection systems and also minimize the need for large amounts of water to enter the storage area in the case of fire. The field of fire detection and suppression is a rapidly developing one and advice should be sought from the fire brigade to ensure that the best method is employed.

9. Maintenance

The information held on magnetic media can only be processed or read by mechanical means, therefore it is essential that equipment is maintained in good condition – poorly maintained equipment may actually cause damage as it processes or plays tapes and disks. The heads, disk drive and tape drive elements of playback and recording equipment should be cleaned on a regular basis according to manufacturers' recommendations.

Tapes should be exercised to improve their life span. Problems such as 'wrinkling' or 'cinching' of tape may build up in a tape pack as it sits in storage. Exercising can reduce the stresses, which cause these problems and may also reduce the danger of print-through.

Exercising involves winding the tape slowly through its entire length at playback speed, without stopping. The process should be carried out in the same environmental conditions in which the tapes are to be stored. Tapes which are to be moved to a different environment for exercising should be allowed a period of 24 hours to acclimatize to the new environment before exercising them. It is generally recommended that exercising be carried out at least every 3 years.

10. Reformatting and data migration

To minimize deterioration due to handling and use, copies of important and frequently used tapes should be made for reference purposes. Ideally, a preservation master copy, a duplicating copy and a reference copy should be produced, with the preservation master copy stored in a different location from other copies. The duplicating copy is used to produce further reference copies, when multiple copies are required. Labels should clearly indicate the status of the copy.

Long-term preservation of magnetic media is affected by two major factors: the intrinsic instability of the media and the likelihood of hardware used to read the media becoming unavailable. Even if tapes or disks made today are in excellent condition in 30 years time, the machines required to play them will almost certainly have been superseded long before. For all practical purposes the records will be unusable. Beta format videotapes are a good example of this problem. Once very common, they have now been entirely superseded by VHS format tapes and it will soon be very difficult to view a Beta video.

The main prospect for long-term retention of the information held on magnetic media seems to be in regular copying or data migration, thus maintaining a good quality signal which can be read using available equipment. Copying can either be to fresh tape or disk, or to some other machine-readable format such as CD-ROM.

Copying to analog tape will involve some loss of image quality at every copying stage. This may be significant after as few as 2 or 3 copies. This can be overcome by copying to a digital format such as digital tape (DAT for audiotapes) or optical disk. The tape used for digital recording is no more permanent than the tape used for analog recordings but the information can be copied many times without a significant loss of quality. Computer tapes are already recorded digitally so this problem does not arise.

Digital recording hardware is expensive. To minimize costs you can record initially on analog tape and then transfer to a digital medium for archiving. You should consider whether the information will need to remain on magnetic media permanently or whether a paper or microfilm format would be a better way of retaining the information. Paper-

based records and microfilm will always last longer than magnetic records stored in the same condition.

ANNEXURE G: Handling optical storage media

1. Types of optical disk

The term 'optical disk' is used to describe a range of disk types where the information is held in a form that is read optically, i.e. by a light source (usually laser) and photoelectric cell.

There are two main types of optical disk:

- **Compact Disks (CDs)** that consist of the following types:
  - **ROM disks** contain information that cannot be changed or added to by the user (ROM stands for 'read-only memory'). The best-known type of CD-ROM is the music compact disk, but they are also becoming popular as a replacement for print copies of large publications, such as encyclopaedias. CD-ROM disks are usually 12 cm in diameter, although other sizes have been used such as the 30 cm laser disks used for motion pictures.

  - **WORM disks** are also known as read-write optical disks (WORM stands for 'write once read many'). They are blank when sold, and allow the user to record information on them, which cannot be removed or changed. Recording onto the disks requires dedicated hardware. They can be read in CD-ROM disk drives. Executable CD-WORM disks are disks where the programme needed to access the content of the disk is recorded on the disk itself.

  - **Rewritable disks** – are a form of optical disk technology that allow the user to record information on a disk, erase it, and replace it with new data. They are used when information is being regularly revised, edited or updated. They are also used for short-term information as they can be wiped and reused when the information is no longer needed. As with WORM disks, recording on to rewritable disks requires dedicated hardware but once this is done they can be read in CD-ROM disk drives.

- **Digital Versatile Disks (DVDs)** which are basically a 2nd generation high density compact disks that also consist of ROM, WORM and Rewritable versions. DVD drivers are backward compatible to enable them to read CD's. The following types exist:
  - DVD video. These DVD's provide a format for showing full-length films using a special DVD player connected to a television set. DVD videos contain a scrambling system that prevents users from copying the contents.
  - DVD-ROM. These DVD's are read-only disks that also have enough storage capacity for a full-length feature film. They are accessed using a special DVD drive attached to a personal computer. Most of these drives are backward-compatible with CD-ROMs and can play DVD video disks.
  - DVD-RAM. These DVD's are rewritable disks with exceptional storage capacity of up to 2.6 GB per side, and come in one- or two-sided formats.
  - DVD+RW. DVD=RW is a direct competitor to DVD-RAM with similar functionality and slightly greater storage capacity.

2. Composition of optical disks

An optical disk has a number of layers. CD-ROMs have a stable polycarbonate plastic base. The polycarbonate base is pressed out from a master mould and holds its information as a series of tiny depressions. The base layer is then covered with a thin layer of metal (usually aluminium) to make it reflective. To protect the metallic layer the

whole disk is entirely sealed with a thin layer of clear polycarbonate. This laminar structure is the main source of many of the preservation problems that arise in optical disks.

WORM and rewritable disks share the same basic structure as a CD-ROM, but with extra layers to allow for the recording process. In the case of rewritable disks one of the additional layers is magnetic.

DVD's are formed by back to back bonding of two 0.6 mm thick 12 cm optical disks. They have four to five times the capacity of normal CD's.

3. Deterioration of optical disks

We cannot control the inevitable deterioration of materials, but we can control how fast it happens.

Certain materials are susceptible to deterioration in particular ways due to their properties, and other materials deteriorate as a result of particular environmental conditions. Optical disks are a very dense form of information storage, so even small amounts of degradation can lead to significant information loss.

Optical disks can be particularly prone to deterioration due to flaws arising in their manufacture, for example:

- Water or air trapped under the coating during moulding can lead to corrosion of the aluminium reflective layer.
- Rapid cooling of the plastic base or coating can result in cracks that also lead to dropout of information.
- Bonding between the different layers may be weak, leading to delamination.
- Inks used to print information on the outer surface may corrode the plastic.
- The polycarbonate plastic layer has a tendency to ‘flow’ over time. This means that the plastic layers may slowly lose their shape, eventually making it difficult for them to be processed by the machinery used to read them.
- Because they are read optically any marking that interferes with the light path, e.g. scratches or surface deposits, can cause reading problems such as skipping or repetition of tracks. Some deposits, such as fingerprints, may cause etching of the plastic surface and can lead to irreversible damage.

Improvements have been made in optical disk technology to address some of these problems. For example, some optical disks are now being produced with a gold metallic layer, which cannot corrode, rather than aluminium.

4. Handling and care of optical disks

- Handle with care.
- Lint-free cotton gloves should be worn to avoid scratching or other marking of the surface. If disks must be handled with bare hands then fingers should never be allowed to touch the reflective side of the disk.
- Disks should only be removed from their protective packaging for use and returned immediately after use.
- Food and drink should never be consumed where optical disks are in use.
- Disks should not be bent or flexed.
- WORM and Rewritable disks should not be left in direct light or sunlight as it causes the dye layer to fade and the disk to become unreadable.

If an optical disk becomes dusty, dirty or fingerprinted it may be possible to clean it

before permanent damage occurs, provided great care is exercised. Gently remove loose dust using a non-abrasive photographic lens tissue, or very soft brush. Oily dirt deposits and finger marks can be removed using a photographic lens cleaning solution and lens tissue. The lens cleaning solution should be applied sparingly to the disk surface and wiped off with the tissue. The cleaning motion should never be circular (along the tracks) – always brush from the centre of the disk outwards. If the cleaning process creates a scratch, it will do less damage cutting across the tracks rather than along them.

5. Protective packaging

Optical disks usually come with their own rigid plastic case, known as a jewel case. These cases are reasonably dustproof and are suitable for long-term storage as they are usually constructed of an inert plastic. Disks that do not have a jewel case should be individually enclosed in a sleeve, bag or envelope made of an inert plastic such as polyethylene, polypropylene or Tyvek.

CDs should not be stacked or packaged in groups so that they lean against each other, causing pressure build-ups, as this may lead to warping or deformation. Jewel cases are the ideal enclosure because they support each disk at the hub and deflect any impact from other items.

Disks should be labelled on their protective packaging rather than directly on the disks themselves. Inks from pens and markers may contain solvents that can damage the disk and graphite dust from pencils may interfere with reading of the disk.

6. Environment

Optical disks should be stored at temperatures between 18-20 ºC and relative humidities between 45 – 50 %. In these conditions the natural deterioration of the items can be slowed. In some instances deterioration can be slowed further by lower temperatures. It is important that these environmental levels are stable. Mould will start to grow around 60 % relative humidity and if the humidity fluctuates more than 10 % in 24 hours or the temperature is too high, the items in the collection will be stressed, speeding up their deterioration.

Materials degrade quicker when exposed to ultraviolet light. Fluorescent tubes that are low in ultraviolet light should be used wherever possible in storage areas. Ultraviolet light can be easily measured with a light meter, and levels should not exceed 75µ W/lumen. Lights should be turned off whenever possible. Storage areas should not have windows, but if they do they should be covered with curtains or blinds.

Insects and rodents once attracted to a records storage area may start eating the records, so:

- do not eat in storage areas
- keep surfaces (floors, tops of shelves) clean
- bait regularly for rodents and fumigate annually for insects.

Insect pest strips can be used as localized insect deterrents. However, the strips should not come into direct contact with individual items.

7. Maintenance of equipment

The information held on optical disks can only be processed or read by mechanical means, therefore it is essential that equipment is maintained in good condition – poorly

maintained equipment may actually cause damage as it processes. To ensure maximum equipment life and to minimize playback problems, optical disk equipment should only be operated in a low-dust environment. Equipment should also be regularly wiped over with a slightly damp cloth to avoid dust build-up. Other maintenance instructions provided by equipment manufacturers should be followed.

8. Reformatting and migration

Long-term preservation of optical disk media is always affected by two major factors: the instability of the media, and the likelihood of technological obsolescence. Even if optical disks made today are in excellent conditions in 30 years time, the machines required to play them may have been superseded. Predictions made about the life expectancy of optical disk media become irrelevant if equipment and software is not available to ensure that information is accessible.

The main prospect for long-term retention of information on optical disks seems to be in regular copying or data migration. This entails copying the information on the disk to a fresh WORM or rewritable disk or to another format such as digital tape (or other new technology formats that may be developed). If this is done regularly then the information should survive indefinitely.

ANNEXURE H: Example of an inventory/catalogue for electronic records systems

NAME OF SYSTEM	PURPOSE OF SYSTEM	FUNCTIONS
LOGISTICS Contact person: Sipho Mokoena	Control and monitor the issuing of consumable state property.	• Monitor consumption figures per accoun-ting officer • Calculate stock on hand • Etc.
PERSAL Contact person: Seipati Ncgobo	To keep a record of the personal information of all personnel employed by the department and to administer all expenses i.r.o. salaries. All state departments use the system.	Maintenance, reports and enquiries i.r.o the following: ID number; Surname; Initials First Names; Date of Birth; Race; Gender; Disability; Citizenship; Date of Citizenship; Nationality; Residential Address; Etc.
PERMIT APPLICATIONS REGISTRATION SYSTEM Contact person: Tumi Mokaba	To keep a register and track of all applications for permits	• Allocates application numbers • Issue acknowledge-ment of receipt • Track status of application • Issue permits • Gather management statistics • Etc.

ANNEXURE I: Characteristics of an authentic records

According to SANS 15489: *Information and documentation – Records management – Part 1: General* the implementation of records management policies, procedures and practices should lead to the creation, management and presentation of authoritative records that are trustworthy and reliable evidence of actions while conducting official business.[63] The Electronic Communications and Transactions Act supports the view that the trustworthiness of records determines their evidential weight in legal proceedings.[64]

The following are the characteristics of an authentic record:

- **Authenticity**

An authentic record is one that can be proven
a) to be what it purports to be,
b) to have been created or sent by the person purported to have created or sent it, and
c) to have been created or sent at the time purported.

To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment.

- **Reliability**

A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

- **Integrity**

The integrity of a record refers to its being complete and unaltered.

It is necessary that a record be protected against unauthorized alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

- **Usability**

A useable record is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of

63 SANS 15489 - *Information and documentation – Records Management – Part 1: General*, p.8
64 Mostert, W. *Legal Considerations for Document Imaging*. Pamphlet issued by Mostert, Opperman, Goodburn Incorporated

activities should be maintained.

ANNEXURE J: Guidelines for the development of a e-mail management policy and example of an e-mail management policy

A: GUIDELINES FOR THE DEVELOPMENT OF AN E-MAIL MANAGEMENT POLICY

A1. INTRODUCTION

A governmental body keeps records to support its operations, as well as to fulfil legal and other obligations.

It is essential for each body to establish its own e-mail management policy to link its unique processes and procedures to the requirements of the National Archives and Records Service of South Africa Act, 1996. The policy should not only be in line with the Act, but should also link up with the body's overall mandate and mission objectives. The e-mail management policy provides the framework within which a governmental body affirms its commitment to create authentic and reliable records. It also ensures that the management of e-mail is not detached from the management of records in all formats regardless of from or medium.

Managing e-mail records poses particular challenges because many of the problems experienced are technological in nature. E-mail systems are not designed to manage, store and preserve records. If governmental bodies do not put specific policies in place to mange user behaviour to ensure that e-mailed records are captured, stored and preserved, records that are critical for business continuity could be lost.

These guidelines are issued in terms of section 13(4) of the National Archives and Records Service of South Africa Act, 1996. The purpose of these guidelines is to enable records managers to compile their own e-mail management policy using the guidelines as a basis to work from.

A2. PLANNING THE POLICY

A governmental body cannot draft an e-mail management policy if it does not know what the specific record keeping and service delivery requirements are. To enable a governmental body to draft a policy that suits the business needs of the specific body, it is advisable that a thorough analysis be done of the environment within which the body operates.

A full and proper understanding of a body's current business and records management operations is of utmost importance to gain insight into the risk involved in not managing records and information properly, as well as the risk of not being accountable for service delivery. The National Archives and Records Service supports the view expressed in SANS 15489: *Information and documentation – Records Management – Part 2: Guidelines* that an understanding of the environment the governmental body operates in, is core to the successful implementation of any record keeping system and records management programme. It is essential that governmental bodies take note of the recommendations in par 8.2 of this document

A3. STRUCTURING AN E-MAIL MANAGEMENT POLICY

The policy document should be clear and concise. All information in the policy should be relevant. Procedures should not be documented in the policy, but should be cross-referenced.

The policy should be
- flexible;
- implementable; and
- cost effective.

The following elements should be addressed in the policy:

A3.1 Policy statement

The policy should
- emphasize that all records created or received during the execution of an body's functions (including electronic records, e.g. e-mail) are public records and that these records must be managed in accordance with the determined policy guidelines;
- stipulate that public records must be classified and stored so that they are easily accessible, thereby facilitating transparency, accountability and democracy.

Note: It is crucial that the policy statement is clear and precise. All staff should be able to understand the purpose of the policy.

A3.2 Relationship with other policies

Describe the relationship with other policies e.g.
- Official e-mail system use policy;
- Records management policy;
- Electronic records management policy;
- Internet policy;
- Information security policy, etc.

A3.3 Scope and intended audience

Policy should give clear indication to the users as to which types of e-mails should be considered to be part of the official records of the body.

Policy should describe the intended audience and target group of the policy.

Note: A policy should not consist of quotations from published source material and standards. It should talk to the audience about the issues at hand.

A3.4 Statutory and regulatory framework

List all the relevant laws and regulations that impact on records creation and records management practices.

A3.5 Roles and responsibilities

A3.5.1 Top and senior management

Define the responsibilities of top and senior management regarding e-mail record keeping and record management.

A3.5.2 Records manager

Describe
- who the records/information manager is and define the records manager's area of responsibility with regards to e-mail management; and
- who the sub-records/information managers are as well as their areas of responsibility

A3.5.3 IT manager

The policy should clearly define the IT manager's area of responsibility.

A3.5.4 Other roles and responsibilities

All other roles that are involved with records creation, record keeping and records management should be identified and defined. This is specific to each office and may include
- users
- registry staff, etc.

A3.6 Filing e-mails as records

Policy should indicate that e-mails should be filed to the official record keeping system and should indicate who is responsible for filing the e-mails.

A3.7 Disposal of e-mails

Policy should clearly indicate that no official record shall be disposed of without a written disposal authority being issued for its disposal. It should also contain information with regards to
- which disposal authorities exist and where to obtain them;
- how staff should deal with e-mails that are not covered by disposal authorities.

A3.8 Creating reliable e-mail records

Policy should address the creation of reliable e-mail records by giving direction regarding the following:
- how outgoing e-mail should be structured;
- the use of subject lines;
- the use of auto-signatures;
- how attachments should be managed;
- the use of official language;
- capturing e-mail strings; and
- when to capture e-mails as records.

A3.9 Metadata

Policy should address which metadata to capture to create reliable e-mail records.

A3.10 Monitor and review

Policy should indicate how often the e-mail record keeping and records management practices should be monitored and who is responsible for this task.

A4. IMPLEMENTING THE POLICY

The top and senior management should support the policy and should issue a commitment statement in this regard.

Top and senior management should lead by example. If they manage their own office's e-mail properly, the staff would more readily buy into the concept.

Top management should also ensure that the records management function is sufficiently resourced to facilitate that effective record keeping becomes a normal administrative practice.

The policy should be disseminated and communicated to the staff. It is recommended that, besides providing staff with copies of the policy document, the records manager should launch a records management awareness campaign to inform all the staff of their responsibilities.

A5. MONITOR AND REVIEW THE POLICY

Once implemented it is necessary to monitor staff compliance to the policy. The staff's awareness and understanding of the policy should be monitored by doing spot checks on their e-mail record keeping and records management behavior so that timely interventions can be made.

The policy itself should be reviewed regularly to ensure that it continuously meets the business and service delivery needs of the body.

A6. INPUT BY NATIONAL ARCHIVES AND RECORDS SERVICE

The National Archives and Records Service encourages governmental bodies to submit their record keeping and records management policies to the National Archives and Records Service to review it to ensure that it is aligned with the requirements of the National Archives and Records Service Act.

Due to the nature of the records created and received by governmental bodies it is advisable that the e-mail policy should be part of a set of records management policies rather than one comprehensive and cumbersome document. Although this example does not contain the full set, it is recommended that the policy should at least consist of the following parts.

Part 1: General record keeping and records management.
This part would contain the:
- general principles according to which records are managed
- paper-based specific policies.

Part 2: Electronic records management policy.
This part would contain the general electronic records management

principles.

Part 2a: E-mail policy.
This part would contain the specific records management policy for e-mail management.

Part 2b: Web content management policy.
This part would contain the specific records management policy regarding web content management.

Part 2c: Document imaging policy.
This part would contain the specific records management policy regarding the imaging of records to guarantee their evidential weight in legal proceedings.

The information security policy could also be considered to be part of the set of records management policies because information security and records management are closely related.

Governmental bodies should decide whether the official e-mail system use policy should be included as part of the e-mail management policy or not.

B. EXAMPLE OF AN E-MAIL MANAGEMENT POLICY

The attached policy is only an example to guide governmental bodies regarding the formulation of the policy. It is generic in nature and governmental bodies should not consider it sufficient to replace the need for a proper investigation into the unique business requirements, and record keeping and records management practices of a governmental body. When drafting a policy, governmental bodies should ensure that the National Archives and Records Services records management requirements are integrated with their own business requirements and administrative practices.

E-MAIL MANAGEMENT POLICY FOR [NAME OF GOVERNMENTAL BODY]

Version [?] of [date]

Second Edition
April 2006

Content

E-Mail Policy for [name of governmental body]

1. Purpose

1.1 The National Archives and Records Service Act applies to e-mail in the same way as it does to records that are created using any other media.

1.2 All public servants are required to create and preserve records of the (name of governmental body's) organization, functions, policies, decisions, procedures and transactions. The records must be properly stored, preserved and available for access.

1.3 The purpose of this policy is to facilitate the proper creation, management, preservation and disposal of e-mail records.

1.4 All employees of (name of governmental body) shall implement the e-mail policy.

2. Policy statement

2.1 All records created and received by [name of governmental body] shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 1996.

2.2 The following broad principles apply to the record keeping and records management practices of [name of governmental body]:

- The [name of governmental body] follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
- The records management procedures of [name of governmental body] comply with legal requirements, including those for the provision of evidence.
- The [name of governmental body] follows sound procedures for the security, privacy and confidentiality of its records.
- Electronic records in the [name of governmental body] are managed according to the principles promoted by the National Archives and Records Service.
- The [name of governmental body] has performance measures for all records management functions and reviews compliance with these measures.

3. Relationship with other policies

3.1 The [name of governmental body]'s, e-mail management policy are related to the

- Official e-mail system use policy;
- Records management policy;
- Electronic records management policy; and
- Web content management policy
- Document imaging policy.

3.2 Other policies that are closely related to the e-mail management policy are

- the information security policy that is managed by the security manger;
- the internet usage policy that is managed by the IT manger; and the
- the promotion of access to information policy that is managed by the Chief Information Officer.

[Note: These are only examples. Governmental bodies should list the policies that

pertain to the records and information management practices in their particular environment.]

4. Scope and intended audience

4.1 Applicability to employees

4.1.1 This policy applies to all staff of (name of governmental body) who generate records while executing their official duties.

4.1.2 Employees of (name of governmental body) should be aware that e-mails are subject to Promotion of Access to Information (PAIA) requests and legal discovery when a lawsuit is pending. Should e-mails that are a subject of a PAIA request or legal discovery be deleted because e-mails are not managed properly (name of governmental body) will face severe court sanctions and/or a criminal charge.

4.1.3 Employees who willfully contravenes the e-mail management provisions in this policy will face disciplinary action.

4.2. Applicability to e-mails as records

4.2.1 E-mails that are evidence of the business transactions of (name of governmental body) are public records and shall be managed and kept for as long as they are required for functional and/or historical purposes.

4.2.2 E-mails that approve an action, authorize an action, contain guidance, advice or direction, relate to projects and activities being undertaken, and external stakeholders, represent formal business communication between staff, contain policy decisions, etc. should be managed as records and should be filed into the file plan. This policy covers the e-mail message itself as well as any attachments that meet these criteria.

4.2.3 An e-mail message is a record if it:

- contains unique, valuable information developed in preparing position papers, reports, studies, etc.
- reflects significant actions taken in the course of conducting business.
- conveys unique, valuable information about (name of governmental body)'s programs, policies, decisions, or essential actions.
- conveys statements of policy or the rationale for decisions or actions.
- documents oral exchanges (in person or by telephone), during which policy is formulated or other business activities are planned or transacted.
- adds to the proper understanding of the formulation or execution of (name of governmental body)'s actions or of (name of governmental body)'s operations and responsibilities.
- documents important meetings.
- facilitates action by (name of governmental body)'s officials and their successors in office.
- makes possible a proper scrutiny by the Auditor-General or other duly authorized agents of the government.
- protects the financial, legal, and other rights of the (name of governmental body) and of the persons directly affected by the (name of governmental body)'s actions.
- approves or authorizes actions or expenditure.
- constitutes a formal communication between staff e.g. correspondence or memoranda relating to official business.
- signifies a policy change or development.

- creates a precedent e.g. by issuing an instruction or advice.
- involves negotiations on behalf of the (name of governmental body).
- has value for other people or the (name of governmental body) as a whole.

4.2.4 E-mails that contain the following do not need to be filed:

- meeting announcements.
- announcements of employees' absences or schedules.
- changes in telephone numbers or office locations.
- meeting arrangements that normally would have been done by telephone.
- copies of memoranda or text sent for information rather than action.
- messages that have only temporary value such as a message that a meeting time has changed.
- messages that contain no evidence of (name of governmental body)'s functions and activities.
- duplicate information already documented in existing records.

5. Regulatory framework

5.1 By managing its e-mailed records effectively and efficiently [name of governmental body] strives to give effect to the actability, transparency and service delivery values contained in the legal framework established by:

- Constitution, 1996;
- National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended);
  - o National Archives and Records Service of South Africa Regulations;
- Public Finance Management Act (Act No 1 of 1999);
- Promotion of Access to Information Act (Act No 2 of 2000);
- Promotion of Administrative Justice Act (Act No 3 of 2000);
- Electronic Communications and Transactions Act (Act No 25 of 2002).

[Note: Governmental bodies should list all other acts, regulations and codes of practices that impact on the record keeping and records management practices of the body.]

6. Roles and responsibilities

6.1 Top management

6.1.1 Top management is responsible for the approval of this policy and for the designation of a senior manager as the records manager. Top management shall mandate the records manager to implement this policy.

6.1.2 Top management shall ensure that the management of records including e-mail is a key responsibility in the performance contracts of all senior managers.

6.2 Senior manager

6.2.1 Senior managers are responsible for the implementation of this policy in their respective units. They shall ensure that the management of records including e-mail is a key responsibility in the performance agreements of all the staff in their units.

6.2.2 Senior managers shall lead by example and shall ensure that records, including e-mail generated by them are managed properly.

6.3 Records manager

6.3.1 The records manager is responsible for:
- the implementation of this policy;
- staff awareness regarding this policy.

6.3.2 The records manager is responsible for ensuring that e-mails are managed as records according to the records management principles prescribed by the National Archives and Records Service Act and in terms of this policy. In this regard the records manager shall be consulted to determine which types of e-mail would be considered official records that should be managed properly, if the specific types are not covered in par. 3 above.

6.3.3 The records manager shall ensure that all records created and received by [name of governmental body] are classified according to the approved file plan and that a written disposal authority is obtained for them from the National Archives and Records Service.

6.3.4 The records manager is responsible for determining retention periods in consultation with the risk manager, the legal services manager and the users and taking into account the functional, legal and historical need of the body to maintain records of transactions.

6.3.5 The records manager is mandated to make such training and other interventions as are necessary to ensure that the [name of governmental body]'s record keeping and records management practices comply with the records management principles contained in the National Archives and Records Service Act.

6.3.6 The records manager may from time to time issue circulars and instructions regarding the record keeping and records management practices of [name of governmental body].

6.3.7 The specific duties of the records manager with regards to the management of e-mail as records are contained in the Records Manager's job description which is published on the intranet [give URL]/filed on file [give file number from the governmental body's file plan].

[Note: Governmental bodies should adapt this as is appropriate for their specific circumstances.]

6.3.8 The [post designation] is the records manager for the whole [name of governmental body].

[Note: If a governmental body has sub-records managers, each sub-records manager's area of responsibility should be defined.]

6.3.9 The records manager shall monitor the implementation of this policy.

6.4 Chief Information Officer

6.4.1 The Chief Information Officer is responsible for approval of requests for information in terms of the Promotion of Access to Information Act.

6.4.2 The Chief Information Officer shall inform the records manager if a request for information necessitates a disposal hold to be placed on records that are due for disposal.

6.5 IT manager

6.5.1 The IT Manager is a sub records manager and he/she is responsible for the day-to-day maintenance of electronic systems that stores records including the (hardware/software) that serves as the conduit for receiving and transmitting e-mail.

6.5.2 The IT manager shall work in conjunction with the records manager to ensure that public records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes.

6.5.3 The IT manager shall ensure that no e-mails are deleted from any system without consulting the records manager.

6.5.4 The IT manager shall ensure that the integrity of any records housed in the e-mail is protected until they have reached their approved retention. Integrity of these record will be accomplished through such procedures as test restores, media testing and data migration and capturing the required audit trails.

6.5.5 The IT manager shall ensure that appropriate systems technical manuals and systems procedures manuals are designed for each electronic system that manages and stores records.

6.5.6 The IT manager shall ensure that all electronic systems capture appropriate systems generated metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created.

6.5.7 The IT manager shall ensure that electronic records in all electronic systems remains accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.

6.5.8 The IT manager shall ensure that all data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.

6.5.9 The IT manager shall ensure that the back-up files for the e-mail system are recognized as being part of the overall records management system in that the subject classification scheme shall be evident if files need to be retrieved from the backups.

6.5.10 The IT manager shall ensure that back-ups are stored in a secure off-site environment.

6.5.11 The IT manager shall ensure that systems that manage and store records are virus free.

6.5.12 Further comprehensive details regarding specific responsibilities of the IT manager are contained in:

- the electronic records management policy;
- the e-mail policy;
- the web content management policy;
- document imaging policy; and the
- information security policy.

[Note: If a governmental body does not have separate policies, the detailed requirements should be included in this document]

6.6 Security manager

6.6.1 The security manager is responsible for the physical security of all records.

6.6.2 Details regarding the specific responsibilities of the security manager are contained in the Information Security Policy.

6.7 Legal services manager

6.7.1 The legal services manager is responsible for keeping the records manager updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of [name of governmental body].

6.8 Staff

6.8.1 Every user of the official e-mail system is responsible for ensuring that e-mails, that are evidence of business transactions, are captured as records.

6.8.2 Every user of the official e-mail system is responsible for ensuring that e-mails a subject classified against the approved file plan.

7. Filing e-mails

7.1 E-mails shall under no circumstances be isolated from (name of governmental body)'s records management systems. They shall be captured into the file plan contained in the Integrated Document and Records Management System.[65] E-mails and attachments shall be captured as separate but linked records.

7.2 If an e-mail impacts on the work of a user and it complies with the criteria stated in par. 3, the e-mail shall be filed by the sender except if:

- there is a person in a unit or project group to whom the responsibility for this task has been designated.
- it is an e-mail received from outside the (name of governmental body) in which case the recipient is responsible for filing it.

8. Disposing of e-mails

8.1 E-mails considered to be public records shall not be deleted or otherwise disposed

---

65 a) State the proper name of the system as it is used in the body.
b) Other options that could be used if a body does not have an Integrated Document and Records Management System are:
- Print the message, and any applicable attachments, to paper and incorporate into the body's paper records management system; or
- Save the message and/or its attachment(s) in a directory outside the e-mail system, which is a part of the body's official records system (e.g., a word processing directory on a local area network directory); or
- Transmit the message electronically to a central records repository, or other appointed representative, for incorporation into the body's records management system.

Governmental bodies need to ensure that the rest of the policy is adapted accordingly when one of the other options apply.
c) Where policy requires e-mails to be retained in paper-based format, they should be filed to the paper-based file plan in the registry E.g. security classified records and other instances identified by legal advisors and risk management. If no such cases exist in the organisation, leave this part out.

of without a written disposal authority issued by the National Archivist.

8.2 E-mails filed to subject files in the file plan are covered by Standing Disposal Authority No (insert number issued by the National Archives and Records Service) and shall be disposed of according to the retention periods in that disposal authority.

8.3 Should an e-mail be received/generated for which an appropriate subject file does not exist in the file plan, the records manager should be contacted to add an appropriate subject to the file plan and to apply for disposal authority on that subject.

8.3 E-mails that are not public records may be disposed of after (governmental body should decide how long) months in terms of the National Archives and Records Service's General Disposal Authority AT2 for the Destruction of Transitory Records.

9. Creating reliable e-mail records

9.1 Structuring an out-going e-mail

9.1.1 E-mails that are public records shall contain sufficient information to ensure that they are properly contextualized and that they are meaningful and accessible over time.

9.1.2 Outgoing mail shall include the reference number of the subject folder in the file plan in the top right hand corner of the message box to provide a contextual link to the business activity that supports the e-mail.

9.2 Proper subject line

9.2.1 Subject lines are very important, since they indicate to a recipient what the message is all about. If subject lines are not used appropriately, the recipients may not realize the importance of the message and choose to read it later or not at all. Users shall allocate useful subject lines to e-mails.

9.2.2 If a user receives a message with a senseless subject line and needs to reply to or forward it, the subject line should be changed to properly cover the subject of the e-mail before sending it off.

9.3 Auto-signatures

9.3.1 Staff should always be contactable even if their e-mail systems are down. Auto-signatures shall be used and shall contain the following identifying information of a sender:

- name of sender
- position of sender
- name of unit/section
- name of the governmental body
- postal address
- phone number
- fax number

9.4 Attachments

9.4.1 If an outgoing mail includes an attachment, the attachment shall be filed into the

file plan in the Integrated Document and Records Management System before it is attached to the e-mail to ensure that it contains the following prescribed minimum mandatory metadata.

- File plan reference number
- Record title: A sensible name given to it by the user
- Author
- Originating organization
- Originating sub office
- Record date
- Record type

[Note: If he office does not have an Integrated Document and Records Management System, the word processing application should be set up to capture this.]

9.4.2 Attachments shall be virus free.

10. Language used in e-mails

10.1 Official communications shall be approached in the same manner as a business letter, thinking it through carefully and using proper grammar and correct spelling.

11. Capturing e-mail string

11.1 E-mail messages on a particular subject can become a string of replies until a matter is finalized. In such cases users shall:

- place all e-mails into the system separately as they occur and relate them to each other or
- capture the final message – in which case user needs to make sure that the final message contains whole thread of the discussion.

12. When to capture e-mails

12.1 Users shall capture official e-mails at the time of the action to ensure that

- the chronological order of the business transaction is clear.
- the authenticity of e-mail is guaranteed.

13. Metadata

13.1 The IT manager shall ensure that the system is set up to capture the following metadata:

- The transmission data that identifies the sender and the recipient(s) and the date and time the message was sent and/or received;
- When e-mail is sent to a distribution list, information identifying all parties on the list must be retained for as long as the message is retained.

14. Monitor and review

14.1 The records manager shall review the e-mail record keeping and records management practices of [name of governmental body] on a regular basis and shall adapt them appropriately to ensure that they meet the business and service delivery requirements of [name of governmental body].

14.2 This policy shall be reviewed on a regular basis and shall be adapted

appropriately to ensure that it meets the business and service delivery requirements of [name of governmental body].

15. Definitions

Correspondence system:

A set of paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.

Disposal:

The action of either destroying/deleting a record or transferring it into archival custody.

Disposal authority:

A written authority issued by the National Archivist specifying which records should be transferred into archival custody or specifying which records should be destroyed/deleted or otherwise disposed of.

Disposal authority number:

A unique number identifying each disposal authority issued to a specific office.

Electronic records:

Information which is generated electronically and stored by means of computer technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

Electronic records system:

This is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and meta data (background and technical information i.r.o. the information stored electronically) and in hard copy. All these components are defined as records by the Act. They must therefore be dealt with in accordance with the Act's provisions.

File plan:

A pre-determined classification plan by which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.

Public record:

A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

Record:

1) Recorded information regardless of form or medium.

2) Evidence of a transaction, preserved for the evidential information it contains.

Record keeping:

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

Records management

Records management is a process of ensuring the proper creation, maintenance, use and disposal of records throughout their life cycle to achieve efficient, transparent and accountable governance.

Retention period:

The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.

System technical manual:

A manual containing information regarding the hardware, software and network elements that comprise the system and how they interact. Details of all changes to a system should also be documented.

System procedures manual:

A manual containing all procedures relating to the operation and use of the electronic system, including input to, operation of and output from the system. A system procedures manual would contain detailed procedures regarding -

- Document capture
- Document scanning
- Data capture
- Indexing
- Authenticated output procedures
- File transmission
- Information retention
- Information destruction
- Backup and system recovery
- System maintenance
- Security and protection
- Use of contracted services
- Workflow
- Date and time stamps
- Version control
- Maintenance of documentation

A systems procedures manual should be updated when new releases force new procedures.

16. References

National Archives and Records Service: *Records Management Policy Manual*, April 2006.

National Archives and Records Service: Managing electronic records in governmental

bodies: Policy, principles and requirements, April 2006.

National Archives and Records Service: Performance criteria for records managers in governmental bodies, April 2006.

National Intelligence Agency: Minimum Information Security Standard.

South African Bureau for Standards: SANS 15489: Information and documentation – Records management – Part 1: General.

South African Bureau for Standards: SANS 15489 Information and documentation – Records management – Part 2: Guidelines.

South African Bureau for Standards: SANS 15801: Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability.

South African Bureau for Standards: SANS 23081: Information and documentation – Records Management processes – Metadata for records – Part 1: Principles.

South African Bureau for Standards: SANS 17799: Information Technology – Security techniques - Code of Practice for Information Security Management.

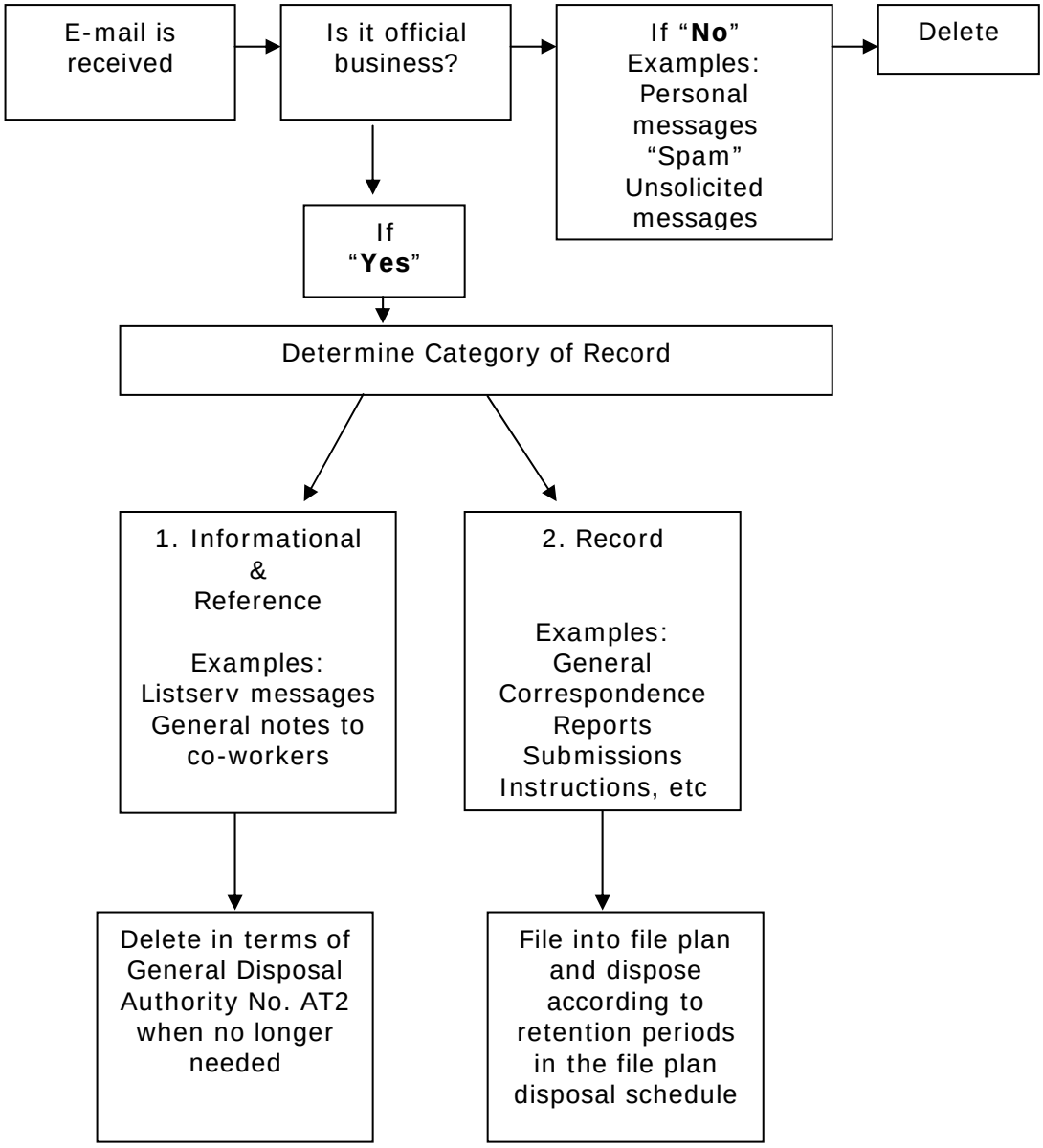
14. Authorization

This policy was approved by [post designation of head of governmental body] on [date].

HEAD OF DEPARTMENT

ANNEXURE K: Examples of a decision sequence for determining e-mail retention

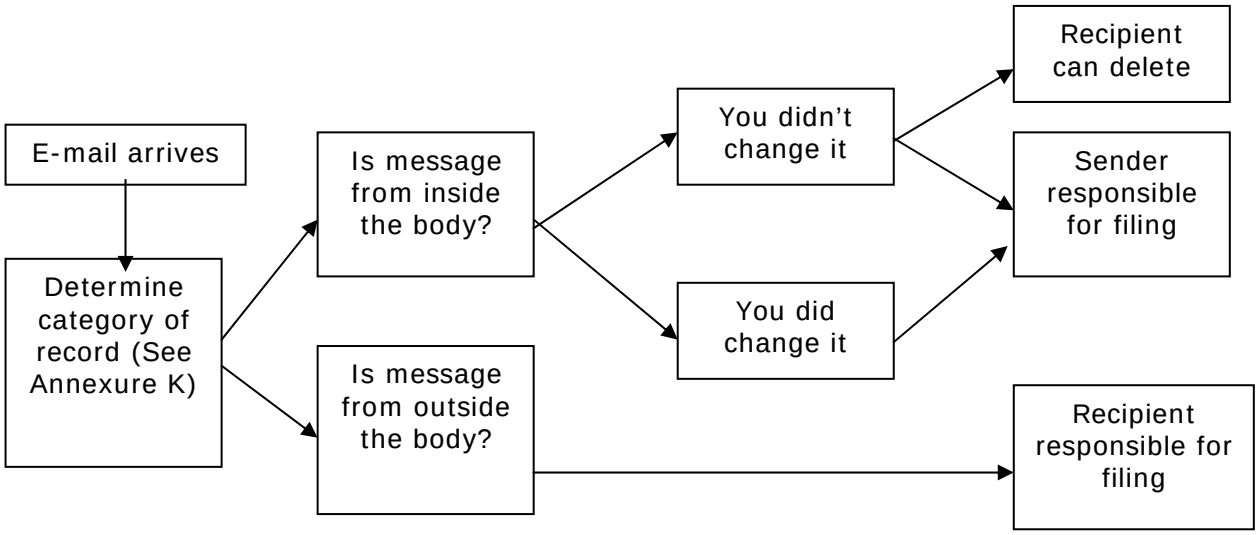
The volume of e-mail received complicates its management. Users need clear guidelines as to which e-mails should be filed as records and which not.[66]



66 These guidelines were adapted from the *Guidelines for Managing E-mail in Kentucky Government* [http://www.kdla.ky.gov/recmanagement/E-mailGuidelines.htm]

ANNEXURE L: Example of a decision sequence for determining responsibility for retaining e-mail messages

Because e-mail messages can be forwarded and routed to multiple addresses, copies of the messages may exist in many areas of the body. In most cases, the author, or originator, of the e-mail message is responsible for maintaining the "record" copy. However, in cases in which the recipient has altered the message (made changes, added attachments, etc.), or when the message comes from outside the body (and therefore not documented anywhere within the body), the recipient is the one responsible for retaining the message. [67]



67 These guidelines were adapted from the *Guidelines for Managing E-mail in Kentucky Government* [http://www.kdla.ky.gov/recmanagement/E-mailGuidelines.htm].

ANNEXURE M: Glossary

Act
The National Archives and Records Service of South Africa Act (Act No. 43 of 1996 as amended).

Appraisal
The process of determining the value and thus the final disposal of records, and the decision regarding the preservation requirements of each record or series of records.

Archival custody
The control of records by an archival institution, based on the physical custody of the records.

Archival value
Those values, administrative, fiscal, legal, evidential and/or informational, which justify the indefinite or permanent retention of records.

Archive
a) A feature of document management systems, in which infrequently accessed documents are moved to off-line or near-line storage; or
b) A copy of data on disks, CD-ROM, magnetic tapes, etc., for long term storage and later access; or
c) The building in which archival records are stored; or
d) A group of records belonging to a specific governmental body.

Archives
Records in the custody of an archives repository.

Archives Repository
The building in which records with archival value, are preserved permanently.

Archiving
Creating a backup copy of computer files, especially for long-term storage.

Audit trail
An electronic means of auditing the interactions with records within an electronic system so that any access to the system can be documented as it occurs for identifying unauthorized actions in relation to the records, e.g. modification, deletion, or addition.

Authentic records
Authentic records are records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.

Authoritative records
Authoritative records are records that are authentic, reliable, trustworthy and useable and are complete and unaltered.

CD-Rewritable/ DVD-Rewritable
A compact disk that can be erased and re-recorded.

CD-WORM/DVD-WORM

Write once compact disks. Information written to a WORM disk cannot be changed. (See also executable CD-WORM disk)

Context
The background information that helps to explain the meaning of the document. This includes information that identifies the particular document, such as the title, author and date of creation and information about the creator and the purpose of creation, for instance, the nature of the function, the creating body and the unit concerned.

Current records
Records that form part of a records classification system still in use.

Custody
The control of records based upon their physical possession.

Digital preservation
The process and activities which stabilize and protect reformatted and digital authentic electronic records in forms which are retrievable, readable, and usable over time.

Disposal
This is the action taken when a body transfers archival records to an archives repository or records centre and destroys/deletes non-archival records.

Disposal authority
A written authorization specifying records to be transferred into the custody of the National Archives and Records Service or specifying records to be otherwise disposed of.

Disposal symbols/instructions
Also known as disposal instructions. Symbols indicating the type of action that should be taken with records. Two symbols (with certain variations thereof) can be found, namely A and D. A refers to the transfer of archival records to an appropriate archives repository for permanent preservation, usually twenty years after creation, or at such time as specified by the National Archivist. D refers to records with no archival value that need not be transferred to the National Archives and Records Service.

Electronic document management system
A computerised environment which enables the creation, capture, organisation, storage, retrieval, manipulation and controlled circulation of documents regardless of specific format.

Electronic mail
A general term covering the electronic transmission, or distribution, of messages. Also called e-mail.

Electronic records
Any information generated electronically and stored by means of computer technology.

Electronic records system
This is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and meta data (background and technical information i.r.o. the information stored electronically) and in hard copy. All these components are defined as records by the Act. They must therefore be dealt with in accordance with the Act's provisions.

Electronic records management system
A (normally out-of –the –box) electronic system that contains business rules to manage

records to ensure that they are authentic and reliable. A.k.a Electronic Records Management Applications.
A.k.a Records Management Applications

Enterprise Content Management (ECM)
A collection of technologies with specified required functionality to support the enterprise wide management of the information content of records

Ephemeral
Records with no archival value, which may be deleted after disposal authority has been obtained from the National Archivist.

Executable CD-WORM
Executable CD-WORM disks are disks in which the programme needed to access the content of the disk is recorded on the disk itself.

File plan
A pre-determined classification plan by which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.

Filing system
The collective noun for a storage system (like files, boxes, shelves or electronic applications and storage systems) in which records are stored in a systematic manner according to a file plan.

Functional Subject File Plan
A pre-determined logical, systematic and hierarchical structure based on business' functions that are then used to determine subject groups and subjects according to which records are filed and/or electronically indexed so as to facilitate efficient retrieval and disposal of records.

Format
The shape, size, style and general makeup of a particular record.

Governmental body
Any legislative, executive, judicial or administrative organ of state (including a statutory body) at the national level of government and, until provincial archival legislation takes effect, also all provincial administrations and authorities.

Head of a governmental body
The chief executive officer of a governmental body or the person who is acting as such.

Input
Data to be entered into a computer for processing.

Integrated Document and Records Management System

A system that supports the medium to long term information needs of an office. It provides functionality over and above that of an electronic document management system to preserve the security, authenticity and integrity of records to enable the permanent preservation of records. Its primary management functions are –

- to manage a functional subject file plan to which records are filed;
- maintaining the relationships between records and files, and between file series and the file plan;
- identifying records that are due for disposal an managing the disposal process;
- associating the contextual and structural data within a document;

- constructing and managing audit trails;
- managing record version control;
- manages the integrity and reliability of records once they have been declared as such;
- managing records in all formats in and integrated manner.

Local area network
A computer network located within a relatively limited area such as a building. Also known as a LAN.

LAN
See Local area network.

Media obsolescence
When storage media is superseded by newer media and the means to read the superseded media no longer exist.

Medium
The physical form of recorded information. Includes paper, film, disk, magnetic tape, and other materials on which information can be created.

Metadata
Background and technical information i.r.o. the information stored electronically.

Metadata schema
A semantic and structural definition of the metadata used to describe record keeping entities. A schema describes the names of metadata elements, how they are structured, their meaning, etc.

Network-attached storage
Devices that plug into the network and appear on the network as storage locations or storage servers for example CD/DVD-ROM towers (juke boxes), etc.

Open source software
Software that is developed, tested, or improved through public collaboration and distributed with the idea that it must be shared with others, ensuring open future collaboration.

Output
Information transmitted from internal to external units of a computer, or to an external medium.

Platform
The underlying software used by a system and the hardware making up the computer.

Preservation metadata
Metadata that supports and document the long-term preservation of digital materials.

Public records
A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

Record
i Recorded information regardless of form (paper, for instance, is used in the form of correspondence files, maps, plans, registers, etc.) or medium (for instance paper, microfilm or electronic media).

ii Evidence of a transaction, preserved for the evidential information it contains.
iii Electronic objects and their concomitant metadata which defines them as records.

Record classification system
A plan for the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in the classification system.

Records control schedule
This is the instrument to control records other than correspondence files, according to which such items are identified, retrieved and disposed of.

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

Records other than correspondence files
Records that do not form part of a correspondence of an office, e.g. minutes, registers, microfilms, electronic records, etc.

Record system
A collection of policies procedures and systems, which capture information according to a records classification system, manage, store and provide access to records and their context over time. A.k.a record keeping system.

Refreshing
Periodically moving records from one storage medium to another of the same kind.

Regulations
The National Archives and Records Service of South Africa Regulations, 2002, Regulation R158 published in the Government Gazette, No 24085 of 20 November 2002.

Repository for electronic records
A direct access device on which the electronic records and metadata is stored.

Retention periods
a) The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.
b) In an electronic document management system, the length of time a record is kept online before it is moved to near-line or off-line storage.

Smart Enterprise Suite
Smart enterprise suite is an integrated suite made up of search, classification, content-management, collaboration, knowledge-management, and process-management components.

Storage area network
A separate, dedicated, high performance, centrally managed, secure network, which moves data between servers and storage systems.

Structure
This relates to both the appearance and arrangement of the content (for example, the layout, fonts, page and paragraph breaks, tables, graphs, charts, etc.) and the relationship of the records to other related records in the system. This includes structural information about the application software used to create the record's content and

information about the system (the platform, hardware, etc.) that manages the links between records.

System technical manual
A manual containing information regarding the hardware, software and network elements that comprise the system and how they interact. Details of all changes to a system should also be documented, as well as details of new releases that were implemented.

System procedures manual
A manual containing all procedures relating to the operation and use of the system, including input to, operation of and output from the system. A system procedures manual would contain detailed procedures regarding:

- document capture,
- document scanning,
- data capture,
- indexing,
- authenticated output procedures,
- file transmission,
- information retention,
- information destruction,
- backup and system recovery,
- system maintenance,
- security and protection,
- use of contracted services,
- workflow,
- date and time stamps,
- version control,
- maintenance of documentation.

A systems procedures manual should be updated when new releases force new procedures.

Technology obsolescence
When current hardware and software are superseded by new technology that are not necessarily compatible with the older systems.

Technology watch
The monitoring of software and hardware dependencies to ensure that when technology obsolescence occurs, appropriate action is taken to update the technology.

Terminated records
Records which were created or received by a governmental body and which were managed by a records classification system no longer in use. The manual should be version controlled.

Transitory records
Transitory records are those records created by officials but not required by the governmental bodies for which they work to control, support or document the delivery of services, or to carry out operations, to make decisions, or to give account of the activities of government. Such records are needed by officials for only a limited time to facilitate the completion of routine actions or to prepare a subsequent record required by a governmental body for the above-mentioned reasons.

Transmission data
Information in electronic mail systems regarding the date and time messages were sent

or forwarded by the author.

Unstructured system
A system containing information not found in relational databases including images, electronic and paper-based documents, forms, CAD/engineering drawings, enterprise reports, and e-mail.

Second Edition
April 2006

ANNEXURE N: Bibliography

Aeon Archive Limited: High tech Solutions for the archiving and preservation of Optical Data Storage Media [http://www.aeon-archive.com]

Aiim International: Aiim/Cohasset White Paper. Realizing the need and Putting Key Components in Place to "Getting it Right" in Records Management [http://www.aiim.org]

Anderson, R.: Message Archiving is a must. Archive of else, 2005.05.12 [http://www.networkcomputing.com/shared/article]

Arthur, M.: DAM vs DM. Intro to Digital Asset Management. Just what is a DAM?, 2005.04.30 [http://www.cmswatch.com/feature/124-DAM-vs-DM]

Assistant Secretary of Defence for Command, Control, Communications and Intelligence: Design Criteria Standard for Electronic Records Management Software Applications, June 19, 2002 [http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf]

Breeding, M.: *Network Design Manual*. "Storage for the network: Designing an effective strategy". [http://www.nwc.com]

Browning, P, and Lowndes, Techwatch Report: Content Management Systems, September 2001 [http://www.jisc.ac.uk]

Burke, B.: Special Report SAN. High performance shared Storage Area Networks. [http://www.westworldproductions.com]

Cloonan MV and Selby Sanett: "Preservation Strategies for Electronic Records Round 1 (2000-2001) Where are we now: Obliquity and Squint?" *A report to the National Historical Publications and Records Commission*, June 1, 2001 [http://i.s.gceis.ucla.edu/us-interpares/index.html]

Dean, J.: Managing Technology Column: Data roundup [http://www.storage.ibm.com]

Digital Preservation Tested White Paper: Migration: Context and current status, Des. 2001 [http://www.digitaleduurzaamheid.nl]

Disa, Joint Interoperability Test Command: Records Management Application (RMA) Certification Testing. [http://jitc.fhu.disa.mil/recmgt/register.htm]

Department of Public Service and Administration: e-Government Policy, Second draft 2001, version 3.1 [http://www.dpsa.gov.za/e-gov/2001docs/e-govpolicyFramework.htm]

Department of Public Service and Administration: Handbook on Minimum Interoperability Standards (MIOS). A blueprint to guide seamlessness and interoperability in public service [http://www.dpsa.gov.za/e-gov/2002docs/MIOS-handbook16April"02.doc]

Eiteljorg, H.: "Preservation for the future – with emulation or migration?" *CSA*

Newsletter Vol. XII, No. 1 Spring 1999
[http://www.csanet.org/newsletter/spring99/nls9906.html]

European Commission: Model Requirements for the Management of electronic records. Moreq specification, March 2001 [http://cornwell.co.uk/moreq]

Fast, S.: The birth of network-attached storage. [http://www.planetit.com]

Gable J.: "A Five-part strategy for records management", *Transform Magazine*, May 2002 [http://www.imagingmagazine.com/cgi-bin/printable.cgi]

GITOC: Using open source software in the South African Government, request for information on a proposed policy by the open source software work group, GITOC, August 2002 Version 11
[http://www.oss.gov.za/osspolicyframeworkVi.pdf]

Granger, S.: "Emulation as a Digital Preservation Strategy". *D-lib Magazine*, Vol. 6, Nr 10, Oct. 2000 [http://www.dlib.org/dlib/October00/granger/10granger.html]

Government of New Foundland and Labrador: Policy on the management of e-mail messages, 7 Nov. 2002 [http://www.exec.gov.nl.ca/exec/treasury/itpolicy/e-mail/email_policy.htm]

Harris, V.S.: Exploring Archives: An introduction to archival ideas and practice in South Africa. Pretoria, 2nd edition, 2000.

Harrison, E.: "Preservation for the future – with emulation or migration?". *CSA Newsletter*, Vol. XII, No. & 7, Spring 1999.
[http://www.csanet.org/newsletter/spring99/nls9906.html]

Haverson D.: "Records Management: Digital Dillemma". *Transform Magazine*, March 2002 [http://www.imagingmagazine.com/cgi-bin/printable.cgi]

Hedstrom, M.: Draft Section of a Report on Migration Strategies prepared for the Experts Committee on Software Obsolescence and Migration which met in Fermo, Italy, April 1996. [http://www.sis.pitt.edu]

Hofman, H.: Metadata and the management of current records in digital form, July 2000. [http://www.ica.org/biblio/com/cer/metadata.htm]

Holdsworth, D and P Wheatley: Emulation, Preservation and Abstraction [http://129.11.152.25/Camileon/dh/ep5.html]

Horsman, P.: Electronic record keeping. The record keeping system as a framework for the management of electronic records, Amsterdam, 2001

International Council on Archives (ICA), Guide for Managing Electronic Records from an Archival Perspective, February 1997
[http://www.ica.org/biblio/cer/guide_eng.html]

International Council on Archives (ICA), Electronic Records: A workbook for Archivists, April 2005

International Standards Organisation, ISO 19005-1: Document Management - Electronic

document file format for long term preservation – Part 1: Use of PDF 1.4 (PDF/A-1.)

International Standards Organisation, "PDF/A-Worldwide collaboration to preserve electronic documents". *ISO Focus*, March 2006.

International Standards Organisation, ISO 14721: Space Data and Information Transfer Systems – Open archival information systems – Reference model.

Jenkins C.: Cedars guide to: Digital Preservation Strategies, Version 3, April 2002 [http://www.leeds.ac.uk/guideto/dpstrategies/dpstrategies.html]

Kentucky Department for Libraries and Archives: Electronic Records Management Guidelines – File Format. [http://www.kdla.ky.gov/recmanagement/tutorial/fileformats.htm]

Kirkwood, C.: "Starting from scratch: Preserving electronic records as part of the cultural heritage", *Archives News* 40, 3 March 1998.

Kronauer, C.: Special Report SAN. Mixed media NAS ready or not? [http://www.westworldproductions.com]

Lavoie, BF.: Technology Watch Report: The Open Archival Information System Reference Model: Introductory Guide, January 2004 [http://www.dpconline.org/docs/lavoie-OAIS.pdf]

Lavoie B and R Gartner, Technology Watch Report: Preservation Metadata, September 2005 [http://dpconline.org/docs/reports/dpctw05-01.pdf]

Lava Systems White Paper: "Just for the record; Effective archive document management" , *Convergence*, Vol. 2, No. 1, pp. 72-75.

McClure, CR and JT Sphere: Guidelines for electronic records management on State and Federal Agency Websites, 00/10/16. [http://www.istweb.syr.edu/mcclure/guidelines.html]

McDonald, SJ.: RUL. WCMS (Web Content Management System), June 2002. [http://www.libraries.rutgers.edu/rul/staff/groups/wcms/reports/wcms_report_1.shtml]

Miller, B.: Managing Electronic Records. It can be done. [http://www.provsys.com]

Mostert, W.: Roadmap on legal requirements for IDMS implementation by Government Departments, July 2004.

National Archives and Records Administration: Managing Electronic Records. Washington, 1990. [http://www.nara.gov]

National Archives and Records Administration: Guidance on Managing Web Records [http://www.archives.gov]

National Archives and Records Administration: Records Management Guidance for Agencies implementing electronic signature technologies, 2000.10.18 [http://www.archives.gov]

National Archives and Records Administration: Vital Records Disaster Mitigation and Recovery: An Instructional Guide, 1999 [http://www.archives.gov.records_management/publications/vital_records.html]

National Archives and Records Service of South Africa: Appraisal Manual. Pretoria, September 1996.

National Archives and Records Service of South Africa: Appraisal Policy Guidelines. Pretoria, 1st Edition, December 1998.

National Archives and Records Service of South Africa: Archives Instructions. January 1999.

National Archives and Records Service of South Africa: Registry Guide. Pretoria, May 1998.

National Archives and Records Service of South Africa: Directive D8. Prototype Records Control Schedule for Local Authorities. Pretoria, February 1999. [http://www.national.archives.gov.za]

National Archives and Records Service of South Africa: Directive D10. General disposal authority number AT2 for the destruction of transitory records of all governmental bodies. Pretoria, July 1998. [http://www.national.archives.gov.za]

National Archives and Records Service of South Africa: Directive D11. General disposal authority number AE1 for the destruction of ephemeral electronic and related records of all governmental bodies. Pretoria, April 1997. [http://www.national.archives.gov.za]

National Archives of Australia: *Archives Advice 5*: Protecting and Handling Magnetic Media. [http://www.naa.gov.au]

National Archives of Australia: *Archives Advice 6*: Protecting and Handling Optical Disks. [http://www.naa.gov.au]

National Archives of Australia: *Archives Advice 24:* Distributed management of electronic records. [http://www.naa.gov.au]

National Archives of Australia: Keeping Electronic Records, 1997. [http://www.naa.gov.au]

National Archives of Australia: Managing Electronic Records - a shared responsibility. 1997. [http://www.naa.gov.au]

National Archives of Australia: Procedure for managing e-mails as records, Feb. 2004 [internal document]

National Archives of Canada: Managing Electronic Records in an Electronic Work Environment, May 1996. [http://www.archives.ca]

National Archives of Canada: Electronic Work Environment (EWE), Vision. May 1996. [http://www.archives.ca]

National Archives of Canada: Managing shared directories and Files, May 1996. [http://www.archives.ca]

National Archives of the UK: Generic requirements for sustaining electronic information over time: Part 1 Defining the characteristics for authentic records [http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs1.pdf]

National Archives of the UK: Generic requirements for sustaining electronic information over time: Part 2 Sustaining authentic and reliable records: management requirements [http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs2.pdf]

National Archives of the UK: Generic requirements for sustaining electronic information over time: Part 3 Sustaining authentic and reliable records: technical requirements [http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs3.pdf]

National Archives of the UK: Generic requirements for sustaining electronic information over time: Part 4 Guidance for categorizing records to identify sustainable requirements [http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs4.pdf]

Orlandi, J.: How to painlessly add storage. [http://www.westworldproductions.com]

Public Records Office: E-government policy framework for electronic records management, version 2.0, July 2001 [http://www.e-envoy.gov.uk]

Public Records Office: Good practice in managing electronic documents using Office 97 on a local area network [http://www.nationalarchives.gov.uk]

Public Records Office: Requirements for Electronic Records Management Systems. 1: Functional Requirement, 2002 revision: final version. [http://www.pro.gov.uk/recordsmanagement]

Public Records Office: Requirements for Electronic Records Management Systems. 3: Reference Document, 2002 revision: final version. [http://www.pro.gov.uk/recordsmanagement]

Public Records Office: Corporate Policy on Electronic Records, Sept. 2000

Public Record Office: Managing Web Resources - Management of electronic records on websites and intranets: An ERM Toolkit, Version 1.0, December 2001 [http:///www.nationalarchives.gov.uk]

Raas, U.: “Electronic record keeping - more than electronic document management.” *Records Management Journal*, vol. 9, no.2. August 1999, pp. 117-129.

Roper, M.: (Gen. Ed.): Managing Public Sector Records. A Study Programme. Managing Electronic Records, International Records Management Trust, 1999.

Sorrentino, P.: E-mail archivin.g [http://www.tacadvisory.com/powertips_sample.asp?NAME=st999720.htm]

State Archives Service: Internal Discussion Document: Premises for the drafting of guidelines for the archival management of electronic records by the Committee on Machine-Readable Archives (COMA). Pretoria, November 1995.

State of Texas: Guidelines for the management of electronic transactions and signed records prepared by the UETA Task Force of the Department of Information Resources and the Texas State Library and Archives Commission [http://www.dir.state.tx.us/standards/UETA_Guideline.htm]

South African Bureau of Standards: SANS 15489: Information and documentation – Records management – Part 1 General.

South African Bureau of Standards: SANS 15489: Information and documentation – Records management – Part 2 Guidelines.

South African Bureau of Standards: SANS 15801: Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability.

South African Bureau of Standards: SANS 23081: Information and documentation – Records Management processes – Metadata for records – Part 1: Principles.

South African Bureau of Standards: SANS 17799: Information technology – security techniques – Code of practice for information security management.

South African Bureau of Standards: A Recommended Practice - ARP 077 – *Document Management Applications - Long term preservation of electronic document-based information*. (Based on ISO 18492)

South African Bureau of Standards: A Recommended Practice - ARP 076 - Electronic Imaging – Human and organisational issues for successful electronic image management implementations. (Based on ISO 14105)

The UK National Archives: *Digital Preservation Guidance Note: 3* – Care handling and Storage of Removable Media. [http://www.nationalarchives.gov.uk]

The UK National Archives: *Digital Preservation Guidance Note – 2*: Selecting Storage Media for Long-term preservation. [http://www.nationalarchives.gov.uk]

The Sedona Conference: The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age, September 2004. [http://www.thesedonaconference.org]

United Nations (Prepared by The Advisory Committee for the Co-ordination of Information Systems [ACCIS]): Management of electronic records: Issues and guidelines. New York, 1990.

US Department of Commerce: E-mail policy. [http://www.ofa.noaa.gov/names/Records_Management/docemail_policy.htm]

Vasudeva, A.: Special Report SAN. SAS, NAS, SAN - Past, Present and Future. [http://www.westworldproductions.com]

Victoria Government: Whole of Victoria Government Web Content Management Requirements Definition Tool, Version 1.0, Introduction, 2003.6.25

[http://www.egov.vic.gov.au]
Victoria Government: Whole of Victorian Government Web Content Management Requirements Definition Report, Version 1.0, 17 June 2003. [http://www.egov.vic.gov.au]

Venter, L.: The National Archives and Records Services requirements for the management of electronic records in the public sector: An archivists' perspective on Records Management v.s Storage Management. [unpublished paper]

Venter, L.: Strategies for the management of e-mail in terms of archival legislation (paper presented at the AMC E-mail management Conference, 12 August 2004).

Whealley, P.: Technology Watch Report: Institutional Repositories in the context of Digital Preservation, March 2004.
[http://www.dpconline.org/docs/dpctwf4=word.pdf]

FURTHER INFORMATION

Further guidance on the management of electronic records can be obtained from:

The Records Management Division
National Archives and Records Service of South Africa
Private Bag X236
Pretoria
0001

Tel: (012) 323 5300
Fax: (012) 323 5287
Fax to e-mail: 086 682 5055
E-mail: erecords@dac.gov.za

CHANGE HISTORY

VERSION NUMBER	CHANGES MADE
2nd Edition	1. Typing errors corrected 2. Major additions to all the paragraphs; and 3. Existing text reorganised.

(HB 4728 v10)