FUNCTIONAL SPECIFICATION FOR INTEGRATED DOCUMENT AND RECORDS MANAGEMENT SOLUTIONS

APRIL 2004

National Archives and Records Service of South Africa
Department of Arts and Culture

draft

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

Version 1, April 2004

The information contained in this publication was, with the kind permission of the UK National Archives, for the most part derived from their *Functional Requirements for Electronic Records Management Systems* {http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/}

CONTENT

1. INTRODUCTION

The National Archives and Records Service endorses the SANS (ISO) 15489 Records Management Standard as the required standard for records management and, in terms of its statutory mandate as set out in sections 13(2)(b)(ii) and (iii) of the National Archives and Records Service of South Africa Act, 1996, requires governmental bodies to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner. To this end the National Archives and Records Service requires a governmental body that wishes to implement electronic systems, to implement and maintain Integrated Document/Records Management Systems (IDRMS), which have built-in records management functionality. The National Archives and Records Service defines an Integrated Document/Records Management System (IDRMS) as a solution consisting of document management, records management, file/document tracking, integrated imaging and scanning, integrated workflow/routing and integrated search and retrieval functionality. The National Archives furthermore requires governmental bodies to implement and maintain approved file plans against which records in all formats can be classified *at creation.*

The attached functional specification for an Integrated Document and Records Management Solution was mainly derived from the UK National Archives' *Functional Requirements for Electronic Records Management Systems*. Information from the US DoD 5015.2 *Design Criteria Standard for Electronic Records Management Software Applications* and the European Commission's *Model requirements for the management of electronic records* were used where applicable. Due to the nature of the National Archives and Records Service's requirements the specifications could not be adopted verbatim. Where necessary the specific requirements were adapted to suit the South African archival legislative framework.

Flowing from the National Archives and Record's Service's requirements, basic document management functionality and file and document tracking functionality are considered core to the successful implementation of an IDRMS. The integrated imaging and scanning and integrated routing functionality are specified only in so far as they have an impact on the records management functionality and/or the usability of the solution. Issues relating to interoperability, integration, security and the systems design and technical architecture fall outside the scope of this specification. These issues should be addressed and clarified by the client offices as part of their normal tender processes.

The long term purpose of the specification is to provide a means of evaluating and certifying integrated document/records management functionality of a solution against the records management functionality required by the National Archives and Records Service in terms of its statutory mandate. However, until the necessary structures, processes and procedures are in place to do product

certification against this specification the NARS's requirement that a solution has proven records management functionality is still applicable. Products that are certified against UK National Archives' *Functional Requirements for Electronic Records Management Systems* and/or the US DoD 5015.2 *Design Criteria Standard for Electronic Records Management Software Applications* would for the time being be considered to possess the necessary proven records management functionality.

This specification could in the meantime be used

- by the NARS's client offices as a comprehensive specification that should be used in tender specifications;
- by software developers with a means to measure their product's compliance to the NARS's requirements, even if the products are US DoD and/or PRO certified, especially in those instances where the NARS's requirements differ from those of the UK National Archives and the US DoD. (E.g. A2.6, A2.27, A2.28, A3.1, A5.48).

In this document:
MUST means that the requirement is an absolute mandatory requirement.
MUST NOT means that the requirement is absolutely prohibited.
SHOULD means that if the requirement cannot be fulfilled out-of-the-box, some other means of fulfilling the requirement should be devised, e.g. by customization or by integrating with another product that can fulfill the functionality.
MAY means that the requirement is optional.

In the text a requirement that is mandatory is indicated with a (M), (HD) means a requirement is highly desirable and should preferably be provided and (D) means a requirement is desirable and that it would be beneficial if it is provided.

2. KEY TERMINOLOGY

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

Archive
a) A feature of document management systems, in which infrequently accessed documents are moved to off-line or near-line storage; or
b) A copy of data on disks, CD-ROM, magnetic tapes, etc., for long term storage and later access; or
c) The building in which archival records are stored; or
d) A group of records belonging to a specific office
e) 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 activity in the system can be documented as it occurs for identifying unauthorized actions in relation to the records, e.g. modification, deletion, or addition.

Authorized user
The Records Manager or the System Administrator or another user who was mandated by a policy to take certain actions against records in an Integrated Document and Records Management System.

Custodian
A person having responsibility for a particular set of records at a particular time, typically a case officer.

Declaration
The process of defining that a document and some of its metadata elements are frozen as it formally passes into corporate control and is thereby declared as a record.

Destruction
The process of eliminating records beyond any possible reconstruction.

Disposal
This is the action taken when a body transfers archival records to an archives repository or records centre and destroys/deletes non-archival records.

Disposal authority
A written authorization specifying records to be transferred into the custody of the National Archives and Records Service or specifying records to be otherwise disposed of.

Disposal instructions
Symbols indicating the type of action that should be taken with records. Two symbols (with certain variations thereof) can be found, namely A and D. A refers to the transfer of archival records to an appropriate archives repository for permanent preservation, usually twenty years after creation, or at such time as specified by the National Archivist. D refers to records with no archival value that need not be transferred to the National Archives and Records Service.

Disposal Schedule
- A set of instructions allocated to a folder to determine the length of time for which the folder should be retained by the organization for business purposes, and the eventual fate of the folder on completion of this period of time
- A set of instructions allocated to a document/record type to determine the length of time for which document and/or records of that type should be retained by the organization for business purposes, and the eventual fate of the documents or records of that type on completion of this period of time

Document
Recorded information or object which can be treated as a unit. A document may be carried on any medium and be of any type. A single document can consist of more that one component.

Document Management System
A set of methods and technologies consisting of messaging & calendaring, imaging & scanning, file/document tracking, electronic document management, electronic records management, workflow and search & retrieval functionalities, used to manage the classification, location, movement, security, auditing, retention, and disposal of an organization's paper-based and electronic documents.

Document type
See Record type

Electronic document
A document which is in electronic form. This includes not only text-based documents, but e-mail messages, spreadsheets, graphics and images, html/xml documents, multimedia documents and other type of documents.

Electronic document management system
A computerized environment which enables the creation, capture, organization, storage, retrieval, manipulation and controlled circulation of documents regardless of specific format.

Electronic folder
A set of related electronic records. Sometimes used in context to mean volume.

E-mail
A general term covering the electronic transmission, or distribution, of messages. Also called e-mail.

Electronic records
An electronic document which has been declared as a corporate record.

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

Electronic Records Management system (ERMS)
A system that supports the medium to long term information needs of an office. It provides functionality over and above that of an electronic document management system to preserve the security, authenticity and integrity of records to enable the permanent preservation of records. Its primary management functions are –

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

Element
An individual metadata attribute applied to an object.

Extract
An *extract* is a copy of a record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released to a requester, for example under PAIA, but part of the record can. An extract of

a whole folder is made by creating extracts from some or all of the records which the folder contains.

File plan:
The full set of series, and the folders which are allocated to them, together make up a file plan. The file plan is a full representation of the business of the organization, within a structure which is best suited to support the conduct of that business and meet records management needs.

Folder
An electronic folder is a (virtual) container for records (which may be segmented by volume). Folders are allocated to a series. A folder is the primary unit of management, and is constituted of metadata. Some of this metadata may be inherited from the series to which the folder belongs; and some may be inherited by the records which the folder itself contains. Where this term is used in isolation, it refers to both electronic folders and paper folders (as the latter are represented in the system). Otherwise, it is used only when qualified, e.g. *electronic folder*, *physical folder* to refer to that specific type of folder.

Format
The shape, size, style and general makeup of a particular record.

Hybrid folder
A set of related electronic and non-electronic *records,* some stored in an electronic *folder* within the system and some in a non-electronic *folder* (typically, a *physical folder*) outside the system.. Both electronic and non-electronic elements of the hybrid folder must be managed as one entity.

Hybrid volume
A set of related electronic and non-electronic *records,* some stored in an electronic *volume* within the system and some in a non-electronic *volume* (typically, a *physical volume*) outside the system. Both electronic and non-electronic elements of the hybrid folder must be managed
as one entity.

Inheritance
Principle by which an object can take on a metadata attribute of its 'parent' entity, either by *Inheritance on creation* where the subordinate (or 'child') object takes the value of that attribute when it is created; or by *Retrospective inheritance* where either the attribute of the parent object is changed or the parent object is altered (e.g. by moving a folder in the file plan so that it has a new parent object).

Integrated document management system
A document management system that is seamlessly integrated with the electronic records management application in such a way that it is not possible to

ascertain what functionality belongs to the document management system and which to the records management system.

Marker
Metadata which describes attributes of a *record* which is stored externally to the system (for example, large paper documents such as building plans, a database held outside the ERMS, a record on a CD-Rom).

Metadata
Background and technical information regarding the information stored electronically.

Migration
The process of moving records from one technological platform to another, to refresh software or media formats, while maintaining their authenticity, integrity, reliability and usability.

Open source software
Software that is developed, tested, or improved through public collaboration and distributed with the idea that it must be shared with others, ensuring open future collaboration.

PAIA
The Promotion of Access to Information Act, (Act N0 2 of 2000)

PAJA
The Promotion of Administrative Justice Act, (Act N0 2 of 2000)

Permanent preservation
The process by which *records* are preserved in perpetuity in the national archive, in an accessible and reliable form and maintaining them as authentic records, reflecting their business context and use.

Physical folder
A physical folder is an entry within the file plan for a legacy physical, usually paper, folder. The folder is not itself held within the system, but is located elsewhere. There are two types of cases in which a physical folder is represented:

- where the physical folder stands on it own, and has no relationship with an electronic folder, other than being allocated the same classification in the file plan
- where the physical folder is the physical equivalent of an electronic folder, and has the same title; the physical and electronic folder together constitute a hybrid folder.

Platform
The underlying software used by a system and the hardware making up the computer.

Pointer
Method of controlling instances of electronic records classified against more than one folder, without physical duplication of the document. More than one pointer can be created within the file plan to reference a single database object, but each must be logically managed as though separate records for disposal.

Presentation
Process of publishing records, folders and their metadata from the ERMS for 'presentation' outside the ERMS environment (e.g. for publication on a website) by methods within ERMS control.

Protective marking
Designations applied to a *record* to show the degree of security that it should be afforded. One of several words and/or phrases taken from controlled lists, which indicate the access controls applicable to a record. A.k.a security classification

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).
- Evidence of a transaction, preserved for the evidential information it contains.

Record type
A definition of a record object which specifies particular metadata attributes and particular forms of behavior. A default record type is the norm, specific record types are deviations from the norm. Specifically, this concept is used to enable different disposal behavior of records created as instances of a limited number of pre-defined record types. This concept can also be used to enable protection of privacy and to mark records for access to information reasons.

Repository
An electronic device on which the electronic records and metadata are stored.

Retention periods
- The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted. As far as non-archival records are concerned the head of the office decides on the retention periods in accordance with the administrative use of the records and the legal obligations the records need to fulfill. In the case of archival records the National Archives of South Africa Act, 1996 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 into archival custody.

- In an electronic document management system, the length of time a record is kept online before it is moved to near-line or off-line storage.

Rendition
Instance of a record rendered into another software format by a process entirely within the control of the ERMS, without loss of content. The content and most of the metadata (i.e. all except the relational linking back to the native format record and details of the software format) are identical. Renditions may be required for preservation or access/viewing purposes.

Review
The examination of the disposal status of a *folder,* or a *volume* of a folder, to determine whether its disposal can now be determined where this has not previously been possible (i.e. that it should be destroyed, sent to an archive, or retained for a further review at a later date in circumstances).
Note: a different meaning attaches to this term in the document management environment, where it describes a stage within the document production cycle.

Role
The aggregation of functional permissions granted to a predefined subset of system users. Note: an example of a role is *records manager*. The records manager role has permissions to access many, but not all, administration functions and most record creation and access functions; the role is associated with all users who have records manager tasks.

Series
Subdivisions according to which the file plan is organized consisting of main series (i.e. the topmost series) that are divided into one or more levels of subdivisions called sub-series.

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.

Transmission data
Information in electronic mail systems regarding the date and time messages were sent or forwarded by the author.

Transfer
The process of *export*ing (usually groups of) complete electronic folders and subsequently destroying them within the exporting system, effectively transferring custody of the records. Records may be transferred for the purpose of permanent

preservation in an archives repository, or some other place of deposit; or following structural changes to the machinery of government which create, dissolve or merge organizations.

Volume

A volume is a segment of a folder; it has no existence independent of the folder. A folder will always contain at least one volume - the first volume – which, until and unless a second volume is created, is co-extensive with the whole folder. The concept of volumes allows the contents of folders which would otherwise be closed to be disposed of in a regular and orderly
manner.

Note: Strictly speaking, records are contained within a volume, although a particular system may present an interface which depicts records as contained directly within a folder.

3. FUNCTIONAL REQUIREMENTS

A CORE REQUIREMENTS

A1: DOCUMENT MANAGEMENT

A1.1 (M) The IDMS must either provide document management facilities as an integral part of the system or must be capable of integration with one or both of:

- an electronic document management system capable of passing management control of documents within its own file store(s) to an ERMS at time of declaration
- an electronic document management system capable of transferring declared documents as records to an ERMS directly from the EDM system.

A1.2 (M) Where an ERMS is integrated with an EDMS, it must in principle be capable of integration with new EDM systems and new versions of existing integrated EDMS.

A1.3 (M) The IDMS must enable a newly created document to be captured at creation.

A1.4 (M) The IDMS must enable a newly created document to be captured and declared by the IDMS in one operation.

A1.5 (M) The IDMS must enable a newly created document to be captured and not declared by the IDMS.

A1.6 (M) The IDMS must enable a document already existing in the document management environment or capability to be declared as a record in one operation.

A1.7 (M) The IDMS must support the creation of versions of electronic documents which are closely bound together, and must manage version control to support progressive drafting and ensure continual integrity of the document as a whole.

A1.8 (M) Where more than one version of the document has been created, the IDMS product set must support the ability to declare:

- the most recent version
- one specified version only

- all existing versions, and hold all of these as a single electronic record.

A1.9 (M) The IDMS product set must be capable of allowing versions of a document to be created, as part of drafting process, without automatically creating a new record on each occasion.

A1.10 (M) The IDMS product set must support the ability to define different templates for electronic documents, and the allocation of different metadata elements sets for each template. Examples of distinct types are:
- pre-defined forms
- report layouts
- standard letter formats.

A1.11 (M) The IDMS product set must be capable of configuring the mapping of electronic document metadata to electronic record metadata, to ensure that an electronic record always possesses correct and authentic metadata as defined by the NARS's minimum mandatory metadata set[1] and in accordance with ERMS functional requirements.

A1.12 (M) The IDMS product set must allow metadata to be acquired from the user during the process of declaration.

A1.13 (M) When declaring a record, the IDMS product set must give precedence to the process of capturing metadata in accordance with ERMS functional requirements above metadata from the document management environment or capability, where any potential conflict arises.

A1.14 (M) The IDMS product set must ensure that any metadata captured in the document management environment or capability, that will be carried over into records management metadata, is managed in accordance with ERMS functional requirements to ensure authenticity.

A1.15 (M) When declaring a record, the IDMS product set must give precedence to the access controls for the record in accordance with ERMS functional requirements above access controls applying in the document management environment or capability, where any potential conflict arises.

A1.16 (M) The IDMS product set must not allow a concept of ownership which, within the document management environment or capability gives rights that must not be allowed within the records management environment or capability, to apply to a declared record.

[1] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm . The metadata set will be finalized when the ISO metadata standard is adopted by NARS.

A1.17 (M) The IDMS product set must not allow a declared record to be checked out, where this implies any capability to amend the record content in any way.

A1.18 (M) The IDMS must support the definition of distinct document types, so that a different management policy can be applied to each document type[2].

A1.19 (M) The IDMS must support a default document type, which is available to all users with the ability to create new documents.

A1.20 (M) The IDMS must support the definition of other document types by an Administrator, and must be capable of restricting the ability to create new documents using these types to selected sets of end users.

A1.21 (M) The IDMS must enable defined document types to possess different metadata attributes, and to exhibit different behavior based on these attributes, from the default document type; in particular, in relation to the allocation of disposal schedules.

A1.22 The IDMS product set should be capable of managing documents and records within the same series and folder structure.

A1.23 (M) Where the IDMS product set is capable of managing documents and records within the same series and folder structure, it must make a clear and immediately visible distinction between documents declared as records and those that are not.

A1.24 (M) Where the IDMS product set is capable of managing documents and records within the same series and folder structure, it must provide options for:

- automatically declaring all undeclared documents in a specified folder or folders as records
- automatically deleting all undeclared documents in a specified folder or folders
- automatically deleting all undeclared documents in a specified folder or folders that are older than a specified period of time.

A1.25 (M) Where the IDMS product set is capable of managing documents and records within the same series and folder structure, it must:

- provide a notification, within the disposal management mechanism, where undeclared documents exist within a folder to be exported, and enable them to be declared as records
- export only the records within that folder
- in a transfer process, automatically destroy any remaining documents when the records are destroyed following confirmation of successful export.

[2] E.g. the document types *draft* and *working paper* are managed differently from the document type *final* even though they may be located in the same folder.

A2: RECORDS MANAGEMENT

Records organization: File plan

A2.1 (M) The ERMS must support a hierarchical subject file plan based on the business activities of the organization.

A2.2 (M) The ERMS must be capable of supporting a file plan, with a minimum of three levels below the root level; and must support the use of different numbering schemes at different points in the file plan.

A2.3 (HD) The ERMS must however not impose a limit on the number of levels in the file plan hierarchy.

A2.4 (M) The ERMS must support the initial construction of a file plan within the ERMS, before the receipt of electronic records.

A2.5 (M) The ERMS must allow and authorized user to add new series to the file plan.

A2.6 (M) The ERMS must allow reports to be run on the new series that were added to the file plan to enable the authorized user to report amendments to the National Archives and Records Service.

A2.7 (M) The ERMS must not limit the number of series that can be created at any point within the file plan, or within the entire ERMS.

A2.8 (M) The ERMS must enable a whole series, including all sub-series, folders, volumes, and records which fall under that series, to be relocated to another point in the file plan and should retain a history in the metadata of where they existed prior to re-classification.

A2.9 (HD) The ERMS should enable an authorized user to mark a series as inactive and should prevent any new folders being opened for that series and sub-series.

A2.10 (HD) The ERMS should allow an authorized user to delete inactive series.

A2.11 (HD) The ERMS must prevent deletion of a series that contains folders, until all the content of all the folders in that series, and sub-series, have been disposed of.

A2.12 (HD) The ERMS should support the definition and simultaneous use of file plans.

A2.13 (HD) The ERMS should support a distributed file plan which can be maintained across a network of electronic record repositories

A2.14 (HD) The ERMS should include a help facility on the use of the file plan.

Series metadata

A2.15 (M) The ERMS must support the capture and use of metadata for folders and series in the file plan; and after a record has been captured the ERMS must restrict the ability to add to or amend its metadata to authorized users.

A2.16 (HD) The ERMS must support the capture and presentation of metadata for series as set out in the NARS's minimum mandatory metadata set[3].

A2.17 (M) The ERMS must be able to provide the following methods of naming a folder:

- the capability to allocate a subject to each series that will be used to allocate the full file plan name to the individual folder; and
- the capability to allocate a structured numeric or alphanumeric code to each series that will be used to allocate the full file plan reference number to the individual folder.

A2.18 (M) The ERMS must allow both naming capabilities to be applied separately or together in the same application at the same time.

A2.19 (M) The ERMS must allow the naming mechanism(s) to be defined at configuration time.

A2.20 (M) The ERMS must allow repetition, at different points in the file plan of a series textual name which represents only one segment of the series name.[4]

A2.21 (M) The ERMS must ensure that the complete textual name of each series (all segments of the name) is unique within the file plan[5].

[3] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.
[4] E.g. the description minutes of meetings can be repeated at different levels and in different places in the file plan.
[5] E.g. Organization and Control/Meetings/Heads of Components/Minutes vs Organization and Control/Meetings/Supervisors/Minutes would be a unique name even though some components of the name are repetitive.

A2.22 (HD) The ERMS should allow the bulk import of a structured assembly of series and metadata from an existing file plan into a new file plan.

A2.23 (M) The ERMS should allow inheritance of metadata by lower level in the file plan hierarchy.[6]

A2.24 (M) Should a change occur within one of the metadata elements of a series, the ERMS should allow for that change to be reflected in the metadata of the folders, the volumes and the records that inherited that specific element.

A2.25 (M) The ERMS must support the ability to amend (i.e. over-ride) inherited metadata attributes on any individual series, folder, volume or record.

A2.26 (HD) The ERMS should support an optional series and folder naming mechanism that is based on controlled vocabulary terms and relationships and should support application of an ISO 2788 or ISO 5964 compliant thesaurus.

Folders

A2.27 (M) Where a hierarchical file plan is in use, the ERMS must allow the addition of folders to any level in the hierarchy except the main series heading.

A2.28 (M) The ERMS must allow reports to be run on the new folders that were added to the file plan to enable the authorized user to report amendments to the National Archives and Records Service.

A2.29 (M) The ERMS should support an optional series and folder naming mechanism which includes names (e.g. personal or corporate names) and dates (e.g. dates of birth) as elements of the folder name to accommodate the opening of case files.

A2.30 (M) When creating a new electronic folder in a file plan or within a series in a file plan which uses a structured numerical or alphanumerical reference, the ERMS should automatically generate the next sequential number available at that position[7].

A2.31 (M) The ERMS must not impose any practical limit on the number of folders which can be created under any series, or within the entire file plan.

[6] For example, for a folder, the value of some of the metadata elements must be inherited from the series level; for a volume, the value of some of the metadata elements must be inherited from the folder level; and for a record, the value of some metadata should be inherited from the volume into which it is stored.
[7] This will for e.g. allow for case files to be numbered consecutively.

Folder metadata

A2.32 (M) The ERMS must support the use of metadata for folders, and must be capable of restricting the addition or amendment of metadata elements to authorized users.

A2.33 (M) The ERMS must support the capture and presentation of metadata for folders as set out in the NARS's minimum mandatory metadata set[8].

A2.34 (M) The ERMS must closely link folder metadata to the relevant ERMS functionality which it represents (i.e. fulfill an active rather than merely descriptive purpose in achieving that functionality automatically)[9].

A2.35 (M) The ERMS must support inheritance of metadata by folders allocated to a series so that, by default, addition of a *new* folder results in automatic inheritance of those attributes which derive from the series to which it is allocated.

A2.36 (M) Should a change occur within one of the metadata elements of a series, the ERMS should allow for that change to be reflected in the metadata of the folders that inherited that specific element.

A2.37 (M) The ERMS must support the ability to select a set of folders in order to perform a bulk amendment of the same metadata element on the whole selected set of folders in one process.

A2.38 (M) The ERMS must support the ability to over-ride inherited metadata attributes on any individual folder and if volumes inherited such metadata elements, any and all volumes of that folder must inherit the changes to the metadata of the folder.

A2.39 (M) The ERM must be capable of enforcing the *mandatory* use of the file plan structure to construct the folder name when new folders are created in a series[10].

A2.40 (M) The ERMS should support the ability to optionally assign one or more controlled vocabulary terms by selection from a pre-defined list, to an electronic folder.

---

[8] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.

[9] E.g. the disposal metadata should be able to trigger disposal events.

[10] E.g. Finance/Expenditure/Claims/Vehicle transport already exists in a series. Should a folder for Travel and Subsistence be added, to the series the folder should automatically inherit the Finance/Expenditure/Claims prefix from the series description.

A2.41 (M) The ERMS must support the use of user-defined metadata fields with folders, for recording descriptive information.

Folder management

A2.42 (M) The ERMS must enable recording of the opening date of a folder.[11]

A2.43 (M) The ERMS must limit the ability to create new folders within an existing series according to user role so that only authorized users can open folders.

A2.44 (M) The ERMS must be able to close a folder or a volume and ensure that no new volumes or records can be added to that closed folder or volume.

A2.45 (M) The ERMS must provide the ability to retrieve and view those records already added to a closed volume or folder.

A2.46 (M) The ERMS must restrict the ability to close a folder to an authorized user.

A2.47 (M) The ERMS must automatically record the closing date of the folder. This date to be actively used by disposal functionality.

A2.48 (M) The ERMS must allow an authorized user to open a previously closed folder for the addition of records and the creation of a new volume if necessary and subsequently to close that folder again.[12]

A2.49 (HD) The ERMS must not allow any volume that has been temporarily re-opened to remain open after the authorized user who opened it has logged off.

A2.50 (M) The ERMS must be able to accommodate the concept of parent files.[13]

A2.51 (M) The ERMS must prevent the destruction or deletion of an electronic folder and any of its records and metadata at all times, with the exceptions of:

- destruction in accordance with a disposal schedule

[11] The opening date may be chronologically earlier than the physical creation date of the folder; this date to be actively used by disposal functionality. The opening date should automatically default to the creation date, but must be amendable by an authorized user.

[12] This action should not automatically change the closing date of the folder held as a metadata attribute.

[13] The system must accommodate the use of parent files as in the example

5/2/1 Transport
5/2/1/1 Official

as opposed to 5/2/1 Transport
5/2/1/1 Official
5/2/1/2 Private
5/2/1/3 Municipal

to provide for information about a subject as a whole or for aspects of a subject that do not accumulate so many records that they warrant separate folders for each.

- deletion by an Administrator as part of an audited procedure

A2.52 (M) The ERMS must allow an electronic folder or group of folders, and all volumes and records which fall under that folder or folders, to be re-classified, by an authorized user, to a different point in file plan.

A2.53 (M) The ERMS must ensure that all electronic records allocated to a folder and all the volumes of a folder remain correctly allocated following the relocation of a folder or group of folders.

A2.54 (M) When any series, folders, volumes or records are re-classified the ERMS must keep a clear trace of their status prior to the re-classification, so that their entire history can be determined easily.

A2.55 (HD) The ERMS should allow all relevant metadata elements which are inherited from the file plan, the series, or the volume to be automatically updated following the re-location of a series, folder, volume or record.

A2.56 (HD) The ERMS should allow an authorized user to add the reasons for re-classification of a series, folder, volume or record to the item(s) re-classified, in one bulk operation.

A2.57 The ERMS should support the creation of cross references (that is, 'see also' type links) between folders which are classified in different parts of the file plan and that are related to each other.

Volumes

A2.58 (M) The ERMS must support the concept of electronic volumes, as a means to segment a folder for management purposes.

A2.59 (M) The ERMS must support capture and presentation of metadata for volumes as set out in the NARS's minimum mandatory metadata set[14].

A2.60 (M) The ERMS must closely link volume metadata to the relevant ERMS functionality which it represents (i.e. fulfill an active rather than merely descriptive purpose in achieving that functionality automatically)[15].

A2.61 (M) The ERMS must support inheritance of metadata by volumes of a folder so that, by default, addition of new volumes result in automatic inclusion of those attributes which derive from the folder to which it is allocated.

[14] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.
[15] E.g. the disposal metadata should be able to trigger disposal events.

A2.62 (M) The ERMS must allow the opening of new electronic volumes to any electronic folder which is not closed; and should be able to restrict this capability to authorized users.

A2.63 (M) The ERMS must ensure that an electronic volume will only contain electronic records (and markers representing physical records where used). It must not be possible for a volume to contain another folder or volume.

A2.64 (M) The ERMS must support the concept of open and closed electronic volumes, and be capable of restricting the ability to close a volume to authorized users.

A2.65 (HD) The ERMS should be able to automatically close a volume on fulfillment of specified criteria to be defined at configuration, including at least:

- volumes delineated by an annual cut-off date; for example, the end of the calendar year, financial year or other defined annual cycle
- the passage of time since a specified event; for example, the last addition of an electronic record to that volume
- the number of electronic records which a volume contains and, optionally, to open a new volume within that folder.

A2.66 (M) The ERMS must ensure that only the most recently created volume within a folder will be open at any one time, and that all other volumes within that folder will be closed, but noting the requirement at A2.72.

A2.67 (M) The ERMS must ensure that the records contained in all volumes, whether open or closed, are equally retrievable and viewable in the same search process.

A2.68 (M) The ERMS must prevent the addition of electronic records to a closed volume, but noting the requirement at A2.72.

A2.69 (M) The ERMS must automatically record the opening and closing dates of a volume as metadata attributes.

A2.70 (M) The ERMS must ensure that the act of opening a new volume automatically closes the preceding volume.

A2.71 (M) The ERMS must automatically add new records classified against a folder to the currently open (the most recent) volume, and should do so without requiring the user to explicitly choose a volume (but noting the exception at A2.72*)*.

A2.72 (M) The ERMS must allow an authorized user to open a previously closed volume for the addition of records, and subsequently to close that volume

again; this action will not, by default, change the closing date of the volume held as metadata.

A2.73 (M) The ERMS must maintain full structural integrity of the series, folder, volume and record structure at all times, regardless of maintenance activities, user actions, or component failures.

A3: RECORD CAPTURE, DECLARATION AND MANAGEMENT

Capture

A3.1 (M) The ERMS must ensure that electronic documents can be captured into the file plan at creation

A3.2 (M) The ERMS must ensure that electronic documents can be captured, so that they can be declared and stored as electronic records, from:

- standard office applications
- operating system directory management facilities
- e-mail client applications
- images created by a document scanning system

A3.3 (M) The ERMS must be capable of supporting document capture from new office applications, including open source software, as these are brought into use by an organization.

A3.4 (M) The ERMS must provide an Application Programming Interface to enable integration with other business applications, so that records of transactions generated by operational and 'line-of-business' systems can be captured.

A3.5 (M) ERMS must support the capture and declaration of any electronic document which is stored as a single electronic file. Examples include:

- XML documents and forms
- word processing documents
- documents produced by text editors
- spreadsheets
- e-mail messages
- e-mail messages with attachments
- e-mail receipts
- encapsulated 'web pages', with all components, in a single physical file
- presentations
- desktop publishing documents
- PDF format documents

- document images from a scanning system
- single static images in common formats
- bit-mapped and vector graphics.

A3.6 (HD) The ERMS should be able to capture compound records retaining a closely bound relationship between all components, so that they are managed as a single record. Examples include:

- multimedia documents, including those with animation and video components
- complete sessions from collaborative systems and 'chat rooms'
- webcasts
- directly interlinked documents, for example by an OLE link
- vector graphics and data in CAD/CAM systems
- map bases and data held in GIS systems
- electronic calendars

A3.7 (M) The ERMS must allow users to capture, declare and store electronic records in their native format.

A3.8 (M) The ERMS must be able to capture an electronic document, even though the generating application is not present.

A3.9 (M) Where the ERMS captures records which are constructed of more than one component, it must be able to:

- capture and declare the record in a way that retains the relationship between its constituent components
- retain structural integrity of the record
- support later integrated retrieval, display, management of the record as one unit
- dispose of the record as a whole unit, in one operation[16].

A3.10 (M) The ERMS must ensure the capture of, and be able to declare, manage, display and dispose of an e-mail message with one or more attachments, maintaining e-mail text and attachments as a single electronic record.

A3.11 (M) The ERMS must be able to capture an e-mail message (and attachments if present) from within an e-mail client.

A3.12 (M) The ERMS must allow a user to choose whether to capture an e-mail message with attachment(s) as:

- the e-mail message only
- the e-mail message with attachments
- the attachment(s) only
- any sequence of all combinations of the above

[16] Examples would be web pages with embedded graphics, Word documents with Excel spreadsheets embedded, etc.

A3.13 (HD) When capturing a document in its native format, the ERMS should be capable of also capturing a rendition of that document in a standard format, and of storing native format and rendition in a close association. Standard rendition formats include: XML, PDF and Postscript.

Declaration

A3.14 (M) The ERMS must support the process of declaration of an electronic document as a formal electronic record directly by an end user. (Capture and declaration may take place in one operation) taking into account the requirement in A3.1

A3.15 (M) The ERMS must prevent any amendment to the content of any electronic record (which has been declared) by any user including an Administrator.

A3.16 (M) The ERMS must at all times prevent the destruction or deletion of any electronic record (which has been declared) with the exceptions of:

- destruction in accordance with a disposal schedule
- deletion by a systems administrator as volume of an audited procedure.

A3.17 (M) The ERMS must support the naming of electronic records, and allow this name to be different from the existing electronic document filename (including e-mail subject lines used to construct record titles); if the existing filename is taken by default, the ERMS must allow this name to be amended at the time of declaration.[17]

A3.18 (M) The ERMS must ensure that the content of the body of an e-mail message and the transmission details cannot be amended in any way between processes of capture and declaration (but excluding the subject line used as record title, which can be edited).

A3.19 (HD) The ERMS should ensure that the content of and the transmission details of other electronic transactions with which the ERMS is closely integrated cannot be amended in any way between processes of capture and declaration.

A3.20 (M) The ERMS must ensure that all electronic records are assigned to at least one folder after declaration.

A3.21 (M) The ERMS must not impose, by its own architecture or design, any practical limit on the number of documents and records which can be captured and declared into a folder; or on the number of records which can be captured and declared into the ERMS as a whole.

[17] Specifically in cases where the document/e-mail does not carry a logical name.

A3.22 (M) The ERMS must allow an electronic record to be assigned to more than one folder without the physical duplication of the record.

A3.23 (M) The ERMS should be capable of relating each assignment of the record to different folders, so that a later retrieval of one assignment enables the identification and retrieval of all other assignments of that record made at the time of capture, or at a later stage from within the ERMS.

A3.24 (HD) The ERMS should alert a user who is attempting to capture and declare a document into a folder in which it has already been declared, where this is evident from captured metadata.

A3.25 (M) Where multiple assignments are achieved by use of a pointer system working with a single actual record, the ERMS must be able to manage the integrity of all pointers or references, to ensure that:

- following a pointer, whichever folder that pointer is located in, will always result in correct retrieval of the record
- change in location of a record also redirects any pointers which reference that record at all times.

A3.26 (M) The ERMS should provide support for decisions on the allocation of electronic records to electronic folders by:

- as initial default, showing only selected sections of file plan, based on user or role profile
- suggesting the most recently used folders by that user
- suggesting folders which contain known related electronic records
- suggesting folders by inferences drawn from record metadata elements: for example, significant words used in the document title
- suggesting folders by inferences drawn from the record contents.

A3.27 (M) The ERMS must support the creation of versions of electronic records.

A3.28 (M) Where more than one version of a record has been created, the ERMS must support the ability link original superseded records to their successor records.

Record types[18]

A3.29 (M) The ERMS must support the definition of distinct record types, so that a different management policy can be applied to each record type[19].

[18] By definition this includes document types.

[19] E.g. the document types *draft* and *working paper* are managed differently from the document type *final* even though they may be located in the same folder.

A3.30 (M) The ERMS must support a default record type, which is available to all users with the ability to create new records.

A3.31 (M) The ERMS must support the definition of other record types by an Administrator, and must be capable of restricting the ability to create new records using these types to selected sets of end users.

A3.32 (M) The ERMS must enable defined record types to possess different metadata attributes, and to exhibit different behavior based on these attributes, from the default record type; in particular, in relation to the allocation of disposal schedules.

Record metadata

A3.33 (M) The ERMS must support the use of metadata for electronic records

A3.34 (M) The ERMS must support the capture and presentation of metadata for electronic records as set out in the NARS's minimum mandatory metadata set[20].

A3.35 (M) The ERMS must provide a mechanism for the definition and later amendment of a rule base of metadata elements (metadata set), and should be able to apply version control to this rule base.

A3.36 (M) The ERMS must ensure the capture of all required metadata elements specified at systems configuration, and retain them with the electronic record in a tightly-bound relationship at all times.

A3.37 (M) The ERMS must be capable of automatically capturing:
- metadata acquired directly from an authoring application
- metadata acquired directly from an operating system
- metadata generated by the ERMS itself.

A3.38 (M) The ERMS must be capable of capturing metadata acquired from the user at the time of declaration.

A3.39 (M) The ERMS must be able to acquire metadata from the document-creating application package and operating system or network software[21].

[20] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.
[21] To allow for the capturing of systems metadata as defined in NARS's metadata set that is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm

A3.40 (M) The ERMS may provide an option for capturing metadata from the 'document properties' information held by a document where this is available; *but if so*, the ERMS *must* allow this metadata to be edited prior to declaration.

A3.41 (M) The ERMS must support the ability for versions of a record to inherit metadata from the original record (noting the requirement at A3.46).

A3.42 (M) The ERMS must support the ability to optionally assign one or more controlled vocabulary terms by selection from a pre-defined list to an electronic record.

A3.43 (M) The ERMS may support the ability to optionally assign one or more controlled vocabulary terms by selection from an ISO 2788 compliant thesaurus  n electronic record.

A3.44 (M) The ERMS must allow entry of further descriptive and other specified metadata at a later stage of processing[22] (i.e. where this is allowable within other requirements); and must be able to restrict this ability to authorized users.

A3.45 (M) The ERMS must prevent any amendment of selected elements of metadata of the electronic record which have been acquired directly from the application package, the operating systems or the ERMS itself (for example, certain dates) as defined by the NARS minimum mandatory metadata set (but noting A3.17 and A3.44).

A3.46 (M) The ERMS must be capable of allowing a user to edit the content of selected elements of metadata of the electronic document during but not after the process of declaration, including Title and Creator.

A3.47 (M) The ERMS must allow an authorized user, after declaration, to edit the content of all metadata elements that have been captured from, or edited by, a user, but not those elements that have been system generated.

A3.48 (M) The ERMS must support:

- the definition of user-defined metadata elements for electronic records, by an Administrator
- the required metadata element set for each new record type to be separately selected when defining the record type (within system requirements)
- each selected metadata element to be defined as either mandatory or optional (except where the system requires metadata elements to be mandatory)
- later reconfiguration of the selected metadata set.

[22] E.g. the capturing of archival descriptive metadata to enable archival functions to be performed on the records when they are in the custody of an archives repository.

A3.49 (M) The ERMS must record the date and time (to the nearest minute) of declaration as a metadata element attached to the record; this data should in addition be recorded in the audit trail.

A3.50 (M) The ERMS must ensure the capture of e-mail transmission data and be capable of mapping this data to electronic record metadata elements, as set out in the NARS's minimum mandatory metadata set[23].

A3.51 (M) When capturing an e-mail message, the ERMS must ensure that e-mail transmission data is included in the body of the record, including sender, recipients, and date of receipt.

A3.52 (M) The ERMS must capture the 'intelligent' version of an e-mail message address, where one is associated with the original message; for example, 'John Smith' rather than js042@aol.com, as well as the full version.

A3.53 (M) The ERMS must validate the content of selected metadata elements, to conform with requirements as set out in the NARS's minimum mandatory metadata set[24]; in particular, in relation to date formats and numeric and alphanumeric formats

A3.54 (M) The ERMS must be able to allocate an identifier, unique within the system, to each electronic record on declaration that serves to identify the record from the point of declaration throughout the remainder of its life within the ERMS.

A3.55 (M) The ERMS must prevent the modification of the unique identifier.

Move, copy, extract and relate

A3.56 (M) The ERMS must allow an electronic record to be re-assigned to another electronic folder or volume, and must be capable of restricting this ability to an authorized user.

A3.57 (M) The ERMS must be able to copy the contents of an existing electronic record, in order to create a new and separate electronic document, while ensuring the original record remains intact.

A3.58 (HD) Where an ERMS does not use pointers, the ERMS should be able to make a controlled copy of an existing electronic record, which can immediately be allocated to a different folder without change to the contents.

[23] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.
[24] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.

A3.59 (M) When a record is retrieved, an ERMS that is able to make controlled copies as in A3.58 must make explicit the existence of, and offer an intuitively clear means of retrieving, any and all controlled copies made from that record.

A3.60 (HD) The ERMS should support the ability to create multiple entries for electronic records in different electronic folders without physical duplication of the electronic record itself. (i.e. relate the record to more than one folder)

A3.61 (HD) The ERMS should be able to mark a record as superseded, and create a navigable link to the superseding record.

A3.62 (HD) The ERMS should be able to declare the extract as a record in its own right, but noting A3.63.

A3.63 (HD) The ERMS should be able to automatically record the relationship between one or more extracts and the originating record.

A3.64 (M) Where an ERMS support direct creation of an extract it must be able to copy existing metadata attributes and access controls from the originating record to the extract, but allow selected items to be amended where necessary.

A3.65 The ERMS should allow the date and reason for the creation of an extract to be captured in the metadata of the extract and in the metadata of the originating record.

A3.66 When an originating record is retrieved, the ERMS should make explicit the existence of, and offer an intuitively clear means of retrieving, all extracts made from that record.

Bulk import

A3.67 (M) The ERMS must be able to capture in bulk records exported from other records management and document management systems, including capture of:

- electronic records in their existing format, without degradation of content or structure,
  retaining the relationship between the components of any individual record
- electronic records and all associated metadata, retaining the correct relationship between individual records and their metadata attributes
- the folder structure to which the records are assigned, and all associated metadata, retaining the correct relationship between records and folders.

A3.68 (HD) The ERMS should be to import any directly associated audit information with the record and/or folder, retaining this securely within the imported structure.

A3.69 (M) Within the schedule for implementation, the ERMS must be able to directly import, in bulk, electronic records in their existing format with associated metadata that is presented according to a pre-defined XML schema mapping this to the receiving ERMS folder and metadata element structures.

A3.70 (M) The ERMS must also be able to indirectly import, in bulk, electronic records in their existing format with associated metadata that is presented in a non-standard format, mapping this to the receiving ERMS folder and metadata element structures.

A3.71 (M) The ERMS should be able to import, in bulk, existing electronic documents, in any and all supported formats, that have no associated metadata presented separately from the document, by:

- placing documents in queues for further processing
- automatically extracting metadata from the document properties where possible
- providing facilities for the addition of missing metadata, and the assignment of documents to folders
- supporting the declaration of documents from these processing queues.

A4: SEARCH, DISPLAY AND PRESENTATION

A4.1 (M) The ERMS must provide facilities for searching, retrieving and displaying series, folders, electronic records and markers (where markers are used).

A4.2 (M) The ERMS must provide an optional search and display interface via a web browser platform, to support retrieval and display of folders and records, and the folder and record metadata normally available to the end user.

A4.3 (M) The ERMS must support graphical browsing of the file plan, and browsing directly from a series to the folders created under that series; and the direct selection, retrieval and display of electronic folders and their contents through this mechanism.

Searching

A4.4 (M) The ERMS must be capable of searching for all records management metadata elements, including user-defined elements (noting requirement A4.18)

A4.5 (M) Where a controlled vocabulary or thesaurus is implemented, the ERMS must be capable of searching for folders and records by terms from the controlled vocabulary or thesaurus.

A4.6 (M) The ERMS must be capable of searching the full-text content of electronic records .

A4.7 (M) The ERMS must present an integrated interface for searching both metadata and record content.

A4.8 (M) The ERMS must allow search terms to be qualified by specifying a metadata element, or record content, as source.

A4.9 (M) The ERMS must be capable of constructing searches by combining multiple terms, from multiple sources.

A4.10 (M) The ERMS must enable default search options for end users to be configured from the full range which is available

A4.11 (M) The ERMS must provide facilities for defining and storing saved searches, for reuse by end users.

A4.12 (HD) The ERMS should support saved searches which can be run with varying parameters, including dates and date ranges.

A4.13 (D) The ERMS should allow the use of propositional search logic, including:
- Boolean operators
- partial matches
- wildcard characters

A4.14 (D) The ERMS may allow the use of advanced search features, such as probabilistic retrieval, relevancy feedback, and pattern matching

A4.15 (D) The ERMS must present search results as a list of folders or records meeting search criteria; and must notify the user if the search results in a null set.

A4.16 (D) The ERMS must be able to search for and retrieve a complete electronic folder, and all its volumes and records, and display a list of all, and only, those volumes and records in the context of that folder as a discrete group and in a single retrieval process.

A4.17 (M) The ERMS must be able to search for, retrieve and list a set of electronic records taken from many different folders, by specifying values to be searched for in electronic record metadata or content.

A4.18 (M) The ERMS must not allow a user to have access to series, folders or records or their metadata (according to configuration) by means of any search and retrieval function, where the access controls and protective markings allocated to those series, folders or records prevent access by that user.

A4.19 (D) The ERMS should be capable of supporting the integration, within the design architecture of ERMS, of a different search engine from the one with which it is routinely supplied.

Display

A4.20 (M) The ERMS must enable the contents of any or all of the folders or records in a set of search results to be directly displayed without requiring a further search, or re-entry of data already retrieved .

A4.21 (M) The ERMS must routinely be able to display the content of all the types of electronic records which it is able to capture, in a manner that:

- shows all the features of visual presentation and layout as rendered by the generating application package
- displays all components of an electronic record together as a unit.

A4.22 (M) The ERMS must provide viewing mechanisms capable of displaying all the types of electronic records which it is able to capture, even though the generating application is not present.

A4.23 (M) The ERMS must support simultaneous retrieval and display of series, folders and records by multiple users.

A4.24 (M) The ERMS must be capable of displaying all available metadata associated with a folder or electronic record on request

A4.25 (M) The ERMS must be able to print all types of electronic records which it is able to capture, and which are printable, in the same manner as they are displayed on screen within the ERMS, without use of ‘screen-dumping’ or ‘snapshots’.

A4.26 (D) The ERMS should allow all the records in a folder or a volume (which are print-able) to be printed in one operation.

A4.27 (D) The ERMS should allow the initial search results – that is, a list of folders or records – to be printed.

A4.28 (M) The ERMS must allow the metadata for a series, folder, and record, to be printed.

Presentation

A4.29 (HD) The ERMS should provide facilities for the presentation of folder metadata, records and record metadata to a destination external to the ERMS, in a form suitable for electronic publication.

A4.30 (HD) The ERMS should support the selection and presentation of:
- whole series, including selected elements of series metadata and a list of folders which that series contains
- whole folders, including selected elements of folder metadata, and a list of record titles which that folder contains
- specified electronic records, including record content and selected elements of record metadata
- specified extracts, including record content and selected elements of meta-data, but without the record to which the extract is related.

A4.31 (M) Where the ERMS is capable of presentation of series, folders and records, these must be able to be rendered in one or more of:
- an XML format suitable for publication
- a non-proprietary HTML format suitable for publication

A3.32 (HD) The ERMS should allow an e-mail retrieved by browsing or searching to be copied to a compatible e-mail application, for transmission in a manner normally achieved by that application.

A5: RETENTION AND DISPOSAL

Disposal schedules : definition

A5.1 (M) The ERMS must provide a mechanism for the definition and later amendment of a rule base of retention and disposal rules (afterwards called disposal schedules), each of which can be allocated to series, folders, and document/record type records.

A5.2 (M) The ERMS must support the use of a disposal authority number (unique identifier) for each disposal schedule.

A5.3 (M) The ERMS must be capable of restricting the ability to define and maintain disposal schedules in the rule base to authorized users.

A5.4 (M) The ERMS must enable an authorized user to re-define an existing disposal schedule in the disposal schedule rule base, and ensure that the re-definition takes force on all the objects to which that schedule is already allocated.

A5.5 (M) The ERMS must be capable of maintaining a history of changes to disposal rules, the date at which the change was made, the name of the authorized user who made the change, and the reason for the change.

A5.6 (M) The ERMS must be able to import and export a set of disposal schedules.

A5.7 (M) The ERMS must support disposal schedules which consist of:
- a retention period, commencement of which is triggered by the effective date of an event type
- an event type, which determines the commencement of a retention period
- a set of disposal instructions, which come into force when the retention period is completed.

A5.8 (M) The ERMS must support retention periods which can be expressed as a period of either:
- a number of whole months, from one to eleven months
- a number of whole years, from one to 100 years
- a combination of whole months and years.

A5.9 (M) The ERMS must support the following internal event types which can automatically trigger the commencement of a retention period:
- opening date of a folder
- opening date of a volume
- closing date of a folder
- closing date of a volume
- last addition (that is, date of declaration) of an electronic record to an electronic folder
- last retrieval of an electronic record from an electronic folder
- date of last review of a folder or volume.

A5.10 (M) The ERMS must support external event types[25] which occurs outside the knowledge of the system which can automatically trigger commencement of a retention period, and must:
- enable an authorized user to notify the ERMS that a specified event has occurred

[25] An event that happens outside the system and which is notified to the system. E.g. a request for information i.t.o. PAIA that should result in the freezing and postponement of a disposal action.

- enable an authorized user to notify the ERMS of the effective date on which the event occurred
- automatically trigger the retention period when notification of the event is received by the ERMS, without requiring explicit amendment of each disposal schedule which is activated.

A5.11 (M) The ERMS must be able to accept definition of more than one external event, each of which may be used separately by different schedules allocated to different groups of folders.

A5.12 (M) The ERMS must support the allocation of disposal instructions as part of a disposal schedule which include:
- review
- export
- transfer (i.e. export, followed by destruction)
- destruction.

A5.13 (HD) The ERMS should support staged disposal by enabling the definition of multiple stages within a single disposal schedule; for each stage it must be possible to define a sequence of separate pairs of disposal dates and actions, each of which will come into force in turn .

Disposal schedules : allocation

A5.14 (M) The ERMS must provide a mechanism for the allocation of a pre-defined disposal schedule to each series, electronic folder and specified document/record types in the ERMS, by selecting from the current defined set of schedules in the rule base.

A5.15 (M) The ERMS must enable, but not require, the allocation of a disposal schedule to a series, to be, by default, inherited downwards by all folders subsequently created under that series (i.e. inheritance on creation).

A5.16 (M) The ERMS must enable a disposal schedule to be allocated to any specific folder, that is different from and can take precedence over (i.e. over-rides), a disposal schedule which may have been inherited from a series and must be able to notify an authorized user when there is a disposal conflict..

A5.17 (M) The ERMS must be capable of restricting the ability to allocate and re-allocate disposal schedules to folders and series, to authorized users.

A5.18 (M) The ERMS should support the ability to allocate a disposal schedule to a pre-defined document/record type which has been defined at configuration as capable of supporting this action (i.e. which is not the default

record type); and if so, must ensure that the capability to allocate such as schedule can be restricted to authorized users.

A5.19 (M) The ERMS should ensure that where a specific disposal schedule has been allocated to a document/record type, each instance of a document/record created under that type will inherit the schedule at the time of document/record creation, regardless of the folder to which it is allocated.[26]

A5.20 (M) Where the ERMS does not support automatic inheritance of a disposal instruction from a document/record type to all instances of documents/records created within that type, the ERMS must:

- enable a disposal schedule to be allocated to an individual instance of a document/record type which allows this capability, *but not* to the standard default document/record type (which does not)
- *and* must ensure that the capability to allocate such as schedule can be restricted according to an authorized user.

A5.21 (M) The ERMS must enable an authorized user to re-allocate a different disposal schedule to an existing folder or series, where that folder or series already has a disposal schedule allocated, at any point in the life of the folder or series.

A5.22 (M) Where a disposal schedule is re-allocated to an existing series, from which one or more folders or series have inherited a disposal schedule, the ERMS should ensure that the new schedule is inherited by those folders or series which previously inherited a schedule from that series, except for those where a different and over-riding schedule has been individually allocated (i.e. retrospective inheritance).

A5.23 (M) Where a disposal schedule is re-allocated to an existing electronic document/record type, under which records of that type have inherited a disposal schedule, the ERMS should ensure that the new schedule is inherited by those documents/records which previously inherited a schedule from the docu ment/record type.

A5.24 (M) When a schedule is re-allocated, or a folder or group of folders is moved from one series to another, the ERMS must *either*:

- offer an option to automatically replace the existing schedules inherited from the source series with schedules to be inherited from the destination series, and to notify of exceptions for manual decision, *or*
- provide an immediate entry into a disposal re-scheduling process in order to manually change all necessary schedules as required.

[26] E.g. A **Disciplinary Warning** allocated to the personnel folder for an individual should normally be removed from the folder after a period of 6 months. A **Disciplinary Warning record type** should allow records created under that type to have an appropriate schedule inherited automatically, which will be different from the schedule allocated to the folder as a whole.

A5.25 (M) The ERMS must enable a disposal hold to be placed on a folder or group of folders by an authorized user, which has the effect of pausing the disposal process (i.e. no disposal action can be taken on the folders and the records contained while the hold is in place).

A5.26 (M) The ERMS must prevent any folder or record which has a disposal hold placed
on it from being deleted by an Administrator, outside of the disposal process.

A5.27 (M) The ERMS must be capable of reporting on folders and records which have a disposal hold placed on them, and enable such a hold to be removed by an authorized user only.

A5.28 (M) The ERMS should maintain a history of disposal schedule rules that have been applied to each folder, series or document/record type as metadata with the folder, series or document/record type.

Disposal execution

A5.29 (M) The ERMS must automatically track the commencement and progress of retention periods, on all folders and records which have been allocated disposal schedules, in order to determine effective disposition dates.

A5.30 (M) The ERMS must provide a disposal management mechanism, which will, once the disposal process is initiated by an authorized user:

- automatically identify all qualifying folders and records where the specified conditions for disposal are fulfilled
- notify an authorized user of all the folders and records so qualifying
- enable re-allocation of a disposal schedule to folders if required, which then determines whether the folders currently qualify for disposal
- carry out the disposal action on confirmation to proceed.

A5.31 (M) The ERMS must ensure that the all actions required by a disposal schedule are applied to all the contents of the folder as a whole, unless a separate disposal schedule for one of its constituent documents/records has been allocated, by use of a specific document/record type which allows this action[27].

[27] Please note

a) If subject matter in the file plan is non-archival, but certain types of records that are archival in nature (e.g. photographs, videos, etc) are placed on such folders, the records manager should be notified of the disposal conflict. The records manager should review the disposal instruction of those specific cases. E.g a folder containing information regarding the routine day-to-day maintenance of a building that also contains photographs and/or a video of the maintenance operations that can later on be used during the restoration of the building for purposes of declaration as a national monument.

b) Subject matter in a file plan is archival but the folder contains drafts, working papers, and other documents (not declared as records) that can be destroyed in terms of a general disposal authority. In such a case

A5.32 (M) The ERMS must always seek confirmation before implementing disposal actions.

A5.33 (M) The ERMS should seek confirmation of irreversible actions twice before proceeding.

A5.34 (M) The ERMS must ensure that all functions of the disposal management mechanism are restricted to authorized users.

A5.35 (M) The ERMS must ensure that, in normal operational conditions, a disposal schedule allocated to any folder is triggered by the system date, and can only become effective in real time (i.e. that the disposal schedule cannot be triggered by artificially advancing the current date within the disposal management mechanism).

A5.36 (M) Where the contents of a metadata field are used by a disposal schedule to determine a disposal date, the ERMS must be capable of tracking any changes made to the contents of that field and re-determining the disposal date once a change is made, after initial allocation of the schedule.

A5.37 (M) When processing a folder which is allocated a disposal schedule that uses the opening or closing date of a volume as the event type which triggers the schedule, the ERMS must apply the disposal action to the specific volume which was opened or closed (and thereby triggered the event), and must not apply the disposal action to any other volumes in the folder, or to the whole folder.

A5.38 (M) The ERMS must be capable of identifying folders and records which have a disposal hold placed on them, so that any disposal action is not carried out while the hold is in force.

A5.39 (HD) The ERMS should be capable notifying an authorized user if a superseded record is to be destroyed when replaced with a new version.

Resolving conflicts

A5.40 (M) The ERMS must at all times ensure that, where a folder is governed by more than one disposal schedule, at the individual folder and at the series levels, which may specify conflicting disposal actions, execution of a disposal action is moderated by the requirements of all other schedules that pertain, so that:

- the most specific schedule (the lowest in the hierarchy) applies

---

the disposal schedule of the document/record type should override the disposal schedule for the folder to allow the documents to be removed from the folder so that only the records remain.

- resolving a disposal conflict must not ever result in a folder which does not yet qualify for disposal becoming 'disconnected' from the series hierarchy by the removal of intermediate structure
- a Review action takes precedence over a Destroy or Export action
- an Export action takes precedence over a Destroy action.

A5.41 (M) Where an electronic record is governed by more than one disposal schedule because the record is assigned to more than one electronic folder, (for example, using a pointer scheme), the ERMS must automatically track all retention periods and disposal actions that are applicable and ensure that the record is unfailingly retained within each folder where it is required, for the retention period which applies to that folder, so that:

- removal of the record from visibility in one folder at an earlier date does not prejudice continued inclusion of that record in another folder until a later date
- continued inclusion of a record in one folder until a later date does not preclude the removal of that record from another folder where the retention period is shorter; and that in such a case, the record is removed from the folder with a shorter retention period.

A5.42 (M) The ERMS must at all times ensure that, where a document/record is governed by more than one disposal schedule, one at the folder level and the other at the document/record type level, which may specify conflicting disposal actions:

- the document/record type schedule, allocated to the individual electronic document/record because it falls within a specific document/record type, takes precedence over the schedule allocated to the folder to which that document/record is assigned, where this calls for destruction or review of the document/record earlier than destruction or review of the folder
- destruction of the individual document/record has no secondary effect on the remaining contents of the folder, other than removal of that document/record
- destruction of the folder before destruction of the individual document/record is due, is not possible, and that an authorized user is notified of this conflict either at time of schedule allocation or at time of attempted disposal.

A5.43 (M) The ERMS must at all times ensure that, where a single document/record is allocated to more than one folder by means of a pointer system, and that document/record is governed by several disposal schedules, at both the individual folder level and at the document/record type level, which may specify conflicting disposal actions:

- the document/record type schedule, allocated to the individual electronic document/record because it falls within a specific document/record type, takes precedence over all schedules allocated to any folders to which the document/record is assigned, where this calls for destruction or review of the document/record earlier than destruction or review of the folder

- destruction of the individual document/record removes the document/record from all folders to which it is allocated, but has no secondary effect on the remaining contents of the folder, other than removal of that document/record
- destruction of a folder to which the document/record is allocated, before destruction of the individual document/record is due, is possible as long as the document/record remains allocated to another folder, but that this action requires notification to and explicit confirmation by an authorized user.
- destruction of the last remaining folder to which a document/record is allocated before destruction of the individual document/record is due, is not possible, and that an authorized user is notified of this conflict either at time of schedule allocation or at time of attempted disposal.

A5.44 (M) The ERMS must ensure that all conflicts in disposal actions are resolved by either:

- automatically applying the strictest schedule according to precedence in the above requirements and alerting an authorized user of this fact if necessary
- notifying an authorized user of the conflict and presenting the available options for immediate resolution.

Review

A5.45 (M) When a disposal schedule triggers a review disposal action on an electronic folder or series, the ERMS must enable the re-allocation of a disposal schedule, which may result in:

- a later review, following a further retention period
- marking for permanent preservation and transfer to the National/Provincial Archives Repository, immediately or following a further retention period
- destruction, immediately or following a further retention period.

A5.46 (M) The ERMS must make all metadata for a folder or series scheduled for review available to the reviewer.

A5.47 (M) The ERMS must make all the contents of a folder or series scheduled for review available to the reviewer on request, within access control restrictions .

A5.48 (M) The ERMS must ensure that immediate destruction after a review occurs within the normal disposal process and that there is no separate delete functionality outside the normal disposal process, except where it is possible to re-allocate a disposal schedule to that series or folder that enables immediate destruction.

A5.49 The ERMS must ensure that the date of, and the name of the user that authorized the re-allocations of disposal schedules that enable immediate destruction of a series or a folder are captured in the audit trail.

A5.50 (M) The ERMS must support the progressive addition of metadata through iterative review processes, and must enable the reason for the outcome of that review to be recorded as folder metadata.

A5.51 (HD) The ERMS should automatically record the date of last review of a folder, so that it can be used as the trigger of a disposal rule.

Export and transfer

A5.52 (M) The ERMS must be able to export electronic folders, folder and series metadata, all their constituent electronic records and the record metadata, for import to another ERMS, or for transfer to the National/Provincial Archives Repository for permanent preservation.

A5.53 (M) Whenever the ERMS exports any series, folder, or volume, the ERMS must be able to export:

- all folders which qualify under the disposal action
- all volumes in the folder(s) which are to be exported
- all records in all folders and volumes which are to be exported
- all metadata associated with folders, volumes and records which are to be exported.

A5.54 (M) The ERMS must be able to export whole electronic folders, and groups of folders, and all associated records in one sequence of operations, such that:

- the content and appearance of the electronic records are not degraded
- all components of an electronic record, when the record consists of more than one component, are exported as an integral unit; for example, an e-mail message with associated file attachment
- all metadata associated with an electronic record is clearly linked to the record to which it belongs, so that the correct metadata can be re-associated with the correct record in the receiving system
- all structural links between records, volumes, folders and series are retained in such a way that the structure of all linked components qualifying for export can be re-built in a receiving system.

A5.55 (M) The ERMS must be able to export and transfer records that are associated with more than one folder, where this is achieved by means of a pointer, ensuring that:

- in a folder to be exported, a physical rather than virtual instance of the record is exported, resulting in an exported record not an exported pointer
- in a folder that is not to be exported, the evident association of the record with that folder, and access to the content of the record, remains unaltered

- where associated with two or more folders qualifying for export, all associations between the record and all exported folders are retained in the exported data.

A5.56 (M) The ERMS should be able to include a copy of audit trail data that is associated with records, volumes and folders as part of the export or transfer process; and must then exclude non-relevant audit trail data.

A5.57 (M) The ERMS must be able to export metadata for folders, volumes and records in an XML format.

A5.58 (M) The ERMS must also be able to export records:

- in their native format, or a current format to which they have been migrated

and in order of preference:

- in an XML format
- or where possible in a rendition where an XML format is not available. Such renditions may be achieved by:
    - capturing an appropriate rendition as part of the record capture process
    - rendering the record as part of the export process
    - exporting directly to another package which is capable of rendering the record within a controlled environment.

A5.59 (M) The ERMS must be able to export all types of records which it is able to capture, regardless of the presence of the generating application software.

A5.60 (HD) The ERMS should be able to export all folders, and groups of folders, that qualify for export at any one time, in one single sequence of steps.

A5.61 (M) The ERMS must produce a report detailing any failure completely to export or transfer any element of electronic records, volumes and folders and associated metadata that are being processed in the disposal management mechanism. The report must identify any records which have generated processing errors during export or transfer, and any folders, volumes or records that have not successfully been exported.

A5.62 (M) The ERMS must enable folders, volumes and records to be exported more than once.

A5.63 (M) The ERMS must support a two-stage transfer process, consisting of:

- export of qualifying folders, volume and records from the system
- subsequent destruction of the exported folders, volumes and records following confirmation of export

A5.64 (M) The ERMS must retain intact all electronic folders, volumes and records that have been exported in the transfer process, at least until confirmation of a successful export (i.e. pause the second stage of the process until confirmation of successful import to the recipient system following the first stage).

Destruction

A5.65 (M) The ERMS must seek confirmation of destruction from an authorized user as a mandatory step in the disposal process, before any action is taken on folders, volumes or records; and enable cancellation of the disposal process at this point if confirmation is not given.

A5.66 (M) The ERMS must ensure that any function to delete records, volumes or folders on an ad hoc basis (outside of the disposal process) is restricted to only the highest level of Administrator and that a second confirmation is required before any deletion is enacted.

A5.67 (M) The ERMS must distinguish between an ad hoc delete function, and the destruction function within the disposal process, so that each can be individually and discretely allocated to differing sets of authorized users as separate functions.

A5.68 (M) Where records are stored on re-writeable media, the ERMS must enable the complete obliteration of records, volumes, folders, and groups of folders that have been so scheduled and confirmed, so that they cannot be restored by operating system features or by specialist data recovery facilities.

A5.69 (M) Where records are stored on write-once media, the ERMS must prevent access to them so that access cannot be restored by normal use of the ERMS, by standard operating system utilities, or by any other application.

A5.70 (M) The ERMS should be capable of retaining a minimum set of metadata associated with destroyed folders, as specified in the National Archives and Records Service's minimum mandatory metadata set[28].

A5.71 (M) Where destruction is initiated from a higher level in the hierarchy, the ERMS should ensure that the correct minimum metadata is individually retained for all folders in all series that were destroyed.

[28] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.

A5.72 (M) Where an Administrator deletes a folder, the ERMS should ensure that the correct minimum metadata is retained; and that the Administrator has an opportunity to enter the reason for destruction in an appropriate metadata field.

A5.73 (HD) The ERMS should provide a facility for an Administrator to optionally archive and then delete minimum metadata for destroyed folders.

A5.74 (M) Where a pointer system is used, the ERMS must maintain complete referential integrity following all destruction processes, consistent with all the requirements in this section.

A5.75 (M) The ERMS must ensure that when a destruction process is applied to any record for which the ERMS also stores alternative renditions, all renditions of the record are also destroyed.

A6: ACCESS CONTROL

Access to ERMS

A6.1 (M) The ERMS must provide an authentication mechanism which controls access to the ERMS and which validates each user attempting access at the start of each user session, linking the user-id to a valid user profile. An individual user-id/password login is the minimum strength requirement for authentication.

A6.2 (HD) The ERMS should enable configuration of an access mechanism which supports access to the ERM system by an integrated network log-in.

A6.3 (M) The ERMS must allow:
- new users to be defined and identified
- existing users to be marked as inactive, with the effect of barring that user from subsequent entry to the ERMS
- existing users to be deleted

by an Administrator at any time.

A6.4 (HD) The ERMS should allow a user to be defined with administration rights over only a section of file plan; that is, define a local records manager.

Access control markings

A6.5 (M) The ERMS must support the definition of all access control markings required prior to their allocation to a user, series, folder or record.

A6.6 (M) The ERMS must restrict the ability to define and maintain available access control markings to an Administrator.

A6.7 (M) The ERMS must grant to each user the ability to allocate to folders and records the access control markings (which have already been defined) which that user has been allocated as access permissions.

A6.8 (M) The ERMS must not allow the allocation to folders and records of access controls by any users who are not themselves allocated those same access permissions.

A6.9 (M) The ERMS must support use of a protective marking scheme in order to control which users are allowed access to which records, folders and series, consisting of a hierarchy of security categories from unrestricted access at the lowest level to highly restricted access at the highest level.

A6.10 (M) The ERMS must support use of access control markings which identify:

- pre-defined groups of users, and separately
- individual users,

in order to control which users are allowed access to which electronic records, folders and series.

User profiles

A6.11 (M) The ERMS must require the definition of a user profile for each user known to the system. A user profile must always identify a functional role for the user, and must enable allocation of access control markings to that user; and must require information necessary for valid authentication (for example, user-id and password).

A6.12 (M) The ERMS must support the allocation of a single security category and membership of multiple pre-defined access groups, recorded in the user profile for each user known to the system; and must restrict the ability to allocate these markings to an Administrator.

A6.13 (M) The ERMS must require each user to be allocated exactly one hierarchical security category, with the default category being the lowest level of the hierarchy.

A6.14 (M) Where an ERMS enables a security category to be inherited from a role, the ERMS must ensure that a different security category can be allocated at the individual user level to replace it.

A6.15 (M) The ERMS must enable each user to be allocated membership of multiple predefined groups; but must not require a user to be a member of any pre-defined groups.

A6.16 (M) The ERMS must allow changes to be made to a user profile at any time, and must restrict this ability to an Administrator.

Roles

A6.17 (M) The ERMS must support the definition of a set of user roles, which control the assignment of rights to specific functions or groups of functions; and must restrict any ability to define or customize these roles to an Administrator.

A6.18 (M) The ERMS must ensure that all users are allocated to one or more user role(s).

A6.19 (M) The ERMS must be able to limit access to system functions and facilities, so that all users will only be able to carry out those functions which are permitted by the user role(s) to which they have been allocated.

A6.20 (M) The ERMS must support a model of user roles which enables functions to be allocated to user types[29].

A6.21 (HD) The ERMS should enable the allocation of a security category, and predefined access control group membership, to a role so that all users allocated to that role automatically inherit the access permissions of the role, and if so must ensure consistent rules of precedence between permissions granted at the role and at the individual user level.

[29] A user could for instance be listed in the Top Secret grouping according to the his/her security clearance, but could be limited to have access only to specific categories of records, folders and series. E.g only the HR Manager who has a top secret clearance has access to certain HR information, while the other managers that also have top secret clearances do not have access to the information because it does not fall within their functional areas..

Groups

A6.22 (M) The ERMS must support the definition of pre-defined access control groups which identify business or other functional groups, so that, in principle, any user can be a member of any group, and differing groups at differing times; and must restrict this ability to allocate and reallocate to an Administrator.

A6.23 (M) The ERMS must allow:
- new groups to be defined
- existing groups to be marked as inactive, which should have the effect of barring access previously allowed by that group marking
- existing groups to be deleted.

A6.24 (M) The ERMS must enable any user to be added to or removed from groups at all times.

A6.25 The ERMS should enable, but not require, the allocation of a series to a group, so that all users allocated to that group are only granted access to that series and its sub-series (i.e. to that section of the file plan).

Allocation of access control to series, folders and records

A6.26 (M) The ERMS must support the allocation of all forms of access control markings to series, folders and electronic records, including:
- security categories (protective markings)
- pre-defined access control groups, (that is, a stable list of named users)
- one or more individual usernames (that is, an *ad hoc* list of named users).

A6.27 (M) The ERMS must enable any and all combinations of protective marking, predefined user groups and individual usernames to be allocated to series, folders and records.

A6.28 (M) The ERMS must ensure that an electronic volume will always inherit the access control markings allocated to the folder which it segments.

A6.29 (M) The ERMS must enable exactly one security category to be allocated to a series, electronic record or folder, with the default category automatically being the lowest level of the hierarchy.

A6.30 (M) The ERMS must ensure that all folders created under a series inherit a security category allocated to that series by default, unless explicitly overridden at the folder level.

A6.31 (M) Where a folder has a higher security category, the ERMS must be capable of automatically upgrading the security category of a record with a lower rating to that of the folder in which it is contained.

A6.32 The ERMS should allow a configuration option, to be set by an Administrator, which allows a record to have a lower level security category than the folder in which it is contained.

A6.33 (M) The ERMS must be capable of automatically upgrading the security category of a folder to the level of the highest rating of any its contents.

A6.34 (HD) The ERMS should allow a configuration option, to be set by an Administrator, which allows a record to have a higher level security category than the folder in which it is contained.

A6.35(M) The ERMS must allow the addition of a description to an electronic folder or record as an element of metadata to indicate why a certain access restriction was placed on a folder or record, for informative use.

A6.36 (M) The ERMS must support the amendment of access control markings on series,
folders and records.

A6.37 (M) The ERMS should retain the previous access control marking(s), and the date of the amendment, as an historical metadata element for that series, folder or record.

A6.38 (HD) The ERMS should support the allocation of a security category to a series, folder or record, which is valid for a limited time period, and should automatically downgrade the marking to the lowest level security category when the time period has expired.

A6.39 (HD) The ERMS may support the allocation of a security category to a series, folder or record, which is valid for a limited time period and should automatically downgrade the marking to a lower, pre-selected, security category when the time period has expired.

A6.40 (M) The ERMS may support notification to an authorized user of the expiry of a selected time period for which a security category has been allocated to a series, folder or record, and allow the security marking to be reassessed and amended.

Custodian

A6.41 (M) The ERMS must enable, but not require, a user or group to be identified as the responsible custodian for an electronic folder, and enable this identification to be changed at a later date.

A6.42 (M) The ERMS must be able to limit access to an electronic folder or record solely to an identified responsible custodian of that folder or record.

A6.43 (M) The ERMS must allow a responsible custodian to limit access by stipulating which other users or groups can access records of which the user is custodian.

A6.44 (M) The ERMS must be capable of restricting the ability to allocate and amend access control markings (including the ability to add or remove users and groups) on electronic folders and records to the responsible custodian of the folder where one is identified, with the exception of an Administrator.

Execution of access control markings

A6.45 (M) The ERMS must allow all users (unless otherwise restricted by functional role) access to all series, folders and records which are not allocated an access control marking other than the lowest security category.

A6.46 (M) The ERMS must limit access to series, folders and records which have been allocated a security category, only to those users who have been allocated an equivalent or higher security category.

A6.47 (M) The ERMS must limit access to series, folders and records which have been allocated a pre-defined access control group, only to those users who are members of that group.

A6.48 (M) The ERMS must limit access to series, folders and records which have been allocated more than one pre-defined access control group, only to those users who are members of the allocated groups.

A6.49 (M) The ERMS must limit access to series, folders and records which have been allocated one or more individual usernames as access control markings, only to those users so named.

A6.50 (M) The ERMS must limit access to series, folder and records which have been allocated one or more forms of access control marking, only to users who have also been allocated all equivalent access control markings; and

prevent access by users who have been allocated some, but not all, the equivalent access control markings.

A6.51 (D) The ERMS should include a configuration option which defines the behavior of the access control mechanism so that:

- *either* a user who is not allowed access to a series, folder or record can never find out that it exists by means of the ERMS (i.e. the user can never see its metadata, in a search result list or at any other time)
- or a user who is not allowed access to a series, folder or record can find out that it exists by means of the ERMS (i.e. the user can see its metadata in a search result list) even though the user cannot access the contents of the record.

A6.52 (M) The ERMS must ensure that a user who is not allowed access to an electronic record or folder cannot receive any information about the record or folder as a result of a full-text search on record content, which that user would not receive through searching on metadata.

Privacy and opening of records

A6.53 (M) The ERMS must support the progressive addition of metadata to folders, records and extracts to inform promotion of access to information (PAIA), promotion of administrative justice (PAJA) and protection of privacy, including:

- information about folders and records that are automatically accessible under PAIA, which may be used as a reference to retrieve full details in a different tracking system
- indicators on disclosability of folders and records under protection of privacy rules
- information regarding the reason why certain decisions was taken.

A7: HYBRID AND PHYSICAL FOLDER MANAGEMENT

A7.1 (M) The ERMS must support the management of physical folders in a manner which is closely integrated with the management of electronic folders and electronic records.

Physical folders

A7.2 (M) The ERMS must enable the definition of physical folders and volumes, and the allocation of physical folders to a series.

A7.3 (M) The ERMS must enable the definition of hybrid folders and hybrid volumes, which are part physical and part electronic, and the allocation of a hybrid folder to a series.

A7.4 (M) The ERMS must support the use of metadata for physical and hybrid folders, and the inheritance of metadata from a series consistent with inheritance by an electronic folder.

A7.5 (M) The ERMS must support the capture and presentation of metadata for physical and hybrid folders as set out in the National Archives and Records Service's minimum mandatory metadata set[30]

A7.6 (M) The ERMS must allow a different metadata element set to be configured for physical folders than that for electronic folders; so that physical folder metadata can include information on the location of the folder; and the ERMS must record the fact of changes to such metadata in the audit trail.

A7.7 (M) The ERMS must allow both the physical and electronic folder associated together as a hybrid to use the same folder title or file plan id, but with an added indication one is a paper and the other an electronic folder.

A7.8 (M) The ERMS must ensure that creation of a new volume within either of an electronic or a physical folder which are associated together as a hybrid, automatically creates a new volume in the companion electronic or physical folder.

Markers

A7.9 (M) The ERMS must support the creation of markers – that is, a metadata profile of a physical record held outside the ERMS – and their allocation to electronic folders.

A7.10 (M) The ERMS must allow the definition of a metadata element set for markers separately from the metadata element set for electronic records; marker metadata must include information about their physical location.

A7.11 (M) The ERMS must allow markers to denote different types of physical record; examples include:

- information about a large volume paper record, map or plan
- information about a database
- information about a video.

[30] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.

A7.12 (M) The ERMS must be able to associate a marker with one or more electronic folders.

A7.13 (M) The ERMS must be able to record the fact of a change made to metadata about a marker in the audit trail.

Retrieval and access control

A7.14 (M) The ERMS must be able to search for and retrieve markers and physical folders, and electronic records and folders, by a single integrated search.

A7.15 (M) The ERMS must ensure that retrieval of a complete electronic folder also retrieves all markers associated with that folder.

A7.16 (M) The ERMS must ensure that retrieval of an electronic folder or physical folder which is part of a hybrid folder, also retrieves the companion electronic or physical folder associated with the hybrid.

A7.17 (M) The ERMS must ensure that (within the ERMS) both electronic and physical folders of a hybrid folder are allocated the same access controls.

A7.18 (M) The ERMS must be able to control user access to metadata about markers and physical folders, (within the ERMS) consistent with access controls for electronic records and folders.

Tracking and circulation

A7.19 (HD) The ERMS should support the production of barcodes for locating and tracking physical folders and volumes.

A7.20 (HD) The ERMS should support check-out and check-in facilities for physical folders and volumes, recording a specific user or location to which a physical folder or volume is checked-out, and the date on which this occurred, and displaying this information where the physical folder is retrieved by another user, unless restricted by access controls or protective marking.

A7.21 (HD) The ERMS should support a bring forward facility for physical folders and volumes, enabling a user to enter a bring forward or reserve date for a physical folder or volume, and generating a consequent message for transmission to the current holder of that folder or another authorized user, according to configuration.

A7.22 (HD) The ERMS should support a bring forward facility for electronic folders, enabling a user to enter a bring forward date for an electronic folder, so that the user receives an automatic reminder bringing the electronic folder to attention at the date to be brought forward.

A7.23 (HD) The ERMS may support an ordering facility, enabling a user to request a physical folder located with another user or a storage facility.

Disposal

A7.24 (M) The ERMS must support the allocation of a disposal schedule to a physical folder.

A7.25 (M) The ERMS must ensure the same disposal schedule is always applied to both of the electronic and physical folders associated together as a hybrid folder

A7.26 (M) The ERMS must ensure that any disposal actions on a hybrid folder are explicitly carried out on both the electronic and physical folder (within the ERMS) associated as a hybrid, at the same time and in the same manner.

A7.27 (M) The ERMS must ensure that any review decisions made on an electronic folder that is associated as a hybrid with a physical folder, are also applied (within the ERMS) to the physical folder.

A7.28 (M) The ERMS must be able to export physical folders, and retain all their associations with series and electronic folders associated as a hybrid, once exported.

A7.29 (M) The ERMS must be able to export markers, and retain all their associations with electronic folders and other electronic records, once exported.

A7.30 (M) Where an electronic folder containing markers is to be destroyed or transferred, the ERMS must ensure that the markers are destroyed at the same time as the contents of the electronic folder.

A7.31 (HD) Where a hybrid folder is to be destroyed, exported or transferred, the ERMS should require an authorized user to confirm that the physical folder of the hybrid has been destroyed, ‘exported’ or transferred before processing the electronic folder.

A7.32 (HD) Where the ERMS supports the maintenance of a minimum metadata ‘stub’ to denote the former existence of a folder, the ERMS must ensure that minimum metadata is maintained for a physical folder that has been destroyed, and for both electronic and physical folders in a hybrid folder.

A8: IMAGING AND SCANNING

A8.1 (HD) The ERMS should provide an interface to:
- one or more low volume, ad hoc, scanning system(s)
- one or more high volume production scanning system(s).

A8.2 (HD) The ERMS should provide an interface to one or more image management system(s).

A8.3 (HD) The scanning product may provide the capability to mark a document as scanned.

A8.4 (HD) The scanning product should provide the capability to classify scanned documents directly into the file plan via the ERMS.

A8.5 (D) The scanning product should alert an authorized user if there are documents that were scanned but not indexed.

A9: AUDIT

A9.1 (M) The ERMS must be able to automatically record an audit trail of events under the control of the ERMS, storing information about:
- the action which is being carried out
- the object(s) to which the action is being applied
- the user carrying out the action
- the date and time of the event.

A9.2 (M) The ERMS must be able to record in the audit trail all changes made to:
- groups of electronic folders
- individual electronic folders
- electronic volumes
- electronic records
- extracts
- metadata associated with any of the above.

A9.3 (M) In particular, the ERMS must be capable of recording information in the audit trail about the following events:
- the date and time of declaration of all electronic records
- re-location of an electronic record to another electronic folder, identifying both source and destination folders
- re-location of an electronic folder to a different series, identifying both source and destination series

- re-allocation of a disposal schedule to an object, identifying both previous and reallocated schedules
- placing of a disposal hold on a folder
- the date and time of a change made to any metadata associated with electronic folders or electronic records
- changes made to the allocation of access control markings to an electronic folder, electronic record or user
- export actions carried out on an electronic folder
- separately, deletion or destruction actions carried out on an electronic folder or electronic record, by all users including an Administrator.

A9.4 (M) The ERMS must track and record information about events in the audit trail without manual intervention, once the audit trail facility has been activated.

A9.5 (M) The ERMS must ensure that audit trail data cannot be modified in any way, or any volume of the data be deleted by any user, including an Administrator

A9.6 The ERMS should allow the extent of audit trail tracking and recording to be user-configurable, so that an Administrator can select the events for which information is automatically recorded; the ERMS must ensure that a minimum level of events includes: Create, Edit (If allowed), Copy, Move, Delete, Destroy, Export.

A9.7 (M) The ERMS must ensure that the selection for audit trail tracking, and all later changes to it, are also recorded in the audit trail.

A9.8 (M) The ERMS must maintain the audit trail for as long as required, which will be at least for the life of the electronic record or electronic folder to which it refers.

A9.9 (M) The ERMS must ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorized external personnel who have little or no familiarity with the system.

A9.10 (M) The ERMS must maintain a log of failed attempts to log-on to the ERMS.

A9.11 (M) The ERMS must be capable of producing ad hoc reports selecting all relevant information from the audit trail for:

- actions carried out by a specified user, or group of users, during a specified date and time period
- actions carried out on a specified folder, or group of folders, during a specified date and time period

- actions carried out on a specified record, during a specified date and time period.

A9.12 (HD) The ERMS should be able to export an audit trail, or volumes of an audit trail, for specified electronic records, electronic folders and groups of folders, in such a way that the exported data can itself be stored as a record.

A10: REPORTING

A10.1 (M) The ERMS must provide, besides the general reporting capabilities, a reporting capability, for Administrators and other authorized users, to provide management and statistical reports on activity and status within the ERMS.

A10.2 The ERMS should be capable of storing standard reports requests and formats, which can be run specifying varying parameters, but without additional design alteration, including parameters for:
- specific dates and date ranges
- specific users or groups of users.

A10.3 (M) The ERMS must be able to produce reports listing all series, folders and volumes, structured according to the hierarchy of the file plan.

A10.4 (M) The ERMS must be able to produce reports listing all series, folders and volumes within a section of the file plan only.

A10.5 (M) The ERMS must be able to produce reports listing all, or a restricted set of, user profiles known to the system.

A10.6 (M) The ERMS must allow reports to be generated for screen display, for printing, and for both display and printing.

A10.7 (M) The ERMS must support reporting tools for the provision of statistics on the activities of users within the ERMS, including:
- the number of electronic folders created within a given period
- the number of electronic volumes opened and closed within a given period
- the number of electronic records created by a user or groups of users, within a given period.
- the number of electronic records viewed by a user or group of users, within a given period.

A10.8 (M) The ERMS must support reporting tools for the provision of statistics on aspects of electronic records in the ERMS, including
- the number and location of electronic records by application type and application package version
- the size and capacity of electronic record stores and repositories

- the number and location of electronic folders and records by specific access control markings.

A10.9 (M) The ERMS must support reporting and analysis tools for the management of retention and disposal schedules, including:

- folders and records with disposal schedules which will come into force over a given period of time, providing quantitative reports on the volume and type of records
- statistics of review decisions made over a given period
- a list of all disposal schedules that are currently defined in the disposal schedule rule base
- a list of all series and electronic folders to which a specified disposal schedule is currently allocated
- all disposal schedules which are currently allocated to a series, groups of series, or group of folders
- all disposal schedules which are currently allocated to a record created as a specific record type
- a list of all folders for which a specified disposal action will be required over a given period

whether this information is inherited or individually allocated.

A10.10 (M) The ERMS must be capable of producing reports documenting the outcome of the export process which list series and folders successfully exported as a record of a specific export action.

A10.11 (M) The ERMS must be capable of producing reports documenting the outcome of the destruction process, which list series and folders successfully destroyed.

A11: USABILITY

A11.1 (M) The ERMS must follow the accepted standard rules for the user interface of each operating system or platform for which it is supplied.

A11.2 (M) The ERMS must consistently present user interface menus, commands and other facilities in all volumes of the application.

A11.3 (M) The ERMS must use consistent terminology to label functions and actions in all volumes of the application.

A11.4 (HD) The ERMS should provide a context-sensitive online help facility.

A11.5 (D) The ERMS may allow customization of the contents of the help facility, by the addition of new, or editing of existing, text.

A11.6 (M) The ERMS must produce error messages which are meaningful and appropriate, and should offer immediate prompts for actions to resolve the error wherever possible.

A11.7 (M) Where validation errors are detected, the ERMS must unambiguously describe the nature of the error, and offer a method of correcting the error, or canceling the action.

A11.8 (HD) The ERMS should be capable of removing the visibility of functions from users who do not have access to those functions in their allocated user role.

A11.9 (HD) The ERMS should not, routinely, allow the intermediate steps of a function to be carried out if the user will not be allowed to complete the function because that function is disallowed by role allocated to that user.

A11.10 (M) The ERMS must provide facilities for end users and Administrators which are intuitive and easy to use, and require as few actions as possible to carry out the function to the required standard; in particular, in normal operation, the ERMS must be able to:

- capture and declare (apart from selection of a folder or entry of metadata attributes) a record within three mouse clicks or keystrokes
- be capable of presenting all mandatory metadata elements for record capture with minimum demands on the user
- display the contents of a record from a search result list within three mouse clicks or keystrokes
- display metadata for a folder or record within three mouse clicks or keystrokes.

A11.11 (M) Where on-screen windows are employed, the ERMS must ensure that where an end user is able to re-size and re-locate windows, the contents of those windows remain correctly aligned.

A11.12 (M) The ERMS must support multiple simultaneous display of folders and records.

A11.13 (HD) The ERMS should support a ‘drag and drop’ method of manipulating folders and records, where this is appropriate for the platform supported.

A11.14 (HD) The ERMS may support the ability to define multiple user views of the series and folder structure, with no effect on the common corporate file plan structure.

A11.15 (HD) The ERMS should be usable with a wide range of common accessibility software features.

A11.16 (HD) The ERMS may support the use of, and navigation by, hyperlinks and other cross-references that are contained in records at time of declaration.

A11.17 (HD) The ERMS should automatically present default values for data entry fields where logically possible, as specified in the National Archives and Records Service's minimum mandatory metadata set[31].

A11.18 (HD) The ERMS should support the pre-definition of a set of allowed values for a particular metadata field by an Administrator, and the implementation of these values as a selection list (i.e. a 'pick list').

A11.19 (M) The ERMS must provide an interface to standard e-mail clients, including MS Outlook and Exchange, which enables e-mail messages to be captured directly into the ERMS from the e-mail client.

A11.20 (M) The ERMS must be capable of integrating with the standard office system packages (for example, MS Office) which the ERMS supports, so that the record can be captured by the ERMS by use of the Save facility.

A11.21 (M) The ERMS must be capable of generating an e-mail message from within the application in order to attach, as options:
- one or more records stored in the ERMS (in the same message)
- active pointer(s) to one or more records stored in the ERMS
- metadata for one or more records stored in the ERMS.

A12: DESIGN AND PERFORMANCE

A12.1 (M) The ERMS must provide a robust and flexible architecture that can evolve to meet the needs of a changing organizational environment, appropriate to the types of implementation for which the ERMS is intended

Integrity

A12.2 (M) The ERMS must enforce data integrity, referential integrity and relational integrity at all times.

A12.3 (M) The ERMS must ensure that all occurrences of series, folders, records, volumes and extracts are allocated a system identifier which is unique within the system.

[31] The draft minimum mandatory metadata set is available on NARS's website http://www.national.archives.gov.za/rms/minimum_mandatory_metadata.htm and will be finalized when the ISO metadata standard is adopted by NARS.

A12.4 (HD) When the ERMS automatically generates an identifier which is available for meaningful operational use by a user or Administrator, the ERMS should allow an Administrator to configure the pattern and starting number(s) or character(s).

A12.5 (M) The ERMS must store calendar years in a four digit format (YYYY) in any metadata field that contains a date.

A12.6 (M) The ERMS must be capable of storing dates that refer to years in the previous, current and subsequent centuries, and must correctly process these dates at all times.

Interfaces

A12.7 (M) The ERMS must support a remote log-in facility, which provides the standard range of functionality which the ERMS offers

Disaster recovery

A12.8 (M) The ERMS must support automated back-up and recovery facilities for all series, folders, records, metadata, audit trails and configuration settings held in the ERMS, either provided by the ERMS itself or by facilities in its environment with which it can interface.

A12.9 (M) The ERMS must support a capability for separate physical storage of back-up Data.

A12.10 (HD) The ERMS should allow an Administrator to:
- specify the frequency of back-up
- select elements of the ERMS to be backed-up.

A12.11 (M) The ERMS must support facilities for an Administrator to restore the whole ERMS from back-ups following a system failure.

A12.12 (M) The ERMS must support facilities for an Administrator to restore the whole ERMS from the most recent back-up state to the point of system failure.

A12.13 (M) The ERMS must be able to determine any updates to the data which are unable to be restored / rebuilt, and provide notification to an Administrator.

A12.14 (M) The ERMS must support restoration of audit trail information by means of the back-up and recovery facilities.

Storage

A12.15 (HD) The ERMS should support a distributed repository with multi-site service.

A12.16 (HD) The ERMS should support caching of frequently and recently used repository content.

A12.17 (HD) When querying a remote repository, the ERMS should minimize the amount of data exchange required.

A12.18 (M) The ERMS must provide facilities for monitoring storage facilities, and automatically alert an Administrator when a capacity threshold is reached, or when an error condition requiring attention occurs.

Performance

A12.19 (M) The ERMS must provide evidence of adequate performance and response times for commonly performed functions under the normal operating conditions for which it is intended. A benchmark for normal operating conditions is:

- 75% of the user population actively using the system
- total record volume to be expected after 5 years use stored
- multiple, concurrent and representative active use of system functionality

Benchmark metrics for performance are:

- time taken to display a graphical view of the series and folder structure
- time to store a set of standard documents at capture and/or declaration
- time to return a search response for a simple search
- time to return a search response for a complex (Boolean) search
- time to display a recently captured record
- time to display an 'inactive' record.

Scalability

A12.20 (M) The ERMS must provide evidence of the degree of scalability which it can support over time, as organizational needs change and develop. Benchmark metrics for scalability are:

- number of geographical locations at which users can be supported, while maintaining the performance metrics demonstrated
- total size of the record repository which can be supported, in Gigabytes or Terabytes, while maintaining the performance metrics demonstrated

- number of total users which can be supported, while maintaining the performance metrics demonstrated
- systems management overhead in maintaining a growth rate for the number of records and users anticipated in the first five years of operation
- amount of re-configuration and downtime required to maintain a growth rate for the number of records and users anticipated in the first five years of operation
- amount of re-configuration and downtime required to make bulk changes to organizational structures, series and folder structures, and user roles with the number of folders, records and user anticipated after five years of operation.

A13: COMPLIANCE WITH OTHER STANDARDS

A13.1 (M) Wherever relevant, the ERMS must comply with, or support compliance with, the following standards :

- ISO 17799 / BS7799 Information Security Management
- ISO 15489 Information and Documentation : Records Management
- ISO 9001 : 2000 Quality management systems : Requirements

These contextual standards form the framework within which these ERMS requirements operate.

A13.2 (HD) Wherever relevant, the ERMS should comply with, or support compliance with, the following standards:

- ISO 23950 Information and Documentation : Information retrieval (Z39.50): application service definition and protocol specification
- ISO 2788 Documentation : Guidelines for the establishment and development of monolingual thesauri
- ISO 5964 Documentation : Guidelines for the establishment and development of multilingual thesauri
- ISO 9075 Information technology: database languages: SQL

These contextual standards form the framework within which these ERMS requirements operate

B: OPTIONAL MODULES

The optional modules are not part of the core records management requirements. An IDRMS may fulfill the core requirements without fulfilling the optional requirements. However if a IDRMS whishes to demonstrate a capability of providing one or more of the optional requirements, it must fulfill all of the mandatory requirements within that module. These optional requirements do not attempt a full definition of authentication and encryption technologies. The aim is to identify only requirements which overlap in functionality with, or which have an

impact on, electronic records management (E.g. issues related to the reliability and authenticity of electronic records and metadata.)

.

B1: AUTHENTICATION AND ENCRYPTION

This module is not a mandatory part of the core records management requirements, but is mandatory if a solution whishes to prove compliance to the Electronic Communications and Transactions Act.

Electronic signatures

B1.1 (M) The ERMS must be capable of configuration to select the extent to which information about the authentication process is routinely stored, including levels that:

- retain the fact of successful authentication only with the record
- retain information about the authentication process with the record
- retain all authentication data, including signatures, with the record.

B1.2 (M) The ERMS must be able to retain the fact that an electronic signature has been verified as authentic, with the electronic record with which the signature is associated.

B1.3 (M) The ERMS must be able to retain and preserve information about the process of verification for an electronic signature, including either or both:

- the Certification Authority with which the signature has been validated
- the date and time of validation.

B1.4 (M) The ERMS must be able to store with the electronic record:

- the digital signature associated with that record
- the digital certificate verifying the signature
- any confirming counter-signatures appended by the certification authority in such a way that they are capable of being retrieved in conjunction with the record, and without prejudicing the integrity of a private key.

B1.5 (M) The ERMS must be capable of interfacing with electronic signature technologies, so that information about the authentication process is captured automatically.

B1.6 (M) The ERMS must be capable of interfacing with PKI-based electronic signature technologies.

B1.7 (M) The ERMS must be capable of checking the validity of a digital signature at the time of declaration of the record.

B1.8 (M) The ERMS must be capable of demonstrating the continued integrity of an electronically signed record, even though allowable changes have been made to the metadata for that record (but not to the content).

B1.9 The ERMS should be capable of applying an electronic signature to a record, or folder of records, during the process of export, in such a way that the signature can be validated externally to the ERMS.

Electronic watermarks

B1.10 (M) The ERMS must be capable of storing records bearing electronic watermarks, and of retaining information about the watermark with the record.

B1.11 (D) The ERMS should be capable of applying an electronic watermark to a record, or group of records, during the process of export from the ERMS, without any subsequent loss of access in a receiving system which is different from the ERMS.

Encryption

B1.12 (M) The ERMS must be able to ensure the capture of, and declare, an encrypted record directly from a software application which has an encrypting capability, and restrict access to those users listed as holding the relevant decryption key.

B1.13 (M) The ERMS must be capable of allowing encryption to be removed when a record is captured or declared directly from a software application.

B1.14 (M) Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the ERMS, the ERMS must be capable of restricting access to that record to users listed as holding the relevant decryption key, in addition to any other access control marking allocated to that record.

B1.15 (M) Where an electronic record in encrypted form has been transmitted by or captured from, a software application which interfaces with the ERMS, the ERMS must be able to keep as metadata with that record:

- the fact of encrypted transmission or capture
- the type of algorithm
- the level of encryption used.

B2: FAX INTEGRATION

B2.1 (HD) The ERMS may provide an interface to a fax server facility.

B2.2 (HD) The fax integration should provide the capability to classify scanned documents directly into the file plan via the ERMS.

B2.3 (HD) The fax integration should provide the capability to send outbound faxes directly from the ERMS after they have been classified into the file plan.

4. REFERENCE DOCUMENTS

SANS (ISO) 15489 *Information and documentation — Records management — Part 1: General,* 2001
SANS (ISO) 15489 *Information and documentation — Records management — Part 2: Guidelines,* 2001
National Archives and Records Service: *Records Management Policy Manual*, April 2004
National Archives and Records Service: *Managing electronic records in governmental bodies: Policy Guidelines*, April 2003