National Archives of South Africa

GUIDELINES FOR THE COMPILATION OF A RECORDS MANAGEMENT POLICY

September 1999

GUIDELINES FOR THE COMPILATION OF A RECORDS MANAGEMENT POLICY

1.   **INTRODUCTION**

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

Information resources should be managed by the organisation in terms of the broad policy guidelines contained in the National Archives Act of South Africa, 1996. It is, however, essential for each organisation to establish its own records management policy to link its own unique processes and procedures to the requirements of the National Archives 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. A records management policy should satisfy the following three criteria:

- It should be flexible;
- It should be implementable; and
- It should be cost effective.

These guidelines are issued in terms of section 13(4) of the National Archives of South Africa Act, 1996. The purpose of these guidelines is to enable records managers to compile their own comprehensive records management policy using the guidelines as a basis to work from.

2.   **POLICY ELEMENTS**

2.1   <u>Records manager</u>

Policy should-

- indicate who the records/information manager is;
- identify the sub-records/information managers as well as their areas of responsibility.

2.2   <u>Identification</u>

Policy should-

- emphasise that all records created or received during the execution of an organisation's functions (including electronic records for e.g. e-mail) are public records and that these records <u>must</u> 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.

2.3   <u>Classification</u>

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;

- emphasise that no revisions and additions may be made to the classification systems without the records/information manager's prior approval.

2.4   <u>Disposal of records</u>

Policy should-

- make it clear that <u>no</u> 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;

- 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 a National Archives repository, unless agreement on a shorter retention period has been reached with the National Archivist;

- give clear guidelines on the disposal of electronic records.

2.5   Custody

- Policy should indicate if there is a disposal agreement with the National Archives in place which 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];

- Policy should indicate that a registry procedure manual exist and should indicate were and from whom the registry procedures can be obtained.

2.6   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 in-appropriate disclosure of information which may harm the organisation or infringe on 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 records' integrity which means that the records should be protected against alteration or deletion;

- the specific concerns concerning 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 emphasise that the National Archivist must immediately be informed in writing when losses of public records occur.

2.7 Legality

Policy should-

- address the need to ensure that records are admissible as evidence in courts of law;

- identify procedures to ensure that all legal obligations relating to information management are satisfied. [This refers to tax laws, audit requirements, copyright, Open Democracy legislation when it becomes law, etc.].

2.8 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.

2.9 Inspections by the National Archives

Policy should-

- indicate that the National Archives, subject to the exemption provision contained in section 13(2)(c) of the National Archives Act, 1996, 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, as well as the reasons, from full and free access by the National Archives.

2.10 <u>Evaluation</u>
- Policy should stipulate criteria for measuring the programme's success.

3. CONCLUSION

Since the ultimate responsibility for the records management practices in a governmental body lies with the head of that governmental body he/she must approve of the policy before implementation.

A copy of the policy should be submitted to the National Archivist for his/her record.

4. FURTHER INFORMATION

Further guidance on records management can be obtained from the Records Management Division at:

National Archives of South Africa
Private Bag X236
Pretoria
0001

Tel: (012) 323 5300

Fax: (012) 323 5287

E-mail: arg11@dacst4.pwv.gov.za