arts and culture

Department:
Arts and Culture
REPUBLIC OF SOUTH AFRICA

GUIDELINES FOR THE COMPILATION OF A RECORDS MANAGEMENT POLICY (INCLUDING AN EXAMPLE OF A RECORDS MANAGEMENT POLICY)

National Archives and Records Service of South Africa

April 2006

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: rm@dac.gov.za

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

1st Edition April 2003
2nd Edition April 2006

The information contained in this publication may be re-used provided that proper acknowledgement is given to the specific publication and to the National Archives and Records Service of South Africa.

CONTENT

A: GUIDELINES FOR THE DEVELOPMENT OF A RECORDS MANAGEMENT POLICY 1

A1. INTRODUCTION 1
A2. PLANNING THE POLICY 2
A2.1 Understanding the environment in which the governmental body exists 2
A2.2 Understanding the business of a governmental body 2
A2.3 Understanding the records generated by the governmental body 2
A2.4 Understanding the impact on the human resources 3
A3. STRUCTURING A RECORDS MANAGEMENT POLICY 3
A3.1 Policy statement 4
A3.2 Relationship with other policies 4
A3.3 Statutory and regulatory framework 4
A3.4 Intended audience 4
A3.5 Roles and responsibilities 4
A3.6 Identification of records systems 5
A3.7 Classification systems 5
A3.8 Disposal of records 5
A3.9 Storage and custody 6
A3.10 Access and security 6
A3.11 Legal admissibility and evidential weight 7
A3.12 Training 7
A3.13 Inspections by the National Archives and Records Service 7
A3.14 Evaluation 7
A4. IMPLEMENTING THE POLICY 7
A5. MONITOR AND REVIEW THE POLICY 8
A6. INPUT BY NATIONAL ARCHIVES AND RECORDS SERVICE 8

B. EXAMPLE OF A RECORDS MANAGEMENT POLICY 9

A: GUIDELINES FOR THE DEVELOPMENT OF A RECORDS MANAGEMENT POLICY

A1. INTRODUCTION

A governmental body keeps records to support its operations, as well as to fulfill legal and other obligations.

Records should be managed by the governmental body in terms of the broad policy guidelines contained in the National Archives and Records Service of South Africa Act, (Act No 43 of 1996 as amended). It is, however, essential for each body to establish its own records management policy to link its unique processes and procedures to the 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 body's overall mandate and mission objectives. The records management policy provides the framework within which a governmental body affirms its commitment to create authentic and reliable records.

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 records management policy using the guidelines as a basis to work from. Governmental bodies should also take note of the recommendations regarding matters that should be addressed in a records management policy contained in the following national standards:

- SANS 15489 – *Information and documentation – Records Management- Part 1: General;*
- SANS 23081 – *Information and documentation – Records Management processes – Metadata for records – Part 1: Principles;* and
- SANS 15801: *Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability*. [1]

The National Archives and Records Service also recommends compliance with the National Intelligence Agency's *Minimum Information Security Standard*[2] and the Department of Public Service and Administration's *Draft Information Security Policies*.[3] Governmental bodies that are not subject to the *MISS* should take note of the guidance in SANS 17799: *Information Technology – Security techniques - Code of Practice for Information Security Management.*[4]

---

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

[2] The *Minimum Information Security Standard* can be obtained from the National Intelligence Agency, Private Bag X87, PRETORIA, 0001, Telephone: 012 427 4000, Fax: 012 427 4651.

[3] 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.

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

A2. PLANNING THE POLICY

A governmental body cannot draft a records 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.

A2.1 Understanding the environment in 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 body and the administrative, legal, business and social contexts in which it operates;
- an understanding of the body'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 body'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 records management policy as well as a functional subject file plan and the preparation of a records disposal authority.

A2.2 Understanding the business of a governmental body

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 records management policy and a file plan, and to gain an understanding of why records are created and why and for how long they should be retained.

A2.3 Understanding the records generated by the governmental body

Records are the reflection of a body's activities. It is essential to know what information a body holds and thus be able to respond to requests for information. A records audit profiles each record series and system, and helps to identify any problems, to establish a records management programme, to design a records management policy and a file plan and to produce a disposal schedule. It also helps to determine what is required to install and maintain the records management programme (space, equipment, personnel, etc) as well as how to evaluate the efficacy and economy of records management systems, particularly in the context of the preparation for compliance with the Promotion of Access to Information implementation.

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:

- a full understanding of the body - the nature of its activities, its mission, objectives, components and operations;
- level of staff awareness of records management;
- what records are held and the activities to which they relate;
- an inventory of record containers (cabinets, shelves, etc);
- records documentation (file lists, indexes, etc.);
- extent of records;
- where copies of records exist;
- date range of the records;
- frequency of consultation of the records;
- tracking systems for the records;
- current records management system and competence levels of records management staff;
- record keeping costs;
- identification of records that should be sustained for the long term.

A2.4 Understanding the impact of records management practices and systems on the human resources

Records management is very much a cultural issue in a governmental body. There should be sufficient understanding of what the current record keeping behaviour of the staff is and how the implementation of a records management policy would impact on the training, skills level and work processes and procedures of the staff.

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 records management policy may have an impact on the job functions of existing staff. Governmental bodies need to determine if it would be necessary to re-skill and redeploy staff. The staff would be more receptive to the policy when they have had an opportunity to raise issues and concerns during such an investigation.

A3. STRUCTURING A RECORDS 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.
- E-mail policy
- Electronic records management policy
- Internet policy
- Information security policy, etc.

A3.3 Statutory and regulatory framework

List all the relevant laws and regulations that impact on records creation and records management practices.

A3.4 Intended audience

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.

A3.5 Roles and responsibilities

A3.5.1 Top and senior management

Define the responsibilities of top and senior management regarding 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 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 Identification of records systems

Policy should-

- identify all systems that are creating and storing records;
- describe the systems;
- describe the information contained in the systems;
- list contact particulars of responsible persons;
- describe additional documentation relating to the system(s) e.g. *System Technical Manuals, Systems Procedure Manuals, File plan, Register of Files Opened, Registry Procedures Manual,* etc.

A3.7 Classification systems

Policy should-

- stipulate that only classification systems that have been approved by the National Archivist may be used for both paper-based and electronic records;
- indicate who to contact when difficulties are experienced with the allocation of reference numbers;
- emphasize that no revisions and additions may be made to the classification systems without the records/information manager's prior approval;
- indicate whether the classification systems are only used in the paper-based environment or electronically;
- if used electronically indicate whether the systems are used in a fully fledged Integrated Document and Records Management System or as a shared environment on a network drive;
- if not used electronically indicate how records on individual personal computers are to be managed;
- indicate how e-mail should be managed, if a separate e-mail policy does not exist.

A3.8 Disposal of records

Policy should-

- make it clear that no public records may be destroyed, erased or otherwise disposed of without prior written authorisation from the National Archivist;
- emphasise that retention periods for non-archival records must be determined by the organisation itself;
- emphasise that the records manager, in consultation with the users, will determine the retention periods;

- indicate that transparency, accountability, the requirements of democracy, any other legal obligations as well as the office's own functional needs must always be considered when determining retention periods;
- insist that the records/information manager must be contacted whenever the staff disagree with an allocated retention period;
- emphasise that archival paper-based records must be kept for a period of 20 years before they are transferred to an archives repository, unless agreement on a shorter period before transfer has been reached with the National Archivist;
- indicate where disposal schedules are to be obtained;
- give clear guidelines on the disposal of electronic records.

A3.9 Storage and custody

- Policy should indicate if a disposal agreement with the National Archives and Records Service is in place that contains special arrangements regarding the custody of records.
- Policy should give precise guidelines on:
    - *where* information resources are kept [In which office, particular locality, hard drive, directory or sub-directory. The level of detail will vary according to specific circumstances];
    - the appropriate physical care of information resources [Consider the special requirements of media like microfilm, videotapes and other magnetic media, appropriate precautions against fires, and so on];
    - under whose immediate control resources are to be kept; which media resources will be kept in. [There should be clarity as to which records should be kept only in electronic form or in both electronic and hard copy];
    - how often records kept on electronic storage media should be refreshed and migrated to new storage media to enable them to be accessible when required;
    - Policy should indicate that a registry procedure manual exists and should indicate were and from whom the registry procedures can be obtained.

A3.10 Access and security

Policy should give clear guidelines on the security of all information systems and resources. Aspects requiring attention include the following:

- general physical security;
- control over the removal of resources from their place of custody or from the control of the responsible person;
- the protection of privacy and confidentiality [Keep in mind the inappropriate disclosure of information which may harm the organisation or infringe the privacy rights of individuals. The right to privacy is now enshrined in the Bill of Rights, and legislation is being prepared to give effect to it];
- protection against unauthorised access;
- maintenance of the integrity of records which means that the records should be protected against alteration or deletion;
- the specific concerns regarding electronic information. [A systematic back-up procedure is imperative. Control over software, particularly pirated software, from getting onto the organisation's computers is also important];
- the protection of vital records [i.e. those records the loss of which would render the organisation partially or totally unable to carry out its normal functions. If the organisation implements a vital records protection programme, its scope and the choice of on-site or off-site security storage should be determined].

Policy should emphasize that the National Archivist must immediately be informed in writing when losses of public records occur.

A3.11 Legal admissibility and evidential weight

Policy should-

- address the need to ensure that records are admissible as evidence in courts of law and in this regard
  - stipulate what metadata should be captured [if a documented metadata schema exists, cross reference to it. If it does not exist policy should contain a brief description of what should be captured. Records manager should then take steps to document in detail]
  - stipulate what audit trail data should be captured and who should have access to it.
- identify procedures to ensure that all legal obligations relating to information management are satisfied. [This refers to tax laws, audit requirements, copyright, the Promotion of Access to Information Act, 2000 etc.].

A3.12 Training

Policy should indicate-

- the relevant records management training courses that should be attended and by which staff members at which time intervals;
- who is responsible for training staff in the allocation of file reference numbers;
- who is responsible for training the registry staff;
- that the records manager should ensure that all staff are conversant with the proper registry procedures to enable them to support registry to function properly.

A3.13 Inspections by the National Archives and Records Service

Policy should-

- indicate that the National Archives and Records Service, subject to the exemption provision contained in section 13(2)(c) of the National Archives and Records Service Act, 1996 as amended, is entitled to full and free access, at all times, to all public records in the organisation's custody;
- mention the records that are exempted, from full and free access by the National Archives and Records Service as well as the reasons.

A3.14 Evaluation

- Policy should stipulate criteria for measuring the records management programme's success.

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 records 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 record keeping and records management behaviour 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 records management policy should consist of a set of 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.

B. EXAMPLE OF A RECORDS MANAGEMENT POLICY

The attached policy serves only as 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 the specific body. When drafting a policy, governmental bodies should ensure that the National Archives and Records Service's records management requirements are integrated with their own business requirements and administrative practices.

RECORDS MANAGEMENT POLICY FOR [NAME OF GOVERNMENTAL BODY]

Version [insert version number] of [date]

Content

1 Purpose
2 Policy statement
3 Relationship with other policies
4 Intended audience
5 Regulatory framework
6 Roles and responsibilities
6.1 Head of [name of governmental body]
6.2 Senior managers
6.3 Records manager
6.4 Chief Information Officer
6.5 IT manager
6.6 Security manager
6.7 Legal services manager
6.8 Registry staff
6.9 Staff
7 Record classification systems and related record storage areas
7.1 Correspondence systems
7.1.1 File plan
7.1.2 Storage areas
7.1.2.1 Paper-based correspondence files
7.1.2.1.1 The central registry
7.1.2.1.2 The Human Resources registry
7.1.2.2 Electronic correspondence systems
7.2 Records other than correspondence systems
7.2.1 Schedule for records other than correspondence systems
7.2.2 Storage areas
7.2.2.1 Paper-based
7.2.2.2 Micrographic
7.2.2.3 Audio-visual
7.2.2.4 Electronic systems other than the correspondence system
8 Disposal
9 Storage and custody
10 Access and security
11 Legal admissibility and evidential weight
12 Training
13 Monitor and review
14 Definitions
15 References
16 Approval

1. Purpose

1.1 Section 13 of the National Archives and Records Service of South Africa Act, 1996 requires the [name of governmental body] to manage its records in a well-structured record keeping system, and to put the necessary policies and procedures in place to ensure that its record keeping and records management practices comply with the requirements of the Act.

1.2 Information is a resource of the same importance to good management as other standard resources like people, money and facilities. The information resources of [name of governmental body] must therefore be managed as a valuable asset. Appropriate records management is a vital aspect of maintaining and enhancing the value of this asset. [Name of governmental body] considers its records to be a valuable asset to:

- enable [name of governmental body] to find the right information easily and comprehensively;
- enable [name of governmental body] to perform its functions successfully and efficiently and in an accountable manner;
- support the business, legal and accountability requirements of [name of governmental body];
- ensure the conduct of business in an orderly, efficient and accountable manner;
- ensure the consistent delivery of services;
- support and document policy formation and administrative decision-making;
- provide continuity in the event of a disaster;
- protect the interests of [name of governmental body] and the rights of employees, clients and present and future stakeholders;
- support and document the [name of governmental body]'s activities, development and achievements;
- provide evidence of business in the context of cultural activity and contribute to the cultural identity and collective memory.

1.3 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

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 Records Management Policy consist of this policy as well as additional parts that cover the unique nature of the broad spectrum of records generated by [name of governmental body]. These policies are managed by the records manager. The following parts exist:

- Electronic records management policy
- E-mail policy;
- Document imaging; and
- Web content management policy

3.2 Other policies that are closely related to the Records Management Policy are

- the Information Security Policy which is managed by the Security Manager;
- the Internet Usage Policy which is managed by the IT Manager; and the
- Promotion of Access to Information Policy which is managed by the CIO.

[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 This policy impacts upon [name of governmental body]'s work practices for all those who:

- create records including electronic records;
- have access to records;
- have any other responsibilities for records, for example storage and maintenance responsibilities;
- have management responsibility for staff engaged in any these activities; or manage, or have design input into, information technology infrastructure.

4.2 The policy therefore applies to all staff members of the [name of governmental body] and covers all records regardless of format, medium or age.

5. Regulatory framework

5.1 By managing its paper-based records effectively and efficiently [name of governmental body] strives to give effect to the accountability, 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);
  - 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 Head of [name of governmental body]

6.1.1 The [post designation] is ultimately accountable for the record keeping and records management practices of [name of governmental body].

6.1.2 The [post designation] is committed to enhance accountability, transparency and improvement of service delivery by ensuring that sound records management practices are implemented and maintained.

6.1.3 The [post designation] supports the implementation of this policy and requires each staff member to support the values underlying in this policy.

6.1.4 The [post designation] shall designate a senior manager to be the records manager of the [name of governmental body] and shall mandate the records manager to perform such duties as are necessary to enhance the record keeping and records management practices of [name of governmental body] to enable compliance with legislative and regulatory requirements.

6.2 Senior managers

6.2.1 Senior managers are responsible for the implementation of this policy in their respective units.

6.2.2 Senior managers shall lead by example and shall themselves maintain good record keeping and records management practices.

6.2.3 Senior management shall ensure that all staff are made aware of their record keeping and records management responsibilities and obligations.

6.2.4 Senior managers 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.

6.3 Records manager

6.3.1 The records manager is responsible for:

- the implementation of this policy;
- staff awareness regarding this policy;
- the management of all records according to the records management principles contained in the National Archives and Records Service Act, 1996.
- The determination of retention periods in consultation with the users and taking into account the functional, legal and historical need of the body to maintain records of transactions.

6.3.2 The specific duties of the records manager 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.]

6.3.3 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.

6.3.4 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].

6.3.5 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.

6.3.6 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.]

6.4 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 responsible for the day-to-day maintenance of electronic systems that stores records.

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 appropriate *systems technical manuals* and *systems procedures manuals* are designed for each electronic system that manages and stores records.

6.5.4 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.

6.5.5 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.

6.5.6 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.

6.5.7 The IT manager shall ensure that back-ups are stored in a secure off-site environment.

6.5.8 The IT manager shall ensure that systems that manage and store records are virus free.

6.5.9 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 Registry staff

6.8.1 The registry staff are responsible for the physical management of the records in their care.

6.8.2 Detailed responsibilities regarding the day-to-day management of the records in the registry are contained in the *Registry Procedure Manual*.

6.9 Staff

6.9.1 Every staff member shall create records of transactions while conducting official business.

6.9.2 Every staff member shall manage those records efficiently and effectively by:

- allocating reference numbers and subjects to paper-based and electronic records according to the file plan;
- sending paper-based records to the registry for filing;
- ensuring that records are destroyed/deleted only in accordance with the written disposal authority issued by the National Archivist.

6.9.3 Records management responsibilities shall be written into the performance agreements of all staff members to ensure that staff are evaluated on their records management responsibilities.

[Note: Governmental bodies should identify and define all other roles and their responsibilities.]

7. Records classification systems and related storage areas

The [name of governmental body] has the following systems that organize and store records:

7.1 Correspondence systems

7.1.1 File plan

7.1.1.1 Only the file plan approved on [date] and implemented on [date] shall be used for the classification of correspondence records. The file plan shall be used for the classification of paper-based and electronic (including e-mail) records.

7.1.1.2 Specific procedures for the allocation of file subjects and reference numbers to electronic records are contained in the [name of system] procedures manual that is published on the Intranet [provide URL]/filed on file [give file number from the governmental body's file plan]. More specific guidance regarding the classification of e-mail is contained in the E-mail management policy that is published on the Intranet [provide 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.]

7.1.1.3 Each staff member shall allocate file reference numbers to all correspondence (paper, electronic, e-mail) according to the approved subjects in the file plan.

7.1.1.4 When correspondence is created/received for which no subject exists in the file plan, the records manager should be contacted to assist with additions to the file plan. Under no circumstances may subjects be added to the file plan if they have not been approved by the records manager. Specific procedures regarding the addition and approval of a subject in the electronic system are contained in the [name of system] procedures manual that is published on the Intranet [provide 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.]

7.1.2 Storage areas

7.1.2.1 Paper-based correspondence files are kept in the custody of-

7.1.2.1.1 The central registry

7.1.2.1.1.1 All paper-based correspondence system records that are not HR related are housed in the central registry.

7.1.2.1.1.2 All these records are under the management of the records manager who is mandated to ensure that they are managed properly.

7.1.2.1.1.3 The registry is a secure storage area and only registry staff are allowed in the records storage area.

7.1.2.1.1.4 Staff members that need access to files in the registry shall place a request for the files at the counter. [Note: Governmental bodies should adapt this as is appropriate for their specific circumstances.]

7.1.2.1.1.5 The registry shall be locked when registry is not in operation.

[Note: Governmental bodies should indicate where all the case files which are listed in the series of separate case files are stored and how they are managed]

7.1.2.1.2 The Human Resources registry

7.1.2.1.2.1 All Human Resources related records are housed in the HR Registry.

7.1.2.1.2.2 The general HR subject files as well as HR case files are under the management of the records manager who is mandated to ensure that they are managed properly.

7.1.2.1.2.3 [name of governmental body] maintains a set of paper-based case files for each staff member. These files are confidential in nature and are housed in a secure storage area in the HR registry.

7.1.2.1.2.4 The case files are managed as part of the List of Series of Separate Case Files that is maintained and managed by the records manager.

7.1.2.1.2.5 The files exist only in paper-based format and the physical tracking of the case files are managed with the file tracking system in the Integrated Document and Records Management System [Note: Governmental bodies should adapt the wording appropriately.]

7.1.2.2 Electronic correspondence records are stored in an electronic repository that is maintained by the IT section.

7.1.2.2.1 Access to storage areas where electronic records are stored is limited to the Information Technology staff who have specific duties regarding the maintenance of the hardware, software and media.

[Note: Governmental bodies have not necessarily implemented Integrated Document and Records Management Systems. Should the electronic records be managed according to the file plan on each individual PC or on a shared drive that should be noted here. If the electronic records are not managed formally, they do not form part of a formal record keeping system and should not be listed here. The details regarding their management should be addressed in the electronic records management policy]

7.2 Records other than correspondence systems

7.2.1 Schedule for records other than correspondence systems

7.2.1.1 The records manager maintains a schedule of all records other than the correspondence system. The schedule contains a description of each set of records other than the correspondence system and indicates the storage location and retention periods of these records regardless of format. The schedule is available on the Intranet [provide 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.]

7.2.1.2 Should records be created/received that are not listed in the schedule, the records manager should be contacted to add the records to the schedule.

7.2.2 Storage areas

7.2.2.1 Paper-based

7.2.2.1.1 The [name of governmental body] has the following sets of paper-based records other than the correspondence systems that are in the custody of the various officials that use them on a daily basis. [List the sets of records here]

7.2.2.1.2 These records are under the control of the records manager who is mandated to ensure that they are managed properly.

[Note: If the governmental body does not have such records not, this paragraph can be omitted]

7.2.2.2 Micrographic records

7.2.2.2.1 The [name of governmental body] has the following sets of microfilmed records that are stored in the [name of storage area]. [List the sets of records here]

7.2.2.2.2 These records are under the control of the records manager who is mandated to ensure that they are managed properly.

[Note: If a governmental body does not have such records this paragraph can be omitted]

7.2.2.3 Audio-visual records

7.2.2.3.1 The [name of governmental body] has the following sets of audio-visual records that are stored in the [name of storage area]. [List the sets of records here]

7.2.2.3.2 These records are under the control of the records manager who is mandated to ensure that they are managed properly.

[Note: If a governmental body does not have such records this paragraph can be omitted]

7.2.2.4 Electronic systems other than the correspondence systems

7.2.2.4.1 [Name of governmental body] has a number of electronic records systems in operation which is not part of the correspondence system and that generate and store public records. [List the sets of records here]

7.2.2.4.2 The IT manager is responsible for the day-to-day maintenance of these systems.

7.2.2.4.3 The records maintained in these systems are under the control of the records manager who is mandated to ensure that they are managed properly.

7.2.2.4.4 Detailed guidance regarding the management of these systems is contained in the electronic records management policy.

[Note: For each system note the name of system, where the database/repository is housed, and where the systems are scheduled.]

8. Disposal of records

8.1 No public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior written authorization from the National Archivist.

8.2 The National Archivist has issued Standing Disposal Authority Number [add number] for the disposal of records classified against the file plan. The records manager manages the disposal schedule.

8.3 The National Archivist issued Standing Disposal Authority Number [add number] on the schedule of records other than correspondence systems. The records manager manages the disposal schedule.

8.4 Retention periods indicated on the file plan and schedule were determined by taking [name of governmental body]'s legal obligations and functional needs into account. Should a staff member disagree with the allocated retention periods, the records manager should be contacted to discuss a more appropriate retention period.

8.5 Disposal in terms of these disposal authorities will be executed annually in December. [Note: Governmental bodies should adapt this as is appropriate for their specific circumstances.]

8.6 All disposal actions should be authorized by the records manager prior to their execution to ensure that archival records are not destroyed inadvertently.

8.7 Non-archival records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions may not be destroyed until such time that the Manager: Legal Services has indicated that the destruction hold can be lifted.

8.8 Paper-based archival records shall be safely kept in [name of storage area] until they are due to transfer to the National Archives Repository. Transfer procedures shall be as prescribed by the National Archives in the *Records Management Policy Manual.*

8.8 Specific guidelines regarding the procedure to dispose of electronic records are contained in the electronic records management policy.

9. Storage and custody

9.1 See par. 7 for an identification of all record keeping systems and their storage locations.

9.2 All records shall be kept in storage areas that are appropriate for the type of medium. The National Archives and Records Services' guidelines contained in the *Records Management Policy Manual* shall be applied.

9.3 Specific policies for the management of electronic storage media are contained in the electronic records management policy.

10. Access and security

10.1 Records shall at all times be protected against unauthorized access and tampering to protect their authenticity and reliability as evidence of the business of [name of governmental body].

10.2 Security classified records shall be managed in terms of the Information Security Policy which is available from the security manager.

10.3 No staff member shall remove records that are not available in the public domain from the premises of [name of governmental body] without the explicit permission of the records manager in consultation with the information security manager.

10.4 No staff member shall provide information and records that are not in the public domain to the public without consulting the Chief Information Officer. Specific guidelines regarding requests for information are contained in the Promotion of Access to Information Policy which is maintained by the Chief Information Officer.

10.5 Personal information shall be managed in terms of the Promotion of Access to Information Act until such time that specific protection of privacy legislation is enacted.

10.6 No staff member shall disclose personal information of any member of staff or client of [name of governmental body] to any member of the public without consulting the Chief Information Officer first.

10.7 An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.

10.8 Records storage areas shall at all times be protected against unauthorized access. The following shall apply:

10.8.1 Registry and other records storage areas shall be locked when not in use.

10.8.2 Access to server rooms and storage areas for electronic records media shall be managed with key card access [Note: governmental bodies should adapt this to specific circumstances]

11. Legal admissibility and evidential weight

11.1 The records of [name of governmental body] shall at all times contain reliable evidence of business operations. The following shall apply:

11.1.1 *Paper-based records*

11.1.1.1 No records shall be removed from paper-based files without the explicit permission of the records manager.

11.1.1.2 Records that were placed on files shall not be altered in any way.

11.1.1.3 No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the records manager.

11.1.1.4 Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

11.1.2 *Electronic records*

11.1.2.1 The [name of governmental body] shall use systems which ensure that its electronic records are:

- authentic;

- not altered or tampered with;
- auditable; and
- produced in systems which utilize security measures to ensure their integrity.

11.1.2.3 The Electronic Records Management Policy contains specific information regarding the metadata and audit trail information that should be captured to ensure that records are authentic.

12. Training

12.1 The records manager shall successfully complete the National Archives and Records Service's Records Management Course, as well as any other records management training that would equip him/her for his/her duties.

12.2 The records manager shall identify such training courses that are relevant to the duties of the registry staff and shall ensure that the registry staff are trained appropriately.

12.3 The records manager shall ensure that all staff members are aware of the records management policies and shall conduct or arrange such training as is necessary for the staff to equip them for their records management duties.

13. Monitor and review

13.1 The records manager shall review the 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].

13.2 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].

14. Definitions

[Note: Only terms that are used in the policy should be defined]

Archives repository:

The building in which records with archival value are preserved permanently.

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.

Correspondence system:

A set of paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.

Custody:

The control of records based upon their physical possession.

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.

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.

Non-archival records:

Records with a short lived interest or usefulness.

Public record:

A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

Records other than correspondence systems:

Records that do not form part of a correspondence file, or a case file e.g. registers, maps, plans, electronic records, audio-visual records, etc.

Record:

1) Recorded information regardless of form or medium.
2) Evidence of a transaction, preserved for the evidential information it contains.

Records 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.

Recording:

Anything on which sounds or images or both are fixed or from which sounds or images or both are capable of being reproduced, regardless of form.

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.

Schedule for records other than correspondence systems:

A control mechanism for records other than correspondence files (other records), which contains a description and the disposal instructions and retention periods of all other records. It consists of the following parts:

- Schedule for paper-based records other than correspondence files;
- Schedule for electronic records systems other than the electronic correspondence system;
- Schedule for microfilm records;
- Schedule for audio-visual 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.

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.

15. References

[Note: Only references that are really applicable and which confirm the policy should be defined]

Department of Public Service and Administration: *Draft Information Security Policies. Securing Information in the Digital Age.*

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.*

16. Authorization

This policy was approved by [post designation of head of governmental body] on [date].

HEAD OF DEPARTMENT
DATE:

Compilation of a Records Management Policy
2nd Edition
April 2006

CHANGE HISTORY

VERSION NUMBER	CHANGES MADE
2nd Edition April 2006	Part A substantially expanded Example of a policy added as part B

HB#4890v1