National Archives of South Africa

GUIDE TO THE MANAGEMENT OF ELECTRONIC RECORDS IN GOVERNMENTAL BODIES

Pretoria

Second Edition

2000

Acknowledgement

In the compilation of this *Guide*, 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.

CONTENTS

Page

Annexures

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 recordkeeping poses particular challenges to governmental bodies and to the National Archives, 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 classification system 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 therefore essential for governmental bodies to give specific consideration to the preservation of electronic records as part of a formal policy of managing electronic records. To promote strategies for the appropriate management of electronic records of government, the National Archives of South Africa Act (No 43 of 1996) 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 *Guide* is to provide practical guidance to governmental bodies to assist them to comply with legislative requirements regarding electronic records as

an integral part of the strategic management of electronic systems. Without such strategic management, the records of governmental bodies will be insecure and the effective functioning of bodies, based as it is on the information held in their own records, will be jeopardised. And there will be no longer-term institutional and social memory of the present age in the National Archives.

Marie Olivier
NATIONAL ARCHIVIST

1. Introduction

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 recordkeeping 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 tool.

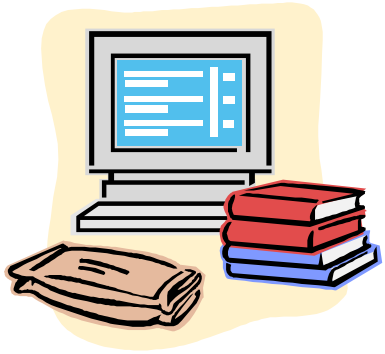
However, the unique and fragile nature of electronic data demands a re-evaluation of the way governmental bodies manage records. Processes and procedures created to meet the needs of recordkeeping in the paper environment do not apply equally to electronic records. A reassessment of records management programmes is therefore required. In order to meet recordkeeping 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.

This publication aims to provide guidance to governmental bodies in South Africa regarding the management of electronic records and

systems. A previous directive entitled *Electronic records and the law: What governmental bodies need to know* served as an introduction to the National Archives' strategy in managing electronic records. It briefly defined the concept of electronic records, the legal implications pertaining to these records, the strategy of the National Archives for electronic records management, as well as the services delivered by the National Archives. This *Guide* is intended to be more comprehensive.

The strategies described in this *Guide* 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 policy 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 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 which can be refined to suit particular cases.



2. What is an electronic record?

The National Archives of South Africa Act (Act No. 43 of 1996) 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 by governmental bodies and which are kept as evidence of a governmental body's functions, activities and transactions.

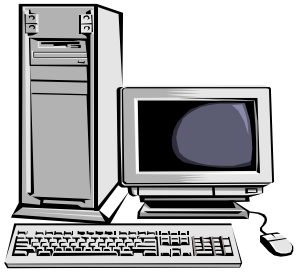
Electronic records are generated electronically and stored by means of computer technology. Electronic records are also considered to include all components of an electronic information system, namely: electronic media as well as all related items such as input documents, printouts, programmes and metadata (background and technical information regarding the information stored electronically.)

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 no longer 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, structure and context 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.

3. Why do we create records?

Both governmental and private institutions routinely create and accumulate records as they undertake their business. These records are created for a purpose and, as evidence of official business, they 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 therefore be negatively affected if sound records management principles are not applied. The need for effective management of records is enhanced by the Promotion of Access to Information Act (Act No 2 of 2000), in terms of which governmental bodies have an obligation to provide information in their records to the public on request and to protect personal privacy at the same time.

Records in electronic form also possess processing capabilities, which could be of considerable value for research and analysis. The high density of electronic data means that it takes up very little storage space, while statistical data can be more easily utilised. Raw data collected for one purpose can be electronically reanalysed for another, while a similar operation might be cumbersome or impossible on paper. The possibility also exists of linking electronic records with common data elements from different files, which would increase the value of such records.

4. The importance of records management and preservation in the electronic environment

4.1 Records management helps governmental bodies to classify records in order to enable them to easily retrieve the records when they are needed and it also helps governmental bodies to decide which records to destroy, and when. 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, governmental bodies must manage their records in a much more disciplined manner than they have in the past. By classifying records and by establishing retention periods in advance, it is less likely that documents will be inadvertently destroyed while they might still be needed for functional, legal or historical purposes.

4.2 As document creators, most public servants have no real mandate, and very little incentive, to concern themselves with the care and management of documents after they are done with them. Records managers/archivists however have a mandate to preserve the documents for the remainder of their lifecycle. Just some of the things that have to be applied to electronic records for the remainder of their lifecycle are:

- For all documents, it must be clear how long they have to be retained, and whether they are to be destroyed or archived;
- Documents 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 documents;

- There must be a means whereby electronic documents can be grouped and otherwise organised for formal disposal.

In short, governmental bodies need a practical means whereby electronic documents can pass from the originator's responsibility, to the people responsible for the corporate memory of the body. The most sensible way to do this is to **use an electronic records management system**. The purpose of an electronic records management system is to manage all records within an organisation including scanned images, word documents, e-mail, paper-based files, etc. to ensure that there is a single database of information accessible from a single interface.

4.3. In the paper-based environment, officials usually create and preserve records in a uniform manner according to a classification system used in the particular governmental body. The records are also physically kept in a uniform matter 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. This could seriously impede effective access for on-going functional purposes as well as long-term retention and preservation.

4.4 It makes little sense to organise paper documents without doing the same for electronic documents. Consider the following:

- How will a body identify both the paper and the electronic documents that it has on a particular subject?
- Even if the paper copy is safely filed, the electronic version is also a public record and the body must be equally aware of and accountable for it.
- It only makes sense to apply a uniform set of standards and

practices for all information in any media, including paper, electronic, audio/video, etc.

4.5 Governmental bodies need a way to organise records so that they can carry out proper retention and disposal. The National Archives requires that they establish a set of subjects, identified by subject title and number, in a hierarchical fashion. Disposal instructions with retention periods are then determined for each unique subject. This scheme of subjects is called a classification system. The classification system with the disposal instructions and the retention periods attached is called a disposal schedule/disposal authority.

4.6 Governmental bodies have to store the physical electronic documents, or they will have no records to manage. End users need ways to classify records and to send them to an electronic repository, without cumbersome processes, and with minimum inconvenience. The goal is to gain as much of the users co-operation as possible, as more often than not the users are making a voluntary decision about the worth of the documents they create. The classification system should be easily accessible and easy to use.

4.7 Classification refers to the process whereby electronic documents stored in the electronic repository are assigned subjects in the classification system that match the document's subject. If this is done consistently for all electronic documents, the disposal and retention decisions will be properly applied to the right documents, and they will be archived/destroyed at the right times.

4.8 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.

4.9 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 an inherently unstable storage medium. Magnetic tape or cassette, CD-WORM (preferably executable CD-WORM) and DVD-WORM can be used for the storage of electronic records. The life expectancy of these media is however 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.

4.10 Each type of storage media (e.g. magnetic tape, CD and DVD) has its own storage and handling requirements (see Annexures F and G) which must be adhered to strictly. Improper treatment of electronic storage media causes physical and chemical damage to the media themselves. The result is that the data stored on these media cannot be accessed.

4.11 The anticipated life expectancy of a magnetic tape is 12-20 years, if stored under optimal conditions and if subject to regular maintenance. This means that simply to preserve the electronic signals on the tape, it is necessary for annual precision rewinding, physical inspection and cleaning to prevent deterioration through chemical reaction. Furthermore, the data has to be transferred to new tapes periodically.

CD-WORM and DVD-WORM seem to offer greater stability for archival storage of electronic records. Accelerated-ageing tests done in terms of the American Standard for Life Expectancy of Information Stored in Recordable Compact Disks Systems (ANSI/PIMA IT9.27) indicates that the life expectancy of these media is 100 years and more if stored under prescribed conditions and handled with care. (See Annexure G). The real goal however, is **access to the disks' content**, not merely the preservation of the physical objects themselves.

4.12 Inaccessibility of data is not necessarily caused by the media and the data being damaged, but rather by a lack of ability to read the data content on the storage media. Technology changes so rapidly that the storage media outlast the software and devices needed to read the content on the storage medium. It is not adequate to focus on the physical storage requirements for preserving the media optimally. One could maintain the media perfectly, but there might be no way in which it could be accessed and read after the passage of time. 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.

4.13 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 the face of constantly changing technology. In order to preserve their integrity records must retain their reliability, completeness,

authenticity and context. To ensure this migration strategies should be built into the electronic system **during the design phase** of an electronic system.

4.14 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. Rather than choosing a single approach to migration the body should select appropriate migration options (see Annexure B) that take into account the need to protect the integrity of the records and the need to retain as much of the utility as possible. Certain formats of records are better suited for specific migration strategies. Furthermore, the adoption of internationally recognised data and document standards will simplify the migration process. It might be necessary to convert the data to standard formats to enable migration strategies to be put in place. [Consult the European Commissions' Open Information Interchange Services' *Standards and Specifications List* at http://158.169.50.95:10080/oii/en/oiistand.html]

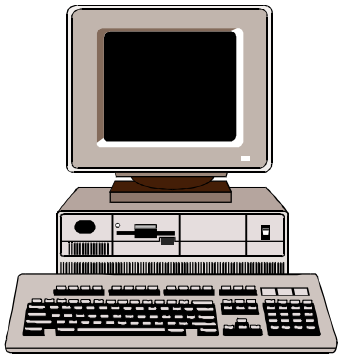
4.15 In order to prevent loss of information and loss of functionality and to ensure legal admissibility and validity for audit purposes a migration programme should involve:

- 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).

4.16 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. The National Archives' electronic records management strategy

While its practical experience in the field is still limited, the National Archives has adopted a strategy underpinned by a legal framework explicitly provided for in the new National Archives of South Africa Act (Act No. 43 of 1996). 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.

NASA's electronic records management programme is built on the following three-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 of South Africa Act allows the National Archives to insist that mechanisms and procedures be put in place to ensure that archival records are identified while still functional and then preserved appropriately.

- The earliest possible transfer into archival custody of electronic records with enduring value. In terms of the National Archives 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 of South Africa Act specifically empowers the National Archivist to make such an arrangement with creating bodies.

These legislative provisions are carried through into the published *Archives Instructions*, which specify the obligations of governmental bodies in terms of the National Archives of South Africa Act. In terms of the *Archives Instructions*, it is required that a Schedule for Electronic Records Systems be compiled as an instrument for obtaining disposal authority and use as a disposal schedule. The schedule requires certain basic information that will provide the National Archives with a general overview of a system's functions. (See Annexure C). As governmental bodies apply electronic systems differently, it is necessary to liaise with the National Archives on the precise manner of scheduling. Schedules for appraisal purposes can then be compiled according to the needs of a particular body.

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.

6. The management of electronic records

6.1 The responsibilities of governmental bodies

6.1.1 The heads of governmental bodies have to shape the electronic 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 policy is understood throughout the organisation.

6.1.2 Governmental bodies have to establish policies and procedures to ensure that electronic records and their documentation are retained as long as is appropriate. Governmental bodies should:

- Notify the National Archives beforehand, in writing of the intention to introduce electronic records management systems.

- Put an integrated electronic records management system in place that is compliant with the US DoD Standard *Design Criteria Standard for Electronic Records Management Software Applications* - US DoD 5015.2-STD (See Annexure A for details.)

- Apply for the appraisal of all electronic records, as well as related documentation and indexes. The information in electronic records systems, including those operated for a governmental body by a contractor, have to be scheduled as soon as possible, preferably before implementation of the system.

- Transfer a copy of the electronic records and any related documentation and indexes to the National Archives at the time

specified by the disposal authority. Transfer may take place at an earlier date if convenient for both the governmental body and the National Archives.

- Establish procedures for regular recopying, reformatting, and other necessary maintenance as well as for migration to new technologies to ensure the retention and usability of electronic records throughout their authorised life cycle.

- Erase electronic records only in accordance with a disposal authority approved by the National Archivist. This should be done in such a manner that ensures protection of any information requiring special security provisions.

6.1.3 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.

6.2 **Procedures to be followed by governmental bodies applying for disposal authority**

Even though the diversity and complexity of computer systems makes it impossible to provide a simple set of guidelines applicable to all systems, an office should follow the guidelines below when applying for disposal authority on electronic records:

6.2.1 The head of a governmental body must notify the National Archivist beforehand, in writing, of the intention of introducing electronic records systems.

6.2.2 Any item forming part of a system in an electronic records system must be preserved and cared for in such a manner as to ensure that they are not exposed to harm or unauthorised access and under such specific conditions as the National Archivist may prescribe.

6.2.3 No destruction, erasure or alienation of any data and related material may take place without the written approval of the National Archivist.

6.2.4 If a governmental body contemplates using an automated correspondence system, a functional subject classification system must be submitted to the National Archivist for approval in terms of article 13(2)(b)(i) of the National Archives of South Africa Act (No 43 of 1996) and for the issuing of disposal authority thereon. This classification system will determine which reference numbers will be allocated to documents and must be maintained just as an approved filing system for conventional paper records by the reporting of amendments and additions.

6.2.5 The same requirements as set out in paragraph 6.2.4 apply to a governmental body that wishes to use image processing on optical disks for the management of a correspondence system.

6.2.6 In order to manage electronic records not mentioned in paragraphs 6.2.4 and 6.2.5 efficiently and determine retention periods a governmental body must compile and maintain a Schedule of Electronic Records Systems (see Annexure C). For a governmental body's own management purposes, it is recommended that a comprehensive inventory of all electronic records systems be compiled according to the elements required in the Schedule of Electronic Records Systems. Such an inventory may already be in existence. The inventory can then be used as the basis for compiling the Schedule of Electronic Records Systems, by first applying the General Disposal Authorities for the disposal of ephemeral electronic

and related records (Annexure D) and transitory records (Annexure E). the general disposal authorities authorize the destruction or erasure of certain categories of electronic records that doe not have archival value.

6.2.6.1 The precise manner of how electronic records should be scheduled can be negotiated with the National Archives. In some cases it may only be necessary to provide an explanation of the purpose of the system and the technology used. The information in each system should, be described in comprehensive fashion. Descriptions 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. (A list of elements that should be included in a complete and accurate description for a schedule, can be found in Annexure C.)

6.2.6.2 A Schedule of Electronic Records Systems normally consists of a separate description for each system.

6.2.6.4 A disposal authority is not normally issued on particular components of a system separately, but rather on all the components of a system as a whole.

6.2.6.5 The described system(s) constitute the Schedule of Electronic Records Systems and must be submitted to the National Archivist for the issuing of disposal authority thereon. (See the attachment to Annexure C for a list of possible disposal instructions for electronic records.)

6.2.7 Any item forming part of a system which qualifies for permanent preservation in terms of a disposal authority issued by the National Archivist is kept in custody by the office of origin (under such specified

conditions as the National Archivist may prescribe) until it is transferred to the repository indicated by the National Archivist. The National Archivist determines the period after which transfer should take place, and it may be shortened or lengthened in consultation with him/her.

6.2.8 As far as original documents that were image processed are concerned, the National Archivist will determine beforehand if the information should be transferred in paper form, micrographic form or in suitable electronic form.

6.2.9 If another Act of Parliament contains provisions with regard to the creation and/or preservation of electronic records, the requirements as set out in this section are still applicable.

6.3 Guidelines for the appraisal of electronic records

6.3.1 Electronic records are subject to the same requirements provided in the National Archives of South Africa Act that apply to other records.

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

6.3.3 Where electronic records have archival value, it is first established whether the records can be transferred to archival custody in a proven archival medium such as paper or microform.

6.3.4 The possibility of the office of origin being required to preserve the electronic records and maintain their functionality permanently is always considered.

6.3.5 Only if the options in paragraphs 6.2.3 and 6.2.4 do not apply are

electronic records considered for archival custody.

6.3.6 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.).

6.3.7 In identifying archival value in electronic records systems, the same theoretical and methodological framework is applied as for all other media.

6.3.7.1 Public records worthy of permanent preservation are identified by following a research-based, government wide, strategically planned and top-down appraisal methodology. This methodology, with the purpose of identifying for acquisition the richest of public records, is termed *macro-appraisal*. It consists of dealing with disposal authority applications submitted by governmental bodies and the issuing of disposal authorities on those applications.

6.3.7.2 The macro-appraisal methodology followed consists of three components, namely a contextual analysis, an appraisal hypothesis and the records appraisal.

- Contextual analysis: In the contextual analysis the contextual milieu in which the records were/are being/will be created, is identified. It includes a complete analysis of the governmental body and its functions. It explains how the governmental body is positioned in government and describes and assesses the functions of the governmental body, the internal structure of the governmental body and the importance of all the office's records

systems - what systems are in use? how do they relate to each other and the office's structure and functions? where do/does the records/records system(s) to be appraised fit into this picture?

- Appraisal hypothesis: Drawing on the research conducted during the contextual analysis, the archivist forms a hypothesis concerning the overall importance/value of the records/records systems(s) being appraised and concerning which of the records in particular have archival value.

The appraisal hypothesis connects the records to the milieu in which they were created - how do they reflect this milieu? what is their overall importance as a documentary reflection of this milieu? which of the records in particular promise to provide the richest, most focused evidence of the milieu?

- Records appraisal: In the records appraisal the hypothesis is tested by detailed analysis of the records. The records are subjected to the tests of age, uniqueness, authenticity, completeness, extent, fragility, manipulability, etc.

6.3.8 Given the unique medium being appraised, the following factors are considered:

6.3.8.1 Electronic media offer huge storage capacity and the facility to manipulate data for secondary purposes using powerful retrieval processing tools. The potential therefore exists that records documenting a particular function in electronic format may be accepted for preservation, despite similar records in paper format being rejected. E.g. the electronic version of the personal staff file may be preserved, while similar paper based files are rejected because of their physical volume and lack of manipulability of the

information they contain for secondary analysis.

6.3.8.2 The use of electronic records is dependent upon hardware and software. It is not viable to preserve all relevant hardware and software in an archival environment, particularly as it rapidly becomes obsolescent. It is, however, necessary to ensure that the functionality of an electronic records system appraised as having archival value can be recreated in the archival environment. As part of the appraisal process, the archivist determines the most appropriate means of preserving functionality. In some cases data is acquired in software independent form, together with full documentation specifying inter alia record layout, codes, etc. In other cases, e.g. relational databases, it may be necessary to acquire the software as well.

6.3.8.3 In cases in which the preservation of functionality is not feasible or desirable because of e.g. software dependence or the originating office being better placed to provide user services, preservation in the originating office rather than an archival repository is considered.

6.3.9 Where more than one medium is involved in a particular system, appraisal needs to take all the media into account so that the disposal authority encompasses all the media. In the case of image processing, disposal authority for the original documents as well as the electronic version should be requested.

6.3.10 Where correspondence systems are maintained in electronic form, the use of an approved classification system to allocate reference numbers to individual electronic records is a prerequisite for appraisal. Such a classification system facilitates retrieval in context. A standing disposal authority is issued on the classification system to allow for the erasure or destruction of ephemeral records, both in paper and electronic media. The National Archives decides on the appropriate medium or format in which records are preserved for archival

purposes.

6.3.11 Open reel or cassette magnetic tapes as well as CD-WORM and DVD-WORM can serve as storage media. However, due to a lack of proper equipment and funds the National Archives is not in a position to take electronic records stored on optical storage media into custody. Neither is the National Archives able to maintain such records or to make them available to the public for research purposes. The onus will rest with the office concerned to preserve and migrate the electronic records at its own cost as technology changes and to make the available for research purposes.

6.3.12 In the case of databases and websites that are continually updated and amended, the National Archives will consider the possibility of obtaining “snapshots” at specific intervals.

6.3.13 When electronic records are recommended for preservation, care should be taken to ensure that the appropriate *metadata* is identified, documented, and transferred into archival custody together with the electronic records. Metadata is 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. Metadata is essential in transforming raw data into records because it provides the means to make sense of the data. 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, its extent and use as well as records formats and other information needed to recreate it. A transfer list in which individual cassettes and their contents are specified is also required.

6.3.14 There may be cases in which electronic records, that have been

appraised as having archival value, would best be preserved in the office of origin, rather than being transferred to archival custody. The following are examples of categories of electronic records, which may be more appropriately preserved in the office of origin.

- Cumulative, longitudinal systems and records, where by definition no data deletion, erasure or replacement occurs.

- Bibliographic or cataloguing systems or records, where the first point of access would never be an archives repository because the latter would only hold an incomplete version of the system.

- Data where the creating institution has as its own operational requirement the provision of extensive and elaborate reference services, and has the willingness to provide such services in a manner that an archives repository could not match.

- Cases where it is not technically feasible or cost effective to provide a version of the record for archival custody.

- Data where institutions for whatever reasons (security, sensitivity) refuse to transfer the record to archival custody, at least until the expiry of a lengthy retention period. This situation cannot be supported unless one of the other circumstances noted above is also present.

6.3.15 Electronic records which are deemed to be of archival value but which would be best preserved by the office of origin, remain at all times subject to the National Archives of South Africa Act. They must be registered with the National Archives even while they remain in custody of the governmental body.

6.3.15.1 The responsibilities of the National Archives towards these records

also remain the same; i.e. they are to be registered and described in the National Archives' control systems, and they remain subject to the normal public access control procedures of the National Archives of South Africa Act.

6.3.15.2 Governmental bodies also have to put into place management, storage and preservation regimes for the records remaining in their physical possession which go beyond those required for normal business or operational purposes.

6.3.15.3 Electronic records of enduring value which are retained in the physical possession of a governmental body (this includes outsourced systems management) must be protected from alteration or destruction, including anything which would render them inaccessible.

6.3.15.4 In order to ensure that electronic records kept in a governmental body remain genuinely accessible over the time they are required to be kept, they must be migrated across any changes in technology, media or application development and review which may occur during that time. Physical formats on which electronic records may be kept change with great rapidity. They can change in their physical dimensions so that later versions no longer fit earlier machinery, and vice versa. Changes like this can mean that electronic records, which have been kept on older physical formats of media, may become unusable when an upgrade of equipment or machinery occurs, although they might still be in quite good condition for their original purpose. A migration path for transferring such electronic records of enduring value to the newer physical formats should be developed as an integral part of the upgrade project planning. (See Annexure B for Migration Strategies)

6.3.15.5 When records of enduring value are retained in the physical possession of a governmental body, they must at all times be

incorporated into the disaster recovery procedures that the governmental body maintains for its operational computer systems.

6.3.15.6 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 in accordance with the National Archives of South Africa Act.

6.3.15.7 When electronic records of enduring value are retained in the physical possession of a governmental body, the National Archives will audit the extent to which such records are being kept in an accessible state. Subject to certain exceptions, the National Archives 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 will seek the assistance of appropriate governmental body staff to ensure that higher value 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.

6.4 Preservation of electronic records

6.4.1 Transfer of archival electronic records to the National Archives

6.4.1.1 Where a disposal authority requires the deposit of specific electronic records in the National Archives, governmental bodies are encouraged to make such a transfer as soon as possible, because of the short life expectancy of storage media. These electronic records are maintained permanently by the National Archives for subsequent use by the original body, other bodies, other organisations, researchers, and the general public. The National Archives generally satisfies such requests by

providing copies of files.

6.4.1.2 Like other secondary users of computer data, the National Archives requires certain documentation (metadata) to accompany computer files. Technical documentation of the records, sufficient to support their use for secondary analysis, must accompany the tape. (Metadata is described in section 6.3.13.) The National Archives also needs specific information on how the tape 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.

6.4.1.3 Before transferring electronic records to the National Archives it is necessary for a governmental body to arrange for the transfer with the National Archives. Any transfer problems can then be resolved beforehand.

6.4.1.4 If records are identified as archival, the National Archives will specify certain requirements regarding the format of the records. If the technology is too advanced for the National Archives 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.

6.4.2 Maintenance of electronic records

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 labelling, indexing, and preservation actions are necessary to ensure that electronic records are available and accessible throughout their useful life.

6.4.2.1 Labelling and indexing electronic records

6.4.2.1.1 Labels are essential to identify electronic media. Labels on a diskette's jacket (external labels) should include the originating office symbol, 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.

6.4.2.1.2 Document, file, and directory naming conventions (internal labels) should be easily understandable and standardised so that authors and their colleagues or successors can find and use information stored on disks or tapes. Naming conventions are particularly useful when several people share a computer with a hard disk if the disk has not been partitioned into individual work directories.

6.4.2.1.3 Labelling, naming, and filing conventions should be simple. One effective system is to file similar documents in the same place (on the same labelled floppy or in the same directory on a hard disk). This avoids the necessity of rummaging through a drawer full of diskettes or searching through multiple directories on a hard disk to find needed documents.

6.4.2.1.4 Indexing is a more complicated way to find electronic documents if a classification system is not used. An indexing system should require the document creator to indicate the name of the document, the addressee, the date, and the identifier of the disk on which it is stored. An abstract of the document may also be useful. The index can be printed out, or stored on cards or in a data base management system on a labelled diskette. The need to establish a formal, office-wide system for filing, labelling, and naming electronic records depends on

how the information is used. Such a system is essential if the office plans to maintain records solely in electronic form, without converting the information to paper or microforms. If there is a high turnover of personnel, or if information is shared or routed electronically, a formal system may be particularly advantageous. If information is shared on paper, however, minimal identifying information should be sufficient.

6.4.2.2 Physical requirements for the preservation of electronic records

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 permanent are maintained in decentralised locations. Par. 6.4.2.2.1 contains general maintenance suggestions for all electronic records, while Annexures F and G contain comprehensive guidelines on handling magnetic and optical media.

6.4.2.2.1 General maintenance guidelines

6.4.2.2.1.1 Back up the files and documents on disks often. This is the single most important action users can take to ensure that the information they need will be available. Central computer facility staffs periodically perform systemwide backups. When users share a microcomputer, or have one on their desks, they must be encouraged to back up their files, preferably after every update. Keep a backup on the other side of a firewall or in an offsite location.

6.4.2.2.1.2 Prohibit the use of diskettes for the exclusive long-term storage of permanent records. Temporary storage of permanent records on diskettes is acceptable, as is the use of them for reference purposes.

Experience shows, however, that careless handling is much more likely with this medium than with magnetic tape, which is the recommended storage medium for permanent records.

6.4.2.2.1.3 Do not allow unauthorised persons to have access to the computer or disk or tape files and documents. Even persons with good intentions can enter commands that will delete files or reformat hard disks.

6.4.2.2.1.4 Tapes should be labelled with reference numbers allocated according to a naming convention, documented in a register, and stored in sequence.

6.4.2.2.1.5 Annually read a statistical sample of all data sets stored on magnetic tape and optical media to detect any loss of data.

6.4.2.2.1.6 Copy data on the tapes to new or recertified tapes at least once every 5-10 years and data on optical storage media more frequently when to prevent the physical loss of data or technological obsolescence of the medium.

6.5 Managing e-mail messages

6.5.1 E-mail messages are records

The National Archives of South Africa Act (Act No. 43 of 1996) 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 by governmental bodies and which are kept as evidence of a governmental body’s functions, activities and transactions.

E-mail can be a form of official communication. 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.

6.5.2 How should e-mail be managed?

E-mail records should be managed according to the basic principles that apply to records in any medium. The management and retention

of e-mail records are subject to the National Archives of South Africa Act (Act No. 43 of 1996), and its regulations.

Records management policies determined by governmental bodies 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. A policy should also explain how the governmental body would implement a records management programme that includes e-mail records. For example, the policy should specify where official records will be kept, such as in a central repository associated with a departmental network or LAN or in decentralized electronic or paper-based filing systems. Governmental bodies should inform end users about policies for security, backup and purging to protect records from alteration, loss, or inappropriate destruction.

6.5.3 Records retention and disposal authority

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.

Where classifications systems with disposal authorities already exist, governmental bodies should file the e-mail records into these systems. The retention periods of the e-mail records will then be the same as that of the specific file. However, if there is no disposal authority on a filing system or electronic classification system, the governmental body should contact the National Archives to obtain one.

6.5.4 Preservation as records

Strategies for managing and preserving electronic messages as records will differ, depending on the specific environment within a governmental body.

There are two basic options for filing and managing e-mail records:

- print messages and file them in paper-based filing systems, or
- transfer e-mail messages to an electronic classification system or repository.

The method chosen will depend on whether the office has a paper-based filing system, or an electronic records management system or both, in place.

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.

Furthermore, both the paper-based and the electronic records management system must ensure that:

- related records are grouped together in accordance with the office's classification system;
- the records are accessible to authorized persons;
- the retention of the records is supported for as long as they are required;
- destruction of records can take place when so scheduled; and
- permanent preservation of archivally valuable records is supported.

When preserving electronic messages, the following specific requirements should also 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 intent 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.

ANNEXURE A

Baseline requirements for an integrated electronic records management system

Integrated electronic records management systems compliant with the US DoD 5015.2 standard support the following:

- Physical storage of 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/ juke boxes, etc. or in separate storage area networks. Whichever method 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.

- Classification system management. Without a proper classification system 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 financial implications. Without a disposal authority in place all electronic records created will have to be migrated across changes in technology to enable them to be readable over a long period of time.

Proper classification system management requires that there should be strict control over making additions to the directory structure or deleting folders from the structure. If folders are added randomly without proper consideration, folders can be added for existing subjects. This can cause confusion when documents are classified. 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 classification system/ directory structure is a function that should only be allocated to the records manager/systems administrator.

- Document filing. In a paper-based filing system documents are filed on 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 classification system in the repository. Without this, there will be no records to manage. In most governmental bodies staff tend not to file records, even in paper-based form. To enable them to buy into filing electronic records is a great challenge. Filing documents should be extremely fast, simple and non-intrusive.

  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 classification system 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 classification system 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 classification system, and assigning the subject identifier to a specific document. This way all documents are associated with a subject in the classification system.

This 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.

The following should also be considered:

- Classification is required in order for disposal instructions and retention periods to be allocated;
- Classification 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 filing 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 the records management application. 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 filing 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 to be recorded. This will enable the users to find both the electronic and paper-based documents on a 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.

- Retention and disposal. Destruction is not applied to individual documents. Sound records management call for destruction on a file level. The disposal instructions and retention periods are applied to each subject file within the classification system. This means that all documents within that subject file carry the same disposal authority and retention period. It also means that the disposal instruction and retention period apply to both the paper-based and

the electronic records of that 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 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 records management software should 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.

- 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 versions 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.

  The appropriate way to do version control is to keep draft versions of documents on the user's desktops and only to file final versions into the repository. Editing of final versions should not be allowed.

  Where it is appropriate to retain various versions of a document 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 it as new records.

- Archiving. 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.

- Quality Assurance. Because of the inherent volatility of electronic records and the larger role played by end users the records manager should play a 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 are staff who need assistance/training in classification techniques.

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

- Security. The records management software is designed to make records easily accessible. However, there is always a need to protect some sensitive records from unauthorised access. A system of security levels should be built into the system. The user can assign security levels to each document to enable only users with the right clearance to access documents.

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

  Records management software that is chosen should preferably also include paper management futures to allow for integrated records management. The following features are examples of paper management futures:

  - File tracking, labelling, destruction and transfer
  - Boxing of paper records
  - Charge-out/in file management
  - Bar coding

- Filing e-mail records. Users must file e-mail messages to the classification system 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 preserve the transfer data (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.

ANNEXURE B

Migration Strategies

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 • ransfer to film or paper eliminates the pro-blems 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 'soft-ware independent' format: This strategy involves trans-ferring 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, hyper-text).

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 hardware 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 standpoint.	• 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

Schedule of Electronic Records Systems

A. General remarks

1. Electronic records are subject to the same requirements provided in the National Archives of South Africa Act (Act No. 43 of 1996) that apply to other records.

2. The Schedule of Electronic Records Systems is a way in which a governmental body describes its electronic records systems so that the archival value of the records in the systems can be determined. Records systems covered in whole by the General Disposal Authorities on electronic and related records and on transitory records should be described only in terms of paragraphs 1, 2, 3, 6 and 11 of the example given below.

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

4. 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.)

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

6. 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.

7. The schedule must be compiled in duplicate.

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

9. Systems should be numbered consecutively.

10. The information required should be given in detail.

B. Information that should be included in an electronic records schedule

A complete and accurate description of all a governmental body's electronic recordkeeping systems should include the elements indicated below.

1. Name of the system: Indicate the commonly used name and acronym of the system.

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

3. Governmental body's programme supported by the system: Show the governmental body's programme(s) or mission(s) to which the system relates.

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

5. 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.

6. Purpose of the system: Indicate the reasons for the system and the requirements met by it.

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

8. 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.

9. 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 microdata or summary data.

10. Location of documentation (metadata see par 6.3.13) needed to read and understand the files: Show 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. 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.

11. 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 attached list 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.

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

C. Disposal Instructions: Electronic Records

It is important to note that the National Archives, 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 instructions, A (representing “archival”) and D (representing “not archival”), with variations determined by retention period. For instance, A1 means transfer to the National Archives 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. 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 of Electronic Records System

DEPARTMENT OF FISHERIES

1. **System name:**
   Documentary System (DOCS)

2. **System control number:**
   FISH2

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

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

5. **Responsible personnel**

Ms B Bass
Information Systems
Room 101
(012) 328 5738 x 346
bass@fish.pwv.gov.za

Mr. FC du Toit
Directorate Administration
Room 311
(012) 328 1369 x 301
toit1@fish.pwv.gov.za

6. **Purpose of the system**

The system supports internal communication within the Department of Fisheries. The system is used to disseminate information concerning a variety of topics including circulars, regulations and laws.

The system provides the following functionality:

The storage of documents of interest to members of the Department of Fisheries

Enquiries against the document database to identify relevant documents.

The browsing and printing of identified documents.

Printing of reports.

Printing of statistics and management information concerning documents used by the Department of Fisheries.

7. **Data input and sources:**

Information gathered through questionnaires, telephone surveys, reporting forms, etc.

All legal and/or official documents regarding the Department, its activities and functions, created by the Department.

Relevant information is also received from several wildlife organisations, universities and similar departments in foreign countries.

Information from the Weather Bureau.

8. **Major output:**

Quarterly and annual reports.

Reports/articles regarding related topics.
Information is sporadically exchanged with similar bodies in other countries.

9. **Information content:**

Legal and/or official documents regarding the Department, its activities and functions.
Relevant information regarding ichthyology, the fishing industry, halieutics, weather patterns, etc.

Date coverage, time span: 1980 - present

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

Update cycle: Every two weeks

10. **Location of documentation (metadata) needed to read and understand the files:**

Codebooks and file layouts are maintained by the Information Systems Division of the Department of Fisheries.

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.

11. **Disposal authority:**

Correspondence filing system: 2-S1NA

Additional information on file 13/2/1/4.

12. **Date prepared:**

1998-07-14

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 of South Africa Act to erase or destroy ephemeral electronic and related records of all governmental bodies when no longer needed.

2. 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 sound records management systems to be in place. This is in fact a requirement in terms of the National Archives of South Africa Act (No. 43 of 1996), section 13(2).

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. 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 (Act No 2 of

2000).

3. Descriptions

3.1 Word Processing Files

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

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

3.1.2 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 authorised for destruction in terms of this disposal authority or another disposal authority issued by NASA.

3.2 Administrative Data Bases

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 authorised for destruction by this disposal authority or another disposal authority issued by NASA, if the hard copy records are maintained in a NASA-approved classification system. Hard copy printouts from these databases that are made for short-term administrative purposes.

3.3 Schedule 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:

3.3.1 Records determined to be personal.

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

3.3.3 All records kept at ministerial level.

3.4 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 authorised for destruction by this disposal authority or another disposal authority issued by NASA.

3.5 Finding Aids (or indexes)

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

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

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

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

3.6.3 Electronic files and hard-copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to access charges for system use.

3.7 Input/Source Records

3.7.1 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 NASA.

3.7.2 Electronic records, except as indicated in 3.7.3 below, entered into the system during an update process and not required for audit or legal purposes.

3.7.3 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.

3.7.4 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.

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

3.8.1 Master files that replace, in whole or in part, administrative records scheduled for destruction in a disposal authority approved by NASA.

3.8.2 Master files that duplicate, in whole or in part, administrative records scheduled for destruction in a disposal authority approved by NASA.

3.9 Data Files consisting of summarised information

Records that contain summarised 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 NASA, 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 NASA approval.

3.10 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 NASA, 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 NASA approval.

3.11 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.

3.12 Technical Reformat Files

Electronic files consisting of data copied from master files or databases for the specific purpose of information interchange and written with varying technical specifications, EXCLUDING files created for transfer to NASA.

3.13 Security Backup 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 of inadvertently erased.

3.13.1 Files identical to records scheduled for transfer to NASA.

3.13.2 Files identical to records authorised for destruction in a disposal authority approved by NASA.

3.14 Special Purpose Programmes

Application software necessary solely to use or maintain a master file or data base authorised for destruction in a disposal authority issued by NASA, 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 NASA or are scheduled for transfer to NASA in terms of a disposal authority.

3.15 Documentation regarding electronic systems

Data systems specifications, file specifications, codebooks, record layouts, user guides, output specifications, and final reports (regardless of medium) relating to a master file or data base that has been authorised for destruction in a disposal authority issued by NASA, EXCLUDING documentation relating to any master file or data base for which disposal authority has not yet been obtained from NASA or are scheduled for transfer to NASA 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 of South Africa Act No. 43 of 1996) to destroy Transitory Records.

2. 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.

3. Guidelines for the Identification of Transitory Records

3.1 Conventional paper based records

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 version, 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.

3.2 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:

3.2.1 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 backup 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.

3.2.2 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.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 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.

3.2.7 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 hardcopy files.

- Working copies of 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.

3.3 Photographic records

Photographic records that are transitory may include:

- process photography, containing negatives created solely as an

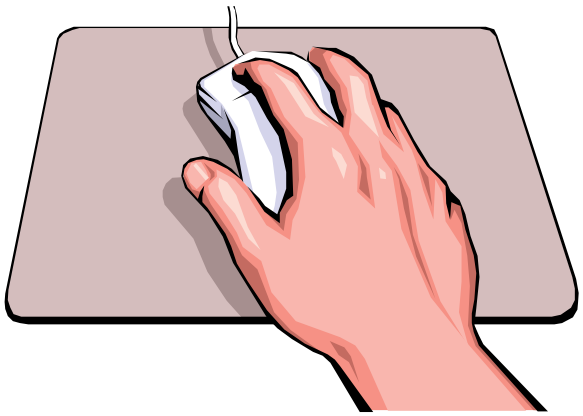
intermediate stage in printing operations, and where such negatives are used to create lithographic or photo off-set plates; and

- outs, containing photographs that 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.

3.4 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 tape, including audio cassettes and reel-to-reel tapes, videotapes, computer tapes both on open reels and in cassettes, and tapes used in digital recording processes such as DAT
- magnetic hard disks
- RAID's (i.e Redundant Arrays of independent hard disks)
- magnetic floppy disks or diskettes.

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 on 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 which 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 which 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 part-way 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 which 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 which 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 which 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 which 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. Carpet 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 which 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 minimise 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 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 acclimatise 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 minimise 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 audio tapes) 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 minimise 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 Disk (CD)** 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 (DVD)** which is basically a 2nd generation high density compact disk that also consist of ROM, WORM and Rewritable versions. DVD drivers are backwards compatible to enable them to read CD's

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 which 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 gold metallic layer, which cannot corrode, rather than aluminum.

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 labeled 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 which 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 localised 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 disk 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

Glossary

Act

The National Archives of South Africa Act (Act No. 43 of 1996).

Appraisal

The process of determining the value and thus the final disposal of records, making them either ephemeral (temporary value) or archival (permanent value).

Archival value

This refers to the long-term use records may have for purposes other than functional use.

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 stores; or
d) A group of records belonging to a specific office.

Archives

Records in the custody of an archives repository.

Archives Repository

The building in which A20 records, i.e. 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

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)

Classification system

A classification plan for the identification, arrangement, storage and retrieval of records.

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.

Disposal

This is the action taken when a body transfers A20 records to an archives repository or records centre and destroys D records.

Disposal authority

A written authorisation specifying records to be transferred into the custody of the National Archives or specifying records to be otherwise disposed of.

Disposal symbols

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.

Electronic document management system:

A computerised environment which enables the creation, capture, organisation, storage, retrieval, manipulation and controlled circulation of documents in an electronic 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

Any records system in which information is generated electronically and stored by means of computer technology.

Electronic records management system:

See Records Management Applications

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 where the programme needed to access the content of the disk is recorded on the disk itself.

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.

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.

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.

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.

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.

Public records

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

Record

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).

Records classification system

A classification plan for the identification, arrangement, storage and retrieval of records. This includes filing systems for conventional paper records as well as classification systems for electronic records and the Records control schedule.

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.

Records management application

Software used by an organization to manage its records. Its primary management functions are categorizing and locating records and identifying records that are due for disposal. RMA software also stores, retrieves and disposes of the electronic records that are stored in its repository.

Records other than correspondence files

Records that do not form part of a filing system for conventional paper records or case files of an office, e.g. minutes, registers, microfilms, electronic records, etc.

Repository for electronic records

A direct access device on which the electronic records and metadata are stored.

Retention periods

The length of time, usually based upon an estimate of the frequency of current and future use, that records should be retained in offices before they are either transferred to a repository or destroyed. As far as ephemeral records are concerned the head of the office decides on the retention periods in accordance with the administrative use of the records. In the case of archival records the Act determines that such records must normally be kept for twenty years after the end of the year in which they were created, before they are transferred.

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

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.

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.

ANNEXURE I

Bibliography

Aeon Archive Limited: *High tech Solutions for the archiving and preservation of Optical Data Storage Media* [http://www.aeon-archive.com]

Disa, *Joint Interoperability Test Command: Records Management Application (RMA) Certification Testing.* [http://jitc.fhu.disa.mil/recmgt/index.htm]

Breeding, M.: *Network Design Manual. Storage for the network: Designing an effective strategy* [http://www.nwc.com]

Burke, B.: Special Report SAN. High performance shared Storage Area Networks. [http://www.westworldproductions.com]

Dean, J.: *Managing Technology Column: Data roundup* [http://www.storage.ibm.com]

Harris, V.S.: *Exploring Archives: An introduction to archival ideas and practice in South Africa.* Pretoria, 1997.

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]

Fast, S.: *The birth of network-attached storage.* [http://www.planetit.com]

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]

Miller, B.: *Managing Electronic Records. It can be done*. [http://www.provsys.com]

National Archives and Records Administration: *Managing Electronic Records*. Washington, 1990. [http://www.nara.gov]

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 respons-ibility*. 1997. [http://www.naa.gov.au]

National Archives of Canada*: Managing Electronic Records in an Electronic Work Environment*. May 1996. [http://archives.ca]

National Archives of South Africa: *Appraisal Manual*. Pretoria, September 1996

National Archives of South Africa: *Archives Instructions*. January 1999.

National Archives of South Africa: *Registry Guide*. Pretoria, May 1998.

National Archives of South Africa: *Directive D8. Prototype Control Schedule for Local Authorities*. Pretoria, February 1999.

National Archives of South Africa*: Directive D10. General disposal authority number AT2 for the destruction of transitory records of all government bodies.* Pretoria, July 1998.

National Archives 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.

Orlandi, J.: *How to painlessly add storage.* [http://www.westworldproductions.com]

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.

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.

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.

Vasudeva, A.: Special Report SAN. SAS, NAS, SAN - Past, Present and Future. [http://www.westworldproductions.com]

FURTHER INFORMATION

Further guidance on the management of electronic records can be obtained from:

The Records Management Division
National Archives of South Africa
Private Bag X236
Pretoria
0001

Tel: (012) 3235300
Fax: (012) 3235287
E-mail: arg16@dacst4.pwv.gov.za