REPUBLIC OF NAMIBIA

MINISTRY OF EDUCATION

NATIONAL ARCHIVES OF NAMIBIA

Draft Records Management Policies

Part A

Records and Archives Management Policy

Part B

E-Records Management Policy for E-Governance

Part C

E-records Management Guidelines

Part D

Functional Requirements for Electronic Records Management Systems

The draft policies and guidelines compiled in this document are components of the ongoing process of policy formulation at the National Archives of Namibia to bring the records management in the Government of the Republic of Namibia in line with the requirements of Vision 2030, technological innovation, administrative efficiency and international developments in the fields of citizens' rights and the combating of corruption.

Part A: Records and Archives Management Policy outlines the general policy for records management, regardless of the format (paper or electronic). It is an internationally accepted principle that a successful transition to electronic records management requires a functional general records management framework.

Part B: E-Records Management Policy for E-Governance outlines the principles which are specifically applicable for electronic records management.

Part C: E-Records Management Guidelines specifies details for the handling of electronic records. The Guidelines deal with the practicalities and procedures in two scenarios: firstly a brief outline of the tasks of an Electronic Records Management System (ERMS), secondly detailed guidelines for handling electronic records without a dedicated ERMS.

Part D: Functional Requirements for Electronic Records Management Systems. This document details the tasks an ERMS is expected to perform, and the technical details required to enable long-term archival storage of permanent records. It is meant as a benchmark test guide for the purchase of electronic records management system software.

Part A

Records and Archives Management Policy

Part A

Records and Archives Management Policy

Table of contents

Executive summary

This policy is to give guidance government ministries, offices and agencies that are required to manage records that are generated electronically. The policy draws its mandate from various legislative and regulatory instruments including the Archives Act (1992). It is also informed by the International Standards Organization (ISO) standard for records management (ISO 15489), best practice guidelines and assessment tools from the International Records Management Trust (IRMT) as well as various international best practice policies and guidelines including those from Australia, Canada, UK, and South Africa.

The policy document has four main sections. The first section is the introduction which provides information on the effective date, versioning and ownership of the document as well as the outlining the legal and regulatory framework from which it draws its mandate. In addition, it has an outline of definitions and summary of benefits of good records management. The second section covers five broad policy statements relating strategy, legislative and regulatory framework compliance, systems design, interoperability and skills and competencies. The third section provides direction on the monitoring and assessment requirement in order to assist government ministries, offices and agencies to comply with the policy. The fourth section is an outline of references used to develop this policy which fall under the general categories of legislation and regulations, national policies, international standards and international best practise.

This policy is provided as an introductory text to a set of policy and guideline documentation by the National Archives relating to records and archives management specifically.

1.0 Introduction to records and archives management

Good record keeping and management go hand in hand with the practice of keeping archives, which are the nation's memory. Archives services are very widely used, for academic research, education, pursuit of family history, business, legal and other purposes. Good record keeping is also essential component of policy making, efficiency, accountability and transparency in government, local and central Bad record keeping and lost information can lead to poor performance and, at worst, to disruptive crises and scandals.

Records and archives make a valuable contribution to the Government's important policy objectives, including modernisation of public services, open and accountable government, education and social inclusion. They help enable all public sector bodies to meet new and demanding standards for corporate governance, and are essential underpinning to meeting many auditing requirements and validating performance in many important areas of work. This is not just a questions of records of central government, but of records of key actions taken by all public authorities, at central, regional and local levels.

The importance of records as evidence of government activity is widely appreciated today. Records provide citizens with the means not only of holding the government to account for its conduct but also, in many cases, of safeguarding their individual rights. New legislation on freedom of information and privacy, in many countries, give citizens the right to see information and records on a wide variety of subjects. These records, and easier access to them, facilitate the reasonable expectation of a democratic society that government should be accountable for its actions.

There are many competing claims on the government's finances, and all government bodies must show that they are achieving value for money for the taxpayers. This includes the National Archives and records professionals throughout the public sector, who must all demonstrate that they are making the best possible use of public funds. In practical terms, this means that there should be effective records management, that the operational benefits of this should be maximised, and that those records of most historical and cultural value to present and gure generations should be kept and treasured.

This policy is to give guidance government ministries, offices and agencies that are required to manage record. The policy draws its mandate from various legislative and regulatory instruments including the Archives Act.

Additionally, this policy is informed by the International Standards Organization (ISO) standard for records management (ISO 15489), best practice guidelines and assessment tools from the International Records Management Trust (IRMT) as well as various international best practice policies and guidelines including those from Canada, UK, and South Africa.

1.1 Effective date, version, ownership and revisions of the framework

This policy takes effect….

This policy will be subject to review two years from the date of its approval.

This policy is mandated by the Archives Act and owned by the National Archives, which is responsible for its further development.

1.2 Acknowledgement

This Records Management Policy is based on similar publications developed internationally and have been modified to suit the records management environment of the Namibian Government, in accordance with the requirements of the National Archives Actt.

The National Archives would like to acknowledge the following publications in the development of this document

- Australia's Mosman Municipal Council's Records and Information Management Policy (2002)
- Australia's National Archives Recordkeeping Policy (2005)
- Canada's Management of Government Information Policy (2003)

- South Africa's Records Management Policy Manual (2004)
- UK's Lord Chancellor's Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000 (2002)

1.3 Legislative and regulatory framework

According to the Archives Act (Sec 3.1a) the Archives is responsible for the regulation, execution and administration of matters concerning the custody and care of public records generated and maintained at all levels of government.

In addition, other legislative instruments have specific requirements

- State Finance Act (Part 1 Sec 4) states "the PS shall keep proper accounts of all transactions in relation to State moneys by means of a system of account books, accounts and registers approved with the Treasury after consultation with the Auditor General"
- Public Service Act (Part 1 Sec 5.2 m) requires "the keeping of records of staff members employed in posts on or additional to the establishment."

1.4 Definitions

Archives: records of enduring value selected for permanent preservation

Authentic record: record one that can be proven: To be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported. Authenticity is conferred on a record by its mode, form, and/or state of transmission and/or manner of preservation and custody

Document: information created, received, and maintained which can be treated as a unit regardless of medium or characteristics.

National Archives: Institution mandated by the Archives Act (1992) and responsible for the regulation, execution and administration of matters related to the custody and care of all public records.

Record: information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business.

Records management: field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of record, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Reliable record: record whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

1.5 Benefits of good records management

Good record management enable the government ministries, offices, and agencies to

- Conduct business in an orderly, efficient, and accountable manner,
- Deliver services in a consistent and equitable manner,
- Support and document policy formation and managerial decision making,
- Provide consistency, continuity and productivity in management and administration,
- Facilitate the effective performance of activities throughout the organization,
- Provide continuity in the event of a disaster,
- Meet legislative and regulatory requirements including archival, audit and oversight activities,
- Provide protection and support in litigation including the management of risk associated with the existence of, or lack of, evidence of organizational activity,
- Protect the interest of the organization and the rights of employees, clients, and present and future stakeholders,
- Support and document current and future research and development activities, developments and achievements, as well as historical research,
- Provide evidence of business, personal and cultural activity, and
- Maintain institutional and/or national collective memory.

2.0 Policy statements for e-records management

Government ministries, offices and agencies must manage records and information in a privacy protective manner that supports informed policy and decision-making and the delivery of high quality programs, services, and information through a variety of channels.

It is the policy of the government that ministries, offices and agencies:

- manage records to facilitate equality of access and promote public trust, optimize records and information sharing, and reduce duplication;
- ensure that record created, acquired, or maintained to meet programme, policy, and accountability requirements is authentic and reliable;
- manage records, regardless of medium or format, to ensure its authenticity, accuracy, integrity, clarity, and completeness for as long as it is required by the *National Archives Act, National Library Act*, as well as other laws and policies;
- document decisions and decision-making processes throughout the evolution of policies, programmes, and service delivery;
- implement governance and accountability structures for the management of records, including during collaborative service delivery arrangements or when record is shared within government ministries, offices and agencies as well as other governments, or non-governmental organizations;
- protect essential records to ensure the continuity of key services and business operations;
- preserve records of enduring value to the nation and it citizens;
- dispose of record no longer required for operational purposes in a timely fashion;
- foster supportive environments for record management and ensure that employees meet their responsibilities for managing record; and
- assess the effectiveness and efficiency of the management of records throughout its life-cycle.

This policy for managing records is necessary in order to

2.1 Enhancing public trust

To deliver programs, services, and record cost-effectively and consistent with the needs of citizens, institutions must:

- ensure the quality, consistency and availability of records across delivery channels;
- organize records to provide clarity, context, and convenient access to relevant, comprehensive, and timely record and services;
- re-use and share records to the greatest extent possible, in accordance with legal and policy obligations;
- document decisions and decision-making processes;
- preserve the integrity of records, particularly when it is used in collaborative endeavours within government ministries, offices and agencies as well as other governments, or non-governmental organizations;
- ensure the appropriate security, protection, and disposition of records.

2.2 Managing records throughout their life cycle

To ensure the effective and efficient management of records, regardless of medium or format, throughout its life cycle, institutions must:

a) include records management considerations in the planning cycle to ensure that:

- records management requirements are incorporated at an early stage in the development of new or modified government policies, programs, services, and technology-based systems;
- governance and accountability structures are in place for the management of records; and
- opportunities for common infrastructures are maximized to optimize the interoperability of records and information management systems.

b) collect, create, receive and capture records in ways that:

- support service delivery, informed policy and decision making, and business, legal, and accountability requirements;
- ensure its relevance, reliability, and completeness;
- optimize its sharing and re-use, in accordance with policy and legal obligations;
- document decisions and decision-making processes to account for government operations, reconstruct the evolution of policies and programs, support the

continuity of government and its decision-making, and allow for independent audit and review; and

- reduce the response burden on the public by avoiding the unnecessary collection of record.

c) organize, use, and disseminate record by:

- establishing a co-ordinated and comprehensive approach to describing the institution's record;
- maintaining a current and comprehensive classification structure or structures, including metadata; and
- providing users with timely and convenient access to records and information, in accordance with legal and policy obligations.

d) maintain, protect, and preserve record to:

- ensure its usability, including the usability of encrypted records and information, over time and through technological change;
- ensure that record of enduring value to the nation or its citizens is available for current and future use;
- safeguard essential records; and
- safeguard it from improper disclosure, use, disposition or destruction, in accordance with legal and policy obligations.

e) ensure disposition of record by:

- adhering to departmental retention and disposition plans, the National Archives-approved Records Disposition Authorities, and other legal and policy obligations to ensure the timely disposition of record that is no longer required by the institution;
- transferring to the National Archives records it has designated as having historical value;
- transferring to the National Library publications that libraries of federal institutions have declared surplus; and
- considering its transfer to non-federal government organizations, subject to legal and policy obligations.

f) assess the effectiveness and efficiency of the management of records throughout its life cycle by:

- establishing accountability frameworks to ensure the appropriate management of records; and
- identifying, documenting, and reporting on specific risks, vulnerabilities, and other significant management issues and undertaking corrective action if required.

3.0 Monitoring or auditing for e-records management

The current e-Governance policy requires baseline information on e-readiness in order to establish the gap between the objectives and current situations. This gap analysis will be used to refine action plans. The strategy specifically mandates the Head of National Archives with these activities. (pg 45)

The National Archives of Namibia is responsible for actively monitoring the overall situation to maintain an ongoing awareness of the state of electronic records management practices and controls across government ministries, offices and agencies.

The monitoring process will be periodically conducted using either

a) Records Management Capacity Assessment System as is described in section 4.4.2.1 of this policy, and/or
b) E-records readiness assessment tool as is described in section 4.4.2.2 of this policy

Additionally, it is mandatory that before there is any implementation of an e-records management system or software package, an assessment is conducted to establish the organizational e-record readiness aptitude. This assessment is critical because

a) it will identify intrinsic organizational issues which are often not addresses merely through the introduction of a software application e.g. procedures for determining authenticity, compliance with legislation, human skills development
b) it will be useful to provide a snap shot of the situation as it existed before technological intervention and use that to assess whether the intervention was successful at the end of the intervention.

At the end of each assessment exercise, the National Archives will communicate the findings to the assessed government ministry, office or agency evaluated as well as the Minister responsible for Archives.

4.0 References

This policy should be read in conjunction with relevant pieces of legislation, regulations, national policies and international standards.

4.1 Relevant national legislation and regulations

- Archives Act
- State Finance Act
- Public Service Act

4.2 International policies

- South Africa's Records Management Policy (2004)

4.3 International standards and best practise

4.3.1 Definitions and strategies

Definitions and strategies were based on

- Standards by International Standards Organization's and specifically ISO 15489: Part 1 and ISO 15489: Part 2
- Research work conducted by International Research on Permanent Preservation of Authentic Records in Electronic Systems - InterPARES (both in InterPARES 1 that lasted between 1999 and 2001, as well as InterPARES 2 which began in 2002 and ends in December 2006)

4.3.2 E-records assessment methodologies

The e-records assessment methodologies adopted in this policy have been developed by the International Records Management Trust. These are

4.3.2.1 Records Management Capacity Assessment System

This is a software application developed from funding from the World Bank as an objective means of assessing the strengths and weaknesses of records management systems. Its framework is based on maturity model principles and has objective capacity checks reliant on three international standards, from the International Standards Organization (ISO 15489), from the European Union (Model Requirements for Electronic Records-MOREQ), and another from Canada (Information Management Capacity Check-IMCC)

4.3.2.2. E-record readiness assessment tool

This is a simplified assessment tool developed from funding from the Commonwealth Secretariat been designed to be used in conjunction with existing e-government readiness tools to provide a simple, high-level assessment that will determine whether a government or public agency's records and information management infrastructure is capable of supporting e-government initiatives.

Part B

E-Records Management Policy for E-Governance

Part B

E-Records Management Policy for E-Governance

Table of contents

Executive summary

E-Governance has been recognized as a unique opportunity for governments the world over to support and simplify administration, service delivery, and interaction between different parties including the government itself, citizens and business. By using electronic means to improve this services and interactions, economic, political and administrative authorities are appropriately and expeditiously supported in order to better manage the affairs of the country at all levels, national as well as local.

However, effective governance is based on evidence. This evidence is found in records. In an electronic environment, such records need to be appropriately generated and maintained in order to fulfill the legal mandate of public offices as well as provide evidence of administrative transactions.

These e-records could, for example, be used to confirm pensions and other entitlements, register births and deaths, verify citizenship, certify voting rights, enable the collection of taxes and censuses, support financial management and audits help resolve land claims, support litigation, document intergovernmental agreements, enable economic planning, document development, and support countless other information-intensive activities. Unless there is adequate infrastructure for managing e-records, the intended benefits of e-government will be compromised.

The speed at which information technologies and e-records are being adopted around the world is not being matched by the skills and infrastructure needed to manage them. E-records must remain accessible and usable as long as they are needed for business or legal purposes; some need to be reserved over the long term or permanently. If e-records are to survive and be valid in the future, government ministries, offices and agencies must address issues such as media instability and deterioration, obsolescence and incompatibility of hardware, software, data formats, and storage media, lack of metadata or contextual information and lack of clearly assigned responsibilities and resources for long-term preservation.

This policy is to give guidance government ministries, offices and agencies that are required to manage records that are generated electronically. The policy draws its mandate from various legislative and regulatory instruments including The E-Governance Policy for the Public Service of Namibia (2005) and the Archives Act

(1992). It is also informed by the International Standards Organization (ISO) standard for records management (ISO 15489), best practise methodologies from an international research project on permanent preservation of records in electronic systems (InterPARES), best practice guidelines and assessment tools from the International Records Management Trust (IRMT) as well as various international best practice policies and guidelines including those from Canada, UK, and South Africa.

The policy document has four main sections. The first section is the introduction which provides information on the effective date, versioning and ownership of the document as well as the outlining the legal and regulatory framework from which it draws its mandate. In addition, it has an outline of definitions and summary of benefits of good records management and perquisites for good electronic records management. The second section covers five broad policy statements relating strategy, legislative and regulatory framework compliance, systems design, interoperability and skills and competencies. The third section provides direction on the monitoring and assessment requirement in order to assist government ministries, offices and agencies to comply with the policy. The fourth section is an outline of references used to develop this policy which fall under the general categories of legislation and regulations, national policies, international standards and international best practise.

This policy is provided as an introductory text to a set of policy and guideline documentation by the National Archives relating to management of e-records specifically and records management in general.

1.0 Introduction to e-records management

E-Governance has been recognized as a unique opportunity for governments the world over to support and simplify administration, service delivery, and interaction between different parties including the government itself, citizens and business. By using electronic means to improve this services and interactions, economic, political and administrative authorities are appropriately and expeditiously supported in order to better manage the affairs of the country at all levels, national as well as local.

However, effective governance is based on evidence. This evidence is found in records. Reliable record management systems provide evidence that is crucial to accountable, transparent democracies. Initiatives aimed at enhancing economic performance, increasing government accountability, and strengthening civil society—such as anticorruption efforts, administrative and civil service reform, decentralization, electronic government, legal and judicial reform, public expenditure management, tax policy and administration, and access to information—all rely on access to accurate evidence. Evidently, effective records management is a crosscutting issue

As government ministries, offices and agencies increasingly deliver services through the deployment of e-governance strategies, it is critical that evidence of these electronically delivered service transactions are appropriately management. This evidence that is be found in e-records could be used to confirm pensions and other entitlements, register births and deaths, verify citizenship, certify voting rights, enable the collection of taxes and censuses, support financial management and audits help resolve land claims, support litigation, document intergovernmental agreements, enable economic planning, document development, and support countless other information-intensive activities. Unless there is adequate infrastructure for managing e-records, the intended benefits of e-government will be compromised.

The speed at which information technologies and e-records are being adopted around the world is not being matched by the skills and infrastructure needed to manage them. E-records must remain accessible and usable as long as they are needed for business or legal purposes; some need to be reserved over the long term or permanently. If e-records are to survive and be valid in the future, government ministries, offices and agencies must address issues such as media instability and

deterioration, obsolescence and incompatibility of hardware, software, data formats, and storage media, lack of metadata or contextual information and lack of clearly assigned responsibilities and resources for long-term preservation.

This policy is to give guidance government ministries, offices and agencies that are required to manage records that are generated electronically. The policy draws its mandate from various legislative and regulatory instruments including The E-Governance Policy for the Public Service of Namibia (2005) and the Archives Act.

Additionally, this policy is informed by the International Standards Organization (ISO) standard for records management (ISO 15489), best practise methodologies from an international research project on permanent preservation of records in electronic systems (InterPARES), best practice guidelines and assessment tools from the International Records Management Trust (IRMT) as well as various international best practice policies and guidelines including those from Canada, UK, and South Africa.

1.1 Effective date, version, ownership and revisions of the framework

This policy takes effect….

This policy will be subject to review two years from the date of its approval.

This policy is mandated by the Archives Act and owned by the National Archives, which is responsible for its further development.

This policy will be maintained in line with The E-Governance Policy for the Public Service of Namibia published by the Office of the Prime Minister in 2005.

1.2 Legislative and regulatory framework

According to the Archives Act (Sec 3.1a) the Archives is responsible for the regulation, execution and administration of matters concerning the custody and care of public records generated and maintained at all levels of government.

In addition, other legislative instruments have specific requirements

- State Finance Act (Part 1 Sec 4) states "the PS shall keep proper accounts of all transactions in relation to State moneys by means of a system of account books, accounts and registers approved with the Treasury after consultation with the Auditor General"
- Public Service Act (Part 1 Sec 5.2 m) requires "the keeping of records of staff members employed in posts on or additional to the establishment."
- The E-Governance Policy for the Public Service of Namibia states
    - "DPSITM in conjunction with the National Archives will ensure that every e-government project will incorporate a suitable records management component" (pg. 41)
    - "DPSITM in conjunction with the National Archives will ensure that archival transfer of electronic records and their continued availability through hardware and software emulations. Software license agreements must take these concerns into account." (pg.41)
    - In the implementation framework the first step of implementation requires a base line study which is to be done in consultation with Head of National Archives (pg. 46)

1.3 Definitions

Archives: records of enduring value selected for permanent preservation

Authentic record: record one that can be proven: To be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported. Authenticity is conferred on a record by its mode, form, and/or state of transmission and/or manner of preservation and custody

Document: information created, received, and maintained which can be treated as a unit regardless of medium or characteristics.

Electronic document management system: system that produces, processes, or stores documents electronically

Electronic records management system: system that preserves security, authenticity, context and integrity of electronic records

Electronic records: records generated and stored in electronic form

Electronic system: system that produces, processes, or stores information electronically.

National Archives: Institution mandated by the Archives Act (1992) and responsible for the regulation, execution and administration of matters related to the custody and care of all public records.

Record: information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business.

Records management: field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of record, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Reliable record: record whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

1.4 Benefits of good records management

Good record management enable the government ministries, offices, and agencies to

- Conduct business in an orderly, efficient, and accountable manner,
- Deliver services in a consistent and equitable manner,
- Support and document policy formation and managerial decision making,
- Provide consistency, continuity and productivity in management and administration,
- Facilitate the effective performance of activities throughout the organization,
- Provide continuity in the event of a disaster,
- Meet legislative and regulatory requirements including archival, audit and oversight activities,

- Provide protection and support in litigation including the management of risk associated with the existence of, or lack of, evidence of organizational activity,
- Protect the interest of the organization and the rights of employees, clients, and present and future stakeholders,
- Support and document current and future research and development activities, developments and achievements, as well as historical research,
- Provide evidence of business, personal and cultural activity, and
- Maintain corporate or collective memory.

1.5 Prerequisites for good electronic record management

Electronic records are fragile, can easily be overwritten, lost or become inaccessible through technology change. Therefore good electronic records management requires:

a) a clear understanding of the nature electronic records, and the information which should be captured as records in order to document the business transactions
b) that the procedures to routinely capture these records are designed into the electronic systems generating the records, and these procedures are easy and understandable to follow
c) electronic record management systems that are designed to management reliable and authentic records, ensuring that the integrity and reliability of electronic records is secured.
d) a strategy to ensure that electronic records will remain accessible and usable for as long as they are needed
e) the ability to apply appropriate appraisal, scheduling and disposal procedures to managed electronic records
f) a culture of best practice records management among managers and end users

2.0 Policy statements for e-records management

Electronic records are generated in the course of affairs of government ministries, offices and agencies. They need to be captured managed and preserved in an organized system which maintains their integrity and authenticity, retaining their value as retrievable corporate records.

2.1 Policy on legislative and regulatory framework compliance for e-records management

Government ministries, offices, and agencies will need to establish mechanisms of compliance to National Archives Act 12 of 1992 and any current or future Acts that regulate the generation and maintenance of records. These may include, but are not limited to, copyright and intellectual property rights, freedom of information legislation, privacy and data protection, e-commerce.

Compliance will ensure the development of an integrated legislative and regulatory framework for managing information and not see these legal instruments as separate strands of activity.

Critical in this framework is the existence of legal and regulatory instruments that
a) recognise e-records as being legally admissible in the event of court proceedings
b) identify processes of determining the e-records' authenticity and/or reliability dimensions which may include, but are not limited to, electronic signatures, digital watermarks, encryption as well as trusted third parties such as certification authorities.

2.2 Policy on strategy for e-records management

Government ministries, offices, and agencies will need to establish a formal strategy in compliance with this policy for maintaining electronic evidence as corporate records.

This strategy will provide guiding principles whenever new structures and systems are developed or whenever existing ones change. An important element of the corporate strategy is the existence of a mechanism for assessing and strengthening compliances, to assess the extent to which the strategy is followed, and to provide the basis for monitoring achievement of strategy goals.

2.3 Policy on systems design for e-records management

Government ministries, offices, and agencies, when implementing new systems, will need to establish a platform for high quality electronic records management. This will also prevent many of the problems experienced in existing systems from recurring.

Considering that electronic records management requirements are not sufficiently recognised in determining the functional requirements for existing or new systems, it is important to ensure that in all new systems, the ability to manage electronic records is a visible thread in the design, and that it permeates all aspects of the implementation.

2.4 Policy on interoperability for e-records management

Government ministries, offices, and agencies will need to comply with common functional requirements that ensure standard interoperable formats for maintaining accessibility that support the exchange and eventual migration of records between technological platforms as software and hardware change or are replaced.

Considering that government ministries, offices, and agencies will increasingly offer integrated services, it is critical that systems are able to share and exchange records. Export and import between records management systems will be much simplified by a common metadata structure and a common vocabulary- by using standard ways of categorising descriptive elements and standard term for their description. This will also be important for migration of electronic records to new hardware/software platforms.

2.5 Policy on skills and competencies for e-records management

Government ministries, offices, and agencies will need to ensure that the required skills and competencies are present to manage electronic records. This requires both the creation and filling of appropriate staff positions by

government ministries, offices and agencies. In addition, there should be adequate transfer of knowledge by systems providers.

Considering that in a fully electronic environment, new record management skills are required of end users as creators and users of records, there are significant training implications for the implementation of enterprise-wide system. The success of implementing any system will depend on knowledgeable and appropriately skilled records specialists and IT staff working in close co-operation.

3.0 Monitoring or auditing for e-records management

The current e-Governance policy requires baseline information on e-readiness in order to establish the gap between the objectives and current situations. This gap analysis will be used to refine action plans. The strategy specifically mandates the Head of National Archives with these activities. (pg 45)

The National Archives of Namibia is responsible for actively monitoring the overall situation to maintain an ongoing awareness of the state of electronic records management practices and controls across government ministries, offices and agencies.

The monitoring process will be periodically conducted using either

c) Records Management Capacity Assessment System as is described in section 4.4.2.1 of this policy, and/or
d) E-records readiness assessment tool as is described in section 4.4.2.2 of this policy

Additionally, it is mandatory that before there is any implementation of an e-records management system or software package, an assessment is conducted to establish the organizational e-record readiness aptitude. This assessment is critical because

c) it will identify intrinsic organizational issues which are often not addresses merely through the introduction of a software application e.g. procedures for determining authenticity, compliance with legislation, human skills development
d) it will be useful to provide a snap shot of the situation as it existed before technological intervention and use that to assess whether the intervention was successful at the end of the intervention.

At the end of each assessment exercise, the National Archives will communicate the findings to the assessed government ministry, office or agency evaluated as well as the Minister responsible for Archives.

4.0 References

This policy should be read in conjunction with relevant pieces of legislation, regulations, national policies and international standards.

4.1 Relevant legislation and regulations

- Archives Act
- State Finance Act
- Public Service Act

4.2 National policies

- The E-Governance Policy for the Public Service of Namibia (2005)

4.3 International standards and best practise

4.3.1 Definitions and strategies

Definitions and strategies were based on

- Standards by International Standards Organization's and specifically ISO 15489: Part 1 and ISO 15489: Part 2
- Research work conducted by International Research on Permanent Preservation of Authentic Records in Electronic Systems - InterPARES (both in InterPARES 1 that lasted between 1999 and 2001, as well as InterPARES 2 which began in 2002 and ends in December 2006)

4.3.2 E-records assessment methodologies

The e-records assessment methodologies adopted in this policy have been developed by the International Records Management Trust. These are

4.3.2.1 Records Management Capacity Assessment System

This is a software application developed from funding from the World Bank as an objective means of assessing the strengths and weaknesses of records management systems. Its framework is based on maturity model principles and has objective capacity checks reliant on three international standards, from the International Standards Organization (ISO 15489), from the European Union (Model Requirements for Electronic Records-MOREQ), and another from Canada (Information Management Capacity Check-IMCC)

4.3.2.2. E-record readiness assessment tool

This is a simplified assessment tool developed from funding from the Commonwealth Secretariat been designed to be used in conjunction with existing e-government readiness tools to provide a simple, high-level assessment that will determine whether a government or public agency's records and information management infrastructure is capable of supporting e-government initiatives.

Part C

E-records Management Guidelines

Part C

E-records Management Guidelines

Table of contents

Table of figures

Executive summary

The ***E-records guidelines*** provide Namibian government ministries, offices and agencies with a guidelines for the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required. This document supplements the ***E-Records Policy for E-Governance*** as well as ***E-records Functional Requirements for Electronic Records Management Systems*** in meeting this objective.

Ministries, offices and agencies are required to make these guidelines in order to inform the processes of effectively and efficiently managing e-records. This document is divided into five separate sections. The first section provides an introduction to the document and it where it draws its legal and regulatory mandate, as well as other institutions from which it draws its principles. The second section provides generic e-records management requirements. The third section provides guidelines for managing e-records in specific environments, either when using ERMS applications or when such applications are not yet present. The fourth section is a strategy for managing or auditing process for the guidelines. The fifth section provides a glossary of terms which is foundational to maintaining vocabulary control over the whole document.

1.0 Introduction to E-records guidelines

The E-records guidelines are to provide direction for government ministries, offices and agencies that are required to manage records that are generated electronically. The guidelines draw their mandate from various legislative and regulatory instruments including The E-Governance Policy for the Public Service of Namibia (2005) and the Archives Act (1992).

Specifically, the E-Governance Policy for the Public Service of Namibia states

- "DPSITM in conjunction with the National Archives will ensure that every e-government project will incorporate a suitable records management component" (pg. 41)

- "DPSITM in conjunction with the National Archives will ensure that archival transfer of electronic records and their continued availability through hardware and software emulations. Software license agreements must take these concerns into account." (pg.41)
- In the implementation framework the first step of implementation requires a base line study which is to be done in consultation with Head of National Archives (pg. 46)

These guidelines therefore seek to present parameters within which government ministries, offices and agencies operate with respect to managing records in the e-government administration sphere.

Additionally, these E-records guidelines are informed by publications from the International Standards Organization, the US' Department of Defence standard, EU's standard and guidelines from national archival institutions in Australia, Canada, South Africa and the UK

1.1 Effective date, version, ownership and revisions of the framework

The E-records guidelines take effect….

The E-records guidelines will be subject to review two years from the date of its approval.

The E-records guidelines are mandated by the Archives Act and owned by the National Archives, which is responsible for its further development.

The E-records guidelines will be maintained in line with The E-Governance Policy for the Public Service of Namibia published by the Office of the Prime Minister in 2005.

1.2 Acknowledgement

The E-records guidelines are based on similar publications developed internationally and have been modified to suit the records management environment of the Namibian Government, in accordance with the requirements of the National Archives

Act as well as The E-Governance Policy for the Public Service of Namibia (2005) and the Draft E-records management policy for E-governance in Namibia (2006).

The National Archives would like to acknowledge the following publications in the development of the ERMS Specifications

- Australia's Functional specifications for Electronic Records Management Systems Software (2006)
- EU's Model Requirements for the Management of Electronic Records (2001)
- International Standards Organization's ISO 15489 standard on records management (2001)
- South Africa's Electronic Records Management Guidelines (2004)
- UK National Archives' Corporate Policy on Electronic Records (2000)
- UK National Archives' E-Government Policy Framework for Electronic Records Management (2001)
- UK National Archives' Management, Appraisal, and Preservation of Electronic Records Vol. 1 and Vol. 2 (1999)
- UK National Archives' Requirement for Electronic Records Management Systems (2002)
- US Department of Defence's Design Criteria Standard for Electronic Records Management Software Applications (2002)

2.0 Guidelines for managing E-records

The objective of these guidelines is the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required.

A record is considered authentic if it can be proven to "to be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported." In order to ensure authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorised and identified and that records

are protected against unauthorised addition, deletion, alteration, use and concealment.

A record is considered reliable if its "contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities." In order to ensure reliability of records, organizations should ensure records are created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

It is crucial to ensure records remain useable for as long as they are required. In the electronic environment various challenges jeopardize long term accessibility of digital information, including

a) the possibilities of altering or deleting information without leaving a trace or auditable trail
b) the fragility of media on which e-records are stored,
c) the rapid obsolescence of both hardware and software

When managing e-records it is critical to realise that an e-record consists of two main types of information:

- the record content and its internal structure, and
- the metadata which describes the record and all it constituent parts. This metadata can be used to describe and profile the electronic objects which make up the record itself, to give indexing information about the record, or to record a history of the context and use of the record.

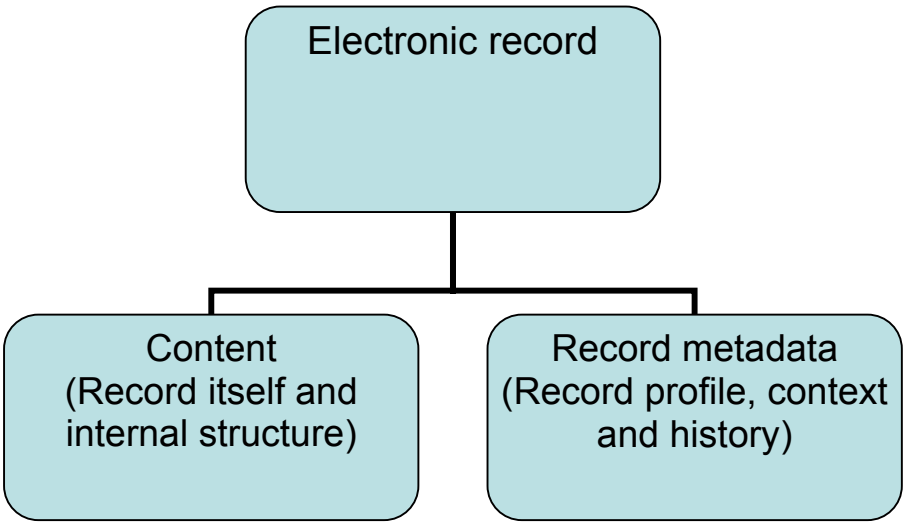


Figure 1: showing the main components of an e-record

In light of the challenges of ensuring authenticity and reliability of e-records as well as supporting their usability over time, this section outlines seven requirements that have to be addressed in order to meet the challenges. This are

a) e-records capture and registration
b) e-records classification
c) e-records storage and handling
d) e-records tracking
e) e-records disposition
f) e-records transfer
g) e-records preservation

Each of these requirements is explained below.

2.1 E-records capture and registration

Capture is the process of determining that a record should be made and kept. Registration is a way of formalizing the capture of the record into record systems. This includes both records created and received by an organization. It involves deciding which records are captured, which in turn implies decisions about who may have access to those records and generally how long they are to be retained.

For E-records, electronic systems can be designed to capture and register records through automatic processes, transparent to the user of the business system from

which records are captured and registered and without the intervention of a records management professional.

Systems that capture records also need to capture metadata associated with the record in a way that:
a) describes the record both for what it contains and the context of the business taking place;
b) enables that record to be a fixed representation of action; and
c) enables the record to be retrieved and rendered meaningful.
These aspects are often referred to as context, content and structure**.**

In cases where capture and registration is not automated elements of the registration process (specifically some of the metadata that are required for registration) can be automatically derived from the computing and business environment from which the record originates.

Whatever form it takes, as a general rule the register is unalterable. If, however, changes are required, there has to be an audit trail.

Registration specifies the following metadata as a minimum:
a) a unique identifier assigned from the system;
b) the date and time of registration;
c) a title or abbreviated description; and
d) the author (person or corporate body), sender or recipient.

More detailed registration links the record to descriptive information about the context, content and structure of the record and to other related records. Each record or group of records should contain information about the context and content of the record and other related records. Specific jurisdictions may have mandated metadata requirements for full and accurate records. Some of these metadata requirements may be met through the initial registration of a record and its relationships.

Depending on the nature of the business recorded, the organization's evidence requirements and technology deployed, the information attached to the record's unique identifier can include:
a) document name or title;
b) text description or abstract;

c) date of creation;
d) date and time of communication and receipt;
e) incoming, outgoing or internal;
f) author (with his/her affiliation);
g) sender (with his/her affiliation);
h) recipient (with his/her affiliation);
i) physical form;
j) classification according to the classification scheme;
k) links to related records documenting the same sequence of business activity or relating to the same person or case, if the record is part of a case file;
l) business system from which the record was captured;
m) application software and version under which the record was created or in which it was captured;
n) standard with which the records structure complies (for example, Standard Generalized Markup Language – SGML, Extensible Markup Language – XML);
o) details of embedded document links, including applications software and version under which linked record was created;
p) templates required to interpret document structure;
q) access;
r) retention period; and
s) other structural and contextual information useful for management purposes.

If a classification scheme is used, the file/record is best classified at the same time as it is registered. The type and complexity of classification depends on the type of company or organization.

2.2 E-records classification

Classification is the process of identifying the category or categories of business activity and the records they generate and of grouping them, if applicable, into files to facilitate description, control, links and determination of disposition and access status.

Using classification system that is related to business functions, the process consists of the following steps:
a) identify the transaction or business activity that the record documents;

b) locate the transaction or activity in the organization's classification system;
c) examine the higher-level classes to which the transaction or activity is linked to ensure the identification of the classification is appropriate;
d) check the activity classification against the organization's structure to ensure it is appropriate to the business unit to which the record belongs; and
e) allocate the identified classification to the record to the levels appropriate to the organization's requirements.

The number of levels of classification and entry point of the classification process (whether at transaction level or above) depends on the following factors:
a) the accountabilities of the organization;
b) the nature of the business;
c) the size of the organization;
d) the complexity of the structure of the organization;
e) the risk assessment of criticality for speed and accuracy in control and retrieval of records; and
f) the technology deployed.

2.3 E-records storage and handling

The decision to capture a record implies an intention to store it. Appropriate storage conditions ensure records are protected, accessible and managed in a cost-effective manner.

It is important to determine efficient and effective means of maintaining, handling and storing records before the records are created and then to reassess storage arrangements as the records' requirements change. It is also important that storage choices be integrated with the overall records management programme.

Organizations may do this by conducting a risk analysis to choose the physical storage and handling options that are appropriate and feasible for their records. The selection of storage options should take into account access and security requirements and limitations in addition to physical storage conditions. Records that are particularly critical for business continuity may require additional methods of protection and duplication to ensure accessibility in the event of a disaster.

Risk management also involves development of a disaster recovery plan that defines an organized and prioritized response to the disaster, planning for the continuance of regular business operations during the disaster and making appropriate plans for recovery after the disaster.

Factors that are important in selecting storage and handling options include:
a) *Volume and growth rate of records*. Projected growth rates may eliminate some storage facilities from consideration if their growth capacity is not sufficient. Similarly, digital storage media for electronic records should be assessed as to storage capacity. The choice of media should be matched to the presumed volume and growth rates of the records.

b) *Use of records.* The various uses of the record will determine the necessary levels of protection against loss or damage. For electronic records, use of reliable systems and media that have greater and more robust life spans will be indicated. In addition, the ease with which backups can be rotated and protected is a key consideration in selection of storage options for electronic records.

c) *Records security and sensitivity needs.* Some records require limitations on access to them for reasons of confidentiality, proprietary nature of the information or due to legal protections.

d) *Physical characteristics.* These factors will influence records storage: weight, floor space required, need for temperature and humidity controls, and the particular physical preservation requirements of the record media (for example, paper, digital storage, microform). Records in electronic form may need to be converted or migrated. Digital storage media may need to be refreshed. Records will need to be protected from fire, flood and other risks according to local circumstances.

e) *Records use as reflected in retrieval requirements.* Retrievability of records is a major consideration. Records that are accessed more frequently will require easier access to the storage facility. Electronic records may be stored in a variety of ways that make their retrieval easier or faster.

f) *Relative cost of record storage options.* Cost considerations may affect decisions about outsourcing of physical and/or electronic storage and the media selected for storage of electronic records.

g) *Access needs.* A cost-benefit analysis of on-site storage vs. off-site storage may indicate that multiple storage facilities, system, and/or equipment may be necessary to fully support the organization's needs.

The storage of records in electronic form necessitates the use of additional storage plans and strategies to prevent their loss:

a) Backup systems are a method of copying electronic records to prevent loss of records through system failures. Such systems ought to include a regular backup schedule, multiple copies on a variety of media, dispersed storage locations for the backup copies, and provision for both routine and urgent access to backup copies.

b) Maintenance processes may be needed to prevent physical damage to the media. Records may need to be copied to newer versions of the same media (or other new media) to prevent data erosion.

c) Hardware and software obsolescence may affect the readability of stored electronic records.

2.4 E-records tracking

Use of the record is a records management transaction that may need to be captured by the system to form part of the metadata. Use of the record may affect its access and disposition status.

Managing the use of records encompasses:
a) identifying the records system user permissions associated with individuals and their positions within the organization;
b) identifying the access and security status of records;
c) identifying the access rights for people external to the organization;
d) ensuring only individuals with the appropriate user classification or security rights have access to records with restricted status;
e) tracking the movement of the record to identify those who have or have had custody of it;
f) ensuring all use of the records is recorded to an appropriate level of detail; and

g) reviewing the access classifications of records to ensure they are current and still applicable.

The tracking of records usage within records systems is a security measure for organizations. It ensures that only those users with appropriate permissions are performing records tasks for which they have been authorized. The degree of control of access and recording of use depends on the nature of the business and the records they generate. For example, mandatory privacy protection measures in many jurisdictions require that the use of records holding personal information is recorded.

The patterns of records usage are useful for establishing the currency of the information contained in the record and provide a measure for determining when disposition action should be taken.

Systems for monitoring use and/or movement of records range from physical card-based movement-recording systems to bar-coding technology, to electronic records systems where viewing a record is automatically captured as a system transaction. Tracking systems have to meet the test of locating any record within an appropriate time period and ensuring all movements are traceable.

2.5 E-records disposition

Records with similar disposition dates and triggering actions should be readily identifiable from the records system, something that is quite easy if they are within a classification system. The use history of records due for disposition action needs to be reviewed to confirm or amend the disposition status. Other important activities are:

a) checking triggers for disposition action;
b) confirming as completed action in which the record may be involved; and
c) maintaining an auditable record of disposition action.

Strategies for retaining electronic records and associated metadata removed from systems have to be formulated and integrated into all systems design processes to ensure that the records and associated metadata will remain accessible and useable for the entire period of their retention.

Records in electronic form can be destroyed by reformatting or rewriting if it can be guaranteed that the reformatting cannot be reversed. Delete-instructions are not sufficient to ensure that all systems pointers to the data incorporated in the system software have also been destroyed. Backups containing generations of system data also need to be reformatted or rewritten before effective destruction of information in electronic form is complete. Physical destruction of storage media is an appropriate alternative, especially if deletion, reformatting or rewriting are either not applicable or are unsafe methods for destroying digital information (for instance, information stored on WORM [**W**rite **O**nce **R**ead **M**any] media).

2.6 E-records transfer

After appraisal, records with enduring value to the nation need to be transferred out of the custody or ownership of the organization or business unit that created them to the National Archives. Where this occurs, the records requiring transfer are identified, removed from existing records systems and physically transferred.

When E-records are transferred the following need to be considered
a) hardware and software compatibility;
b) metadata (control and contextual information);
c) data documentation (technical information on data processing and data structure);
d) licensing agreements; and
e) standards.

2.7 E-records preservation

Preservation strategies for records, especially electronic records, may be selected on basis of their ability to maintain the accessibility, integrity and authenticity of the record over time, as well for their cost effectiveness. Preservation strategies can include copying, conversion and migration of records.
a) Copying is the production of an identical copy within the same type of medium– for example, the production of backup copies of electronic records (which can also be made on a different kind of electronic medium).
b) Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content)

c) Migration involves a set of organized tasks designed to periodically transfer digital material from one hardware/software configuration to another, or from one generation of technology to another. The purpose of migration is to preserve the integrity of the records and to retain the ability for clients to retrieve, display and otherwise use them. Migration may occur when hardware and/or software becomes obsolete or may be used to move electronic records from one file format to another.

3.0 Managing E-records in particular environments

These guidelines, drawing from regulatory and legislative mandate, require that all e-records be effectively and efficiently in order to ensure that the seven requirements of e-records management are fulfilled (as highlighted in section 2 above).

The most effective tools for fulfilling these requirements are Electronic Records Management Systems (ERMS) which are system that preserve security, authenticity, context and integrity of e-records. Section 3.1 provides guidelines on how to use ERMS products to manage e-records.

However, these guidelines acknowledge that many ministries, offices and agencies do not have the resources or capacity to implement ERMS applications immediately. Section 3.2 is a set instructions in to provide transitional guidelines on how to manage e-records that already exist in local area or shared networks. This is definitely not ideal but as a better interim mechanism while working towards systems that will assist in the ultimate aim of the guidelines which is to creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required. Section 3.2 is as comprehensive a section as is possible serving to demonstrate the complexity of managing e-records when not using ERMS applications.

3.1 Managing E-records using ERMS systems

This section provides guidelines for organizations that use dedicated software (ERMS) applications to manage their e-records. As demonstrated in the figure below, ERMS applications facilitate various processes within an organization i.e. accession, structure, protection/security and access/retrieval.

The current e-Governance policy requires baseline information on e-readiness in order to establish the gap between the objectives and current situations. This gap analysis will be used to refine action plans. The e-Government policy specifically mandates the Head of National Archives with these activities.

The E-records policy specifically states that before any ministry, office or agency implements an ERMS applications, an assessment is conducted to establish the organizational e-record readiness aptitude. This assessment is critical because

e) it will identify intrinsic organizational issues which are often not addresses merely through the introduction of a software application e.g. procedures for determining authenticity, compliance with legislation, human skills development
f) it will be useful to provide a snap shot of the situation as it existed before technological intervention and use that to assess whether the intervention was successful at the end of the intervention.

After this assessment, a realistic road map can be charted on how best to introduce and implement ERMS applications. The National Archives requires that any such implementations follow a standard process as shown in figure 2 below

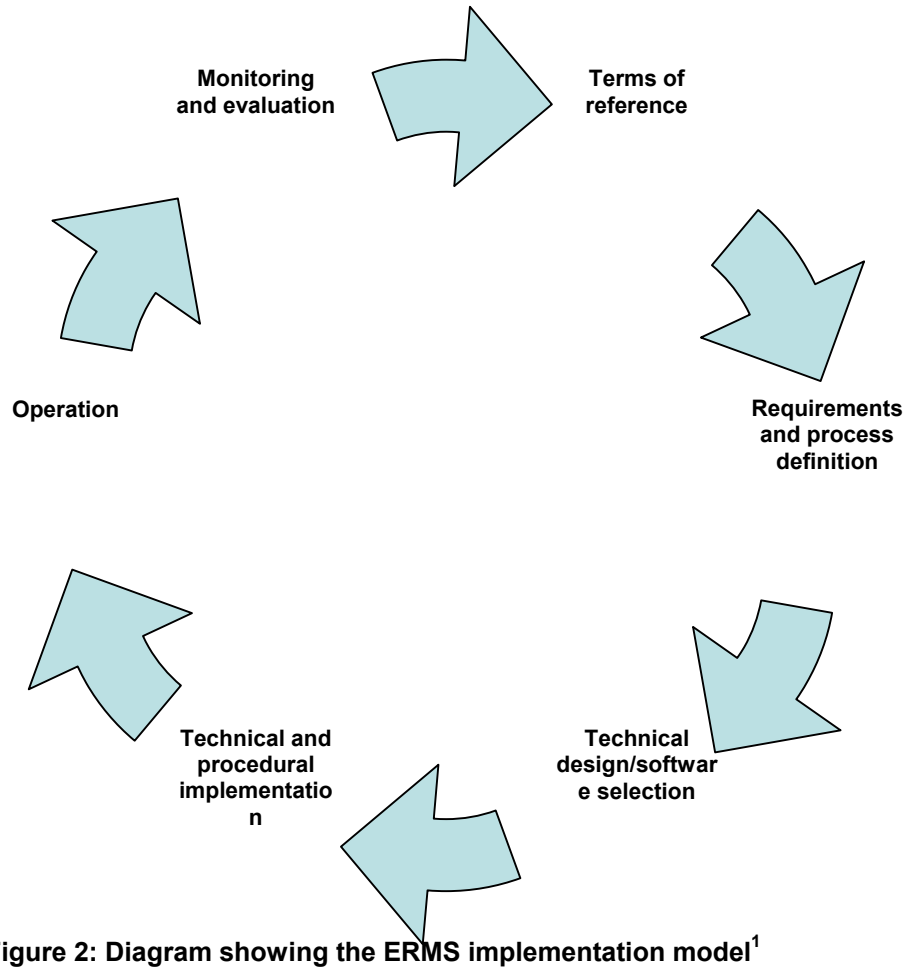


Figure 2: Diagram showing the ERMS implementation model[1]

Throughout this process, different phases are aimed at achieving different results

- terms of reference – outlining the project objectives for the task team
- requirements and process definition – outlining business functionalities and processes required to fulfil them.
- software selection – outlining selection process for identifying applications that meet the requirements from the proceeding process
- technical and procedural implementation – outlining the processes of planning system rollout, user awareness and education, and implications for work patterns and cultural change
- operation – outlining the operationalisation and institutionalisation of the system
- monitoring and evaluation – outlining the assessment of fulfilment of objectives and consideration for replication of project beyond its limited context.

[1] UK National Archives (2001) **E-Government Policy Framework for Electronic Records Management** Pg 53

The National Archives has produced a set of ***E-records Functional Requirements for Electronic Records Management Systems*** as a separate document that complements these guidelines and should be carefully considered during the process of implementing ERMS systems.

ERMS provide full records management functionality including records review, file plan structure, classification and maintenance and monitoring tools. Record-keeping and accountability are built into the business processes and electronic work environment, thereby ensuring that records are available, understandable and usable. When ERMS are used with workflow products, records management aspects are automated and users have a comprehensive suite of tools to organize, monitor and control the information management process.

3.1 ERMS facilities for users

Depending on their role, each user has access to a range of activities which are supported by various system facilities. In each activity a number of record types and functions are available to trigger the initiation of specific tasks. This approach means that the ERMS system has sufficient knowledge of the task being carried out, and the person undertaking it, to enable the record profile to be completed largely automatically.

3.2 ERMS facilities for records

Facilities for the life cycle management of information are included in the system based on business and operational rules and criteria agreed across the organization, to ensure a consistent approach to the identification, description, classification and organization of the records. Search engines and other mechanisms provide the benefit of access to all records for all users (limited where necessary for confidentiality or security classification), including version control of documents and records.

Automatic generation and completion of a profile for every document/record is stored within the corporate information structure. This will hold additional contextual information which groups or associates records into logical assemblies, and ensures

that they can be completely retrieved and managed in these assemblies. The profiles are updated to reflect the disposition of the record and may be retained after the corresponding record is no longer required and has been destroyed.

A standard filing system is used to assign a term from within the corporate file plan/thesaurus which matches the subject or function of the record. Individual electronic records are then tagged with others of the same category to form an assembly or 'file' within the corporate filing structure. Where appropriate, this scheme should be linked with the file system for paper records to ensure that all documents of both media are managed against the same retention and disposition procedures, and that all holdings of any given subject can be accounted for.

Automatic disposition, security downgrades and updating of essential records are conducted on pre-determined periods of time and pre-approved actions, with notification/confirmation to user, and an override capability.

ERMS systems should also have the capability of managing non-electronic records ie paper records. The management features include:

- folder tracking, labelling, destruction/transfer
- location records for paper files packed in boxes
- recording issue and return of files
- bar coding of file covers for inventory.

3.2 Managing E-records in a local area network

This section covers:

- naming conventions for documents and folders
- document metadata, templates and formats
- managing e-mail
- shared network drives
- building corporate filing structures

3.2.1 Naming conventions

Naming conventions are standard rules to be applied to e-records, and to electronic folders that contain these e-records, in order to enforce consistency in the form of name and in the words and phrases used. Essentially, naming conventions have two related functions:

- bringing related items together under a common label – such as for a folder or set of documents
- distinguishing similar items by naming in a consistent, logical and predictable way.

In the context of this document, the term *folder* refers to a Windows operating system folder unless otherwise specified.

At a basic level, use standard forms of names and avoid redundancy

- develop standard ways of ordering elements in more complex titles
- establish standard ways to identify document versions
- apply consistent conventions to both document and folder titles
- keep conventions as simple as possible and easy to use

3.2.1.1 Standard terms

Standard terms and forms of name should be used wherever it is sensible to do so. In particular, this can apply to:

- names of organizations and people
- names of projects and activities
- logical document types.

At this basic level, names should consist of sensible, short phrases. Proper names should always use *either* the full form of the name *or* the acronym.

Examples of rules for standard terms

- *Use **e-government** and not **electronic government***
- *Use **doh** and not: **dept. of home affairs; d-home-affairs; dept-h-a***
- *Do not use author's name in the title of a record*
- *Use standard terms for: **agenda; letter; minutes; project report***

3.2.1.2 Structured titles

The naming convention approach can be developed into a more detailed structuring system for the individual elements of document titles. The general principle is to identify the logical aspects of a document type, and to list these in the most effective order for access, rather than to describe record in full.

Examples of structured titles for records

- *consistently structure personal names in **surname, forename** order*
- *arrange document titles which reflect organizational structure in reverse hierarchical order (most specific first) as in **Training Unit : Personnel**, but do not repeat elements already in the folder title in which the document will be filed*
- *where a date is necessary in the document or folder title, order the elements so that they display chronologically, for example in a **YYYYMMDD** pattern; months spelled alphabetically do not file in chronological order*
- *for standard document types, combine elements of a title to give the most useful information first, bearing in mind the folder structure and titling; for example, for a letter: **topic – recipient – letter type**.*

Document titles should contain enough information to identify them if they become detached from the correct folder – a large number of documents entitled *2000-04 Minutes* is not helpful. Naming conventions should aim to strike the right balance between:

- *brevity* : keeping titles short; and *usability*: usefully describing the content
- *specificity* : using very precise terms; and *collocation*: grouping under broad headings that will assist effective management and retrieval.

3.2.1.3 Document version control

Consistent naming rules can link different versions of the same document, by including a version number as part of the title. This will also help to provide an audit trail for future tracking of document development; but does depend for success on disciplined use and careful tracking of versions. There is a danger of inconsistency if a document version is updated separately by different users without co-ordination, so that varying versions may exist each with different parts, but neither with all, of the full updated content. Well-developed and robust procedures are important for control of document versions in a multi-user environment.

The document name, and not the document extension, should be used to indicate the version number. Use of document extensions for version control will immensely complicate the mapping of document extensions to applications that can read them, creating a complex management overhead and the potential for conflict with later applications which may expect to use already allocated file extensions.

Example of version control information

Show document versions by structuring the title as:

<document name> - <version number>- <draft/fina l>.extension

as in:

staff management report - 0.4 - draft.doc

A common method for version control numbering is to use the ordinal number (1, 2, 3, etc) for major version changes and the decimal number for minor changes, as in:

ver: 0.5; ver. 1.0; ver. 2.7

A version 1.0 normally denotes a first document version given wider circulation – a document moving from personal to corporate workspace.

Footer information in documents is also useful for showing version information, and the location of equivalent paper documents.

3.2.1.4 Folder titles

Naming principles can be applied to folders. Two ways in which this can be done are:

- using standard terms for themes and activities which recur across the organization: for example, project organization structures that are common despite differences in project focus
- using consistent logical labels to describe business activities and functions which are common across an organization.

Standard folder titling can be applied at:

- the corporate level, applying organization-wide rules
- the workgroup level, where more specialized rules reflecting local conditions may be appropriate
- the personal level, to assist the individual with organizing and developing working documents.

Standard folder titling may be developed into a structure which aims to mirror appropriate parts of the established paper filing structure, where this is desirable.

3.2.1.5 Usability: length and readability

In the electronic environment, folder structures tend to contain more folders each containing fewer documents than occurs in the paper environment. This may lead to a greater depth in the folder structure itself. The length of folder (and document) titles can become an issue where a long pathway is built up through the folder hierarchy.

In most cases, an average of about 16 – 20 characters will be adequate, if care is taken to avoid repetition and redundancy. Long folder titles lead to very long pathways for an individual document, with the possible result that the relevant application is unable to open the document successfully.

Example of titling usability
An example of poor usability in a pathway name is:
Staff reports\ Registry \ Surveys of Government Departments \ 1999 – 3RMG 13.11 \ Staff Survey 1999 – Analysis and Results Process – 3RMG 13.11.2 \ Survey Forms Returned
better to use:
Staff reports \ Survey 1999 \ Survey Forms Returned
and reference the file numbers elsewhere, if they are needed.

A balance must be struck between emulating the paper system, and recognizing the different demands of usability and practical use which operate in the electronic environment.

3.2.2 Standard settings

Decisions on when to use standard settings, and which to use, should be based on a balance between:

- keeping it *simple*: too much complexity will confuse and alienate the end user, and lead to potential misinformation
- keeping it *useful*: only those standard settings which have a demonstrable value should be used
- keeping it *flexible*: where it is hard to anticipate all valid variations, it is usually better to adopt a minimal approach that can be adapted case-by-case.

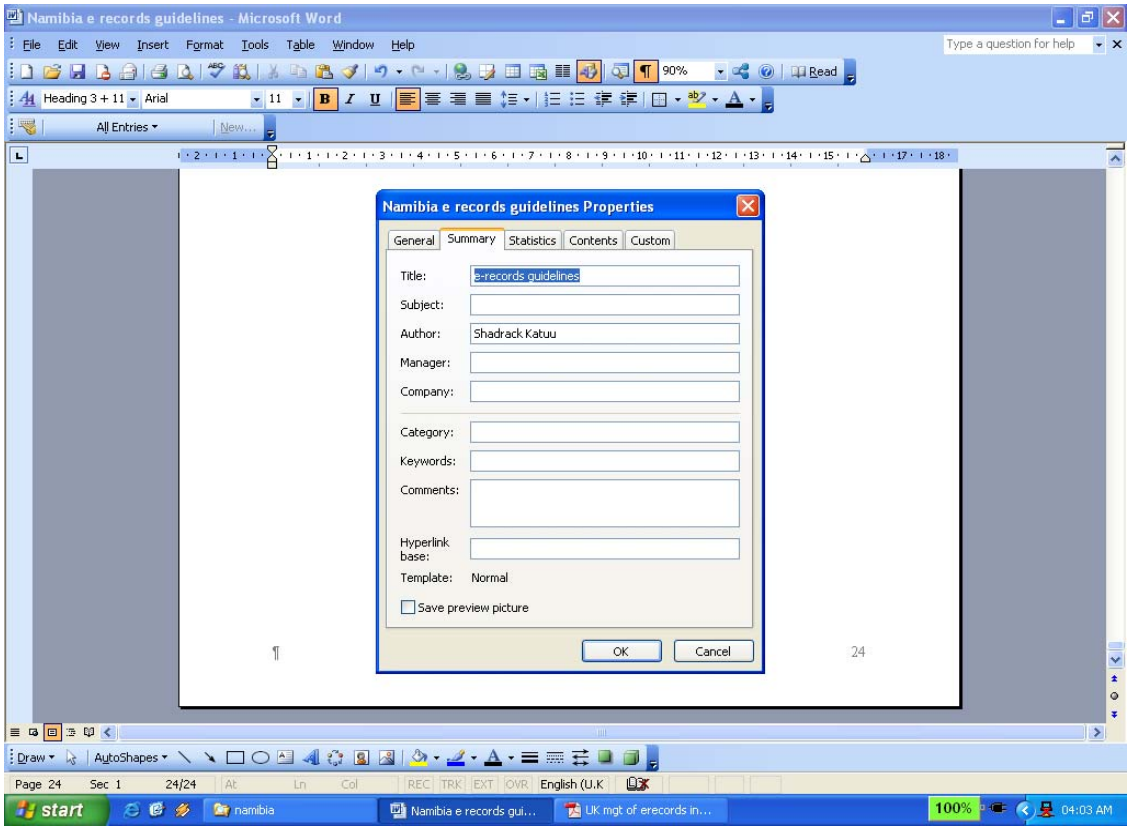
There are many potential metadata characteristics and template features that can be used in the MS Office application suite. Only a few of these can sensibly be put into practice in most government environments, unsupported by sophisticated ERMS systems. This section deals only with those which may be the most useful.

In brief, standard settings should

- use the Document Properties box for metadata, but sparingly
- design standard templates for very common document types
- standardize storage and distribution formats
- avoid using dynamic dates and linked documents

3.2.2.1 Document properties

Most standard Windows applications contain some form of *Properties* area, which contains a set of fields that can be filled in as metadata, either by hand or automatically by the software application.



Document properties could be filled in automatically or filled in by the individual at the time of creation or further editing.

Some advantages of using Properties are:

- standard key metadata terms accompany the document at all times
- support for document history tracking (although the level may be quite detailed)
- support for later migration to an ERMS which is capable of capturing metadata from document properties information.

Some disadvantages are:

- more work for the end user
- potentially misleading metadata where document production is shared: for example, where the *Author* field takes the last named editor, but the *Organization* field remains the same
- in practice, no-one may bother to use the metadata gathered in this way effectively.

3.2.2.2 Standard templates

Templates can be designed as basic standard forms for document types such as: letters, memos, requests, reports. They will:

- ensure a greater level of consistency in document (and record) production
- enable documents which should be kept as corporate records to be more readily identified
- support a closer integration of document production with line-of-business operations.

It is not feasible to attempt to design templates for every identified document type, or to construct variants for different folders. Only those document types which are in common use across the whole organization should be candidates for a standard template.

Example of standard template settings

While the design of more specialized templates will depend on the nature of the document type and the business activity which it supports, there are some basic features which can be used for all types of document. Some of these features can be incorporated into the basic template for all documents generated by an application:

- headers can show a title taken from the Title field of the Properties
- header or footer can show organizational unit or work team
- footers can show pathname, version number, and various forms of date.

3.2.2.3 Dynamic dates

In MS applications, it is possible to insert a generic date field which can be updated automatically by the application. These are convenient when used carefully, but will provide false information if used indiscriminately, particularly where different types of date are not clearly labeled and identified.

Example of dynamic dates

A *Date of Saving* field is updated each time the action takes place, and may be confused with other types of date. Use of these fields in a template should always be preceded by an appropriate phrase, as in:

Last edited on: {SAVEDATE}

so that its use for tracking edited versions is made clear, appearing in the document as:

Last edited on: 07/11/00

3.2.2.4 Storage and distribution formats

Where more than one version of a particular software application is in use, the physical format in which documents are saved should be defined. It is always preferable to limit the number of formats as far as possible, so that current access and future migration problems are reduced. The basic options are:

- Standardize on an **exchange format**, when multiple application versions are in use.

  For example, use the Microsoft version of RTF, by saving all corporate documents in a .rtf format (which the application can be set to do automatically). These documents will be accessible by different application versions (e.g. MS Word 97 and MS Word 95) and by other word processors; but some formatting information may be lost in certain circumstances.
- Standardize on a **distribution format,** where documents are finalized and will not be changed in content.

For example, a PDF rendition has the advantage of making documents effectively read-only, but requires the necessary Acrobat software to produce the rendition. This option is unlikely to be cost-effective for a large number of direct users, and will depend on some form of centralized or clustered storing function.

- Standardize on an **Internet format**, where an Intranet is the main distribution channel, supported by good document control facilities.
  For example, an HTML format makes the documents very widely accessible through a standard browser; but Office products are unsophisticated at producing html renditions, the html syntax may contain proprietary elements, and it is harder to control document versions.

3.2.3 Email and messaging

E-mail messages should always be treated as potential corporate records of the organization. More and more departmental business is conducted by e-mail, replacing the conventional memo and, increasingly, the formal letter. These guidelines therefore are necessary in order to

- develop policies clarifying which e- mails should be kept
- develop procedures for managing messages within the e-mail system
- extend procedures to include use of shared drive folders when feasible
- develop guidance for managing e-mail composition and dialogues
- help individuals to manage their own mailbox

Valuable material will be lost if e-mail is not managed in some way; but this can be difficult to do because:

- e-mail is not a simple record series, but a mechanism for transmission, so an e-mail system cannot be scheduled in its entirety
- retention depends on the content and context of the message, and is different for different messages sent or received by the same user, which must be treated separately essentially, e-mail is an individual channel, and is managed by the end user, or not at all.

3.2.3.1 Email policies

There is therefore need to develop clear policies to guide users on which types of e-mail message should be retained in the medium to longer term. These should cover:

- which messages a user sends that should be retained
- which messages a user receives that should be retained
- which dialogues should be recorded
- where drafts should be retained
- requirements for access to all these types of messages.

In addition, organisational policies should emphasise:

- an assumption that any e-mail message relating to departmental business may be kept as a record
- care in composing and expressing content
- expectations of privacy
- avoidance of inappropriate content.

There are three main approaches to managing e-mail records without the support of EDMS OR ERMS software:

- by a 'print-to-paper' policy – but this tends to work even less well than with word processed documents
- by managing within the e-mail system
- by saving messages to a shared drive.

3.2.3.2 Print to paper policy

Organizations' staff use office software and e-mail to create and exchange electronic documents. However, often there are no specific guidelines that successfully address the risks of 'print to paper' policy. For example, on the one hand, documents are often not actually printed and placed on a paper file, because this is seen as increasingly burdensome by the end user at the desktop. On the other hand, the electronic version of the document is not consistently managed either; documents may be stored unpredictably in a variety of locations and under varying names, and with no guarantee of lasting access or accuracy.

3.1.3.3 Managing within the e-mail system

The types of folders within an e-mail system follow the three-level workspace model described in the section summary for this section:

- **personal** folders are limited to individual access only, and cannot constitute a corporate record
- **shared** folders are a workteam space, where messages within an organisational unit can be stored and shared
- **public** folders are equivalent to corporate space.

The aim is to encourage users to store messages appropriately in one of these three areas. To be successful, the co-operation of the individual in regularly moving relevant messages from the personal mailbox to shared or public folders is required. Guidance should therefore always stress the benefits to the individual as well as the organisation.

Advantages of managing messages within the e-mail system are:

- all metadata relevant to the record is captured and preserved
- within a manageable environment
- with built-in filtering and deletion facilities available.

There are some **disadvantages**:

- e-mail messages are not integrated with other relevant documents or records in one structure
- so that parallel filing structures will develop, potentially including an individual's personal folder structure
- in addition, deletion does not ensure destruction, since the e-mail will be retained on back-ups.

Although probably not the ideal solution in the long term, this approach will provide valuable groundwork for the move to corporate level EDMS OR ERMS, by establishing good habits and practices in individual and team handling of e-mail as well as demonstrating the value of well-organised records.

3.2.3.4 Saving to a shared drive

The option of saving messages to a shared drive has the advantage of bringing together all documents and messages relevant to a theme or activity in the same

folder, and making this available for corporate access. It is, therefore, closer to the way in which e-mail messages would be managed in a full EDRMS. Unfortunately, the process of manually saving to a shared drive is rather cumbersome. This option would be best suited to a user population which has already developed good practices in handling e-mail.

User guidance will be needed on the appropriate *save* format and method to use:

- when to use the *Save as …* command and when to *Save attachments* separately. Where any significant information is contained in the body text of the e-mail itself, both the message and any attachments should be saved together in one operation.

Messages can be saved in various formats:

- a *.msg* format is convenient for use within the Outlook environment, but is proprietary and may be difficult to migrate over time
- a *.rtf* format is a (fairly) standard exchange format, which will embed any attachments within the message body, but will usually take a greater amount of disk space
- use of a..*html* format is not recommended here.

Message formats:

- transmission data, showing fields such as date of sending and receipt, recipients, subject title, should always be saved with the message text
- messages should not be saved to a shared corporate drive in any encrypted formats.

3.2.3.5 Conclusion

Managing email either within the email system or through shared drives has its limitations. However, unless there are EDMS or ERMS systems are in place, then these options ensure procedures are in place, albeit limited, in order to manage organizational records.

3.2.4 Use of shared networks

This section deals with the use of shared drives for managing corporate documents. In most local area network architectures, network drives appear to the user as various logical drives, typically arranged as:

- a corporate-wide shared drive, containing documents relevant to the whole organization
- a branch, or divisional shared drive, containing documents relevant to a single organizational unit
- a personal drive (for example, a P: or U: drive), containing documents relevant only to the individual.

Using shared network drives assists in

- encouraging 'publish and point' rather than multiple duplication
- developing logical and useful filing structures for shared drives
- developing common terminology and links to the paper filing systems
- establishing control over folder creation
- considering use of electronic zero files
- developing 'good housekeeping' for synchronising and deleting documents

In all cases, it will be necessary to identify clear and acceptable use policies for all three categories of drive. Good practices in managing electronic documents should be initiated in both the user workspace and the corporate space – good practice starts with the individual.

3.2.4.1 Publish and point

A *publish and point* policy is a method of controlling the duplication of a document which is being widely circulated. Instead of attaching the document to an e-mail message, which gives each recipient an individual copy, a read-only version of the document is placed on a shared drive – *published* – and a *pointer* or shortcut is emailed to alert intended recipients. Recipients can then retrieve the document from the shared drive as required.

This policy will:

- help to encourage a culture of sharing documents, within a forum and as an organizational resource, rather than as individually owned items

- encourage users to think more carefully about the most appropriate method for publishing information to recipients and to treat these consistently as formal corporate documents
- reduce keeping of multiple working copies in the folders of many individuals.

A *publish and point* policy will tend to decrease the requirements for individual document storage, but increase the need for network bandwidth by generating more traffic from common storage.

3.2.4.2 Filing structures

Where there is a significant number of electronic documents stored on a shared network drive, a basic general filing structure should be established. Where a division or branch (and any project–based structures) has specific filing structures, these should aim to conform to the principles of a general filing structure to prevent divergent practices and application.

Basic filing structure on shared drives should

- use simple but logical structures which meet the needs of both the organisation and the users
- *not* use individual names or position titles for directory or folder names use names which identify logical elements, such as business functions and activities or theme: sub-theme relationships
- have an established responsibility for creating and naming folders.

While the need for good filing structures in a shared network drive is primary, end users should also be encouraged to use consistent filing structures in their own group and personal workspaces. This will help with the co-ordination between working papers and formal finalised documents, and will ease retrieval and access across all workspaces for the individual.

3.2.4.3 Common terminology

Use of a common terminology is essential to integration; planning the use of shared drives should be done in conjunction with thinking about naming conventions.

- work towards consistent use of common terminology across all departments and units of the whole organisation
- develop formal liaison mechanisms between those responsible for records at the local level to establish and enforce these conventions
- where feasible, make terminology in the shared network folder structure consistent with terminology in the paper filing system
- make links with entries in the inventory of record collections.

3.2.4.4 Relating to paper filing system

The organisation of a shared network drive can usually be made to reflect the paper filing structure so that electronic documents are stored in a manner compatible with their paper counterparts. This may be achievable by building a hierarchical 'folder within folder' structure using Windows, to simulate the structure of a paper fileplan.
Some considerations are:

- there is little point in building a paper-based structure in electronic folder form which is not working well in the paper environment; and in most cases, a formal move towards implementation of EDRM will probably require some re-thinking of the approach and structure which is most appropriate for the new environment electronic structures tend to be broader and flatter – have less depth – than their paper counterparts; it is important to control the number of levels to retain usability; carefully consider the categories and terminology used at higher levels – in general, more than about 4/5 levels to a hierarchy can quickly become confusing and cumbersome
- alphabetical folder titles are generally more usable (in the electronic environment) than numerical fileplan / classification reference numbers and using both together will produce very long folder titles
- paper filing systems tend to use longer names than are comfortable in a Windows environment, resulting in file directory displays where the relevant, lowest part of the hierarchy is off-screen and not visible; in these circumstances it is also possible, when the full pathway of a document is constructed, to exceed the limit with which a software application can deal and thereby render the document apparently unusable.

3.2.4.5 Control over folder creation

Where the folder structure on shared drives is formalised in this way, clearly set out rights and responsibilities for folder creation and, where this is restricted, allocate these to specific roles. Consider:

- the extent to which a formal link to paper filing control systems, and the information which they contain (such as retention and disposal information) is desirable
- the role of local records officers in maintaining electronic filing structures
- the extent to which workgroups are able to create electronic folders themselves
- mechanisms for guiding and controlling the use of terminology.

3.2.4.6 Use of Zero files

A Zero file is a file which contains metadata about a series of folders, recording common information about that series, including its history, retention and disposal, opening and closing dates, and relationships to other record series. A zero file is sometimes used in paper filing systems, and can be adapted to the electronic environment. Potential uses include:

- as a link to the entry in the inventory of record collections for a set of electronic folders
- as an updateable link to parallel paper series structures, to maintain integrated control, whether the electronic or paper version is considered to be the formal record copy
- recording any access restrictions
- identifying users who are responsible owners
- retention beyond the life of the electronic folders, to document actions taken on the material (important for Freedom of Information)

3.2.4.7 Balancing drive usage

Gradual extending records management disciplines to the shared network drive environment will eventually involve decisions on technological support platforms and

network bandwidth; complementary technical policies and procedures will need to be developed. Consideration should be given to:

- the risks of lost documents in a shared network environment, where more reliability is expected
- the need to provide back-up and (perhaps) mirrored storage
- the implications of shared storage for network traffic and bandwidth requirements
- clear identification of material that should be entrusted to a shared drive and material that should be entrusted to the non-shared environment (and therefore printed to paper).

The move to full EDRM will require decisions on these kinds of issues in any case.

3.2.4.8 Disposing of documents

In all cases, 'good housekeeping' of both shared and personal drives is essential to maintaining long-term viability, removing material which should no longer be kept, whether classed as document or record. Since good management in this semistructured environment depends largely on the application of developed procedures and is not supported by corporate-wide document management software systems, some duplication and redundancy will probably be necessary to ensure good access for business purposes. Guidance should aim to reduce this to the right balance for the organisation – excess redundancy also works against usable access.

Guidance is needed for removing:

- unnecessary duplicates of final documents
- working copies which are no longer required
- documents which have no continuing value.

Users of local drives and personal areas of a network drive should also be encouraged to perform basic housekeeping. Regular use of the Windows Explorer *Find* facility for documents created and modified in a given period of time, will help ensure that locally held files are deleted or copied to the relevant shared drive as appropriate. Local drives should not be used for long-term storage of corporate level documents.

3.2.4.9 Laptops and synchronisation

Laptop and handheld computers are now widely used, at all levels of an organisation. These can cause particular difficulties when used in conjunction with a standard desktop PC, where documents are duplicated for working on in a different location. Lack of proper procedures may result in documents existing in different and potentially conflicting versions; it is particularly important to

- maintain a working structure on a laptop which is consistent with that visible from the main desktop machine
- develop a disciplined approach to updating document versions
- nominate a single storage location for documents in development, to hold the primary version and later updates.

File synchronisation facilities such as Windows Briefcase, which keep track of changes to particular files, can help to manage this duplication, as long as use of the facility is clearly understood. Windows is not designed as a robust medium for handling file conflicts, and will not substitute for sound agreed working procedures, particularly where several members of a workteam are working on the same documents.

A similar synchronisation facility is often used with MS Outlook and MS Exchange to synchronise folders in a local copy of an e-mail mailbox held on a laptop, with the same recipient's primary network mailbox. Many people use this facility to create and reply to e-mails using the local laptop copy, that are later uploaded to the main mailbox for despatch. The synchronisation facility harmonises changes in both main and local mailbox versions. Potential difficulties can arise where two separate copies – local and main copy – of a message have been separately edited producing conflicting versions. Careful following of a procedure to ensure that all local changes have been uploaded to the main mailbox before editing existing main mailbox versions will minimise potential replication conflicts.

3.2.4.10 Secure shared drive

A secure record drive is a shared network drive which has been configured in such a way as to prevent the amendment or unauthorised deletion of documents which have

been saved to the secure drive. With such a mechanism, organisations *may* feel able to treat the electronic documents stored in this way as the formal corporate record, even though a paper copy may also exist. Where this is the case, they should be stored within a separate structure from electronic documents which are not treated as corporate records; with clear definition of who has the right to add to, or delete from, the drive.

- Use a separate logical hard drive with *read-only* settings to prevent any changes being made to documents which have been saved to the drive.
- Users should be able to *read* and *create* documents, but not be given edit rights to existing documents.
- Ensure appropriate back-up and recovery procedures, and maintain the necessary level of access security at the operating system level.
- Assess the criteria and risks involved in this approach and clearly identify the types of document which it may be acceptable to manage in this way; a secure drive does not provide the same level of assurance as a fully managed EDRMS.

Departments and agencies should be aware that, although this method can provide reasonable sound storage of documents in the short term, there may be problems with migrating the material to a full EDRMS in due course. The Windows directory structure does not easily provide document and folder level metadata that will support a structured migration to an EDRM system; and although migration can be achieved it may be a relatively expensive process.

3.2.4.11 Sensitive information

The shared drive areas where corporate documents are made available should be capable of control by read/write permissions and by password control. Password control will enable control of user access to certain documents, either by:

- saving the document with password control if the application software supports this (as for example MS Word does) and copying the documents to the drive in this form
- placing password control on the entire logical drive. This may provide some basic access control, but the method has limitations:
- application software password control is not particularly sophisticated

- circulating a password to a number of different people is inherently insecure
- in a read-only drive, the document cannot be easily changed to amend or remove the password, because it is tightly bound with the contents. In practice, documents containing any sensitive or classified information should probably not normally be storage on a secure shared drive.

4.0 Monitoring/Auditing for E-records management

The current e-Governance policy requires baseline information on e-readiness in order to establish the gap between the objectives and current situations. This gap analysis will be used to refine action plans. The strategy specifically mandates the Head of National Archives with these activities. (pg.45)

The National Archives of Namibia is responsible for actively monitoring the overall situation to maintain an ongoing awareness of the state of electronic records management practices and controls across government ministries, offices and agencies.

The National Archives will periodically communicate their findings to both the institution evaluated as well as the Minister responsible for Archives.
The monitoring process will be periodically conducted using either

e) Records Management Capacity Assessment System as is described in section 4.4.2.1 of the ***E-Records Policy for E-Governance***, and/or
f) E-records readiness assessment tool as is described in section 4.4.2.2 of ***E-Records Policy for E-Governance***

Additionally, it is mandatory that before there is any implementation of an e-records management system or software package, an assessment is conducted to establish the organizational e-record readiness aptitude. This assessment is critical because

g) it will identify intrinsic organizational issues which are often not addresses merely through the introduction of a software application e.g. procedures for determining authenticity, compliance with legislation, human skills development
h) it will be useful to provide a snap shot of the situation as it existed before technological intervention and use that to assess whether the intervention was successful at the end of the intervention.

There are three reasons for monitoring and auditing records systems:
a) to ensure compliance with the organization's established standards;
b) to ensure that records will be accepted as evidence in a court of law should this be required; and
c) to improve an organization's performance.

Monitoring helps to ensure continued legal accountability of the records system. The monitoring processes are documented to provide evidence of compliance with policies, procedures and standards the organization has adopted.

Systematic monitoring programs, developed and designed in accordance with existing rules and regulations, can best meet the requirements for such corporate accountability.

It is important that for every ministry, office or agency, an appropriately qualified person oversee compliance, reporting independently to senior management.

Compliance is most appropriately conducted by whoever designed or implemented the monitoring programs, or by the person responsible for managing the records.

Monitoring should take place regularly at intervals agreed and set down in the organization's records management policy.

5.0 Glossary

Access: The right, opportunity, or means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any of the resources of the computer system.

Application: Computer software that allows the user to process data or perform calculations necessary to achieve a desired result, as opposed to the operating system designed to control the computer's hardware and run all other programs.

Archives: records of enduring value selected for permanent preservation

Attachment: An item added or appended to a document.

Audit trail: Information about transactions or other activities which have affected or changed entities, held in sufficient detail to allow the reconstruction of a previous activity.

Authentic record: record one that can be proven: To be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported. Authenticity is conferred on a record by its mode, form, and/or state of transmission and/or manner of preservation and custody

Backup: A duplicate copy of all or portions of software or data files on a system made for safety purposes.

Capture: Registration, classification, addition of metadata and storage of a record in a system that manages records.

Conversion: Changing the medium and/or physical form of the record, leaving intact the intellectual form, for purposes of security, disaster prevention, conservation, overcoming technology obsolescence, or compacting the information while preserving the record's reliability and authenticity. This includes migration, refreshment, reproduction, etc.

Copying: making reproduction of a record in any state of transmission for business purposes.

Data: electronic representations of information in any form suitable for transmission, interpretation or processing

Database: Any grouping of data for a particular purpose or for the use of a particular set of end users, usually organized via fields, which enables manipulation of the data such as sorting, grouping and extraction.

Destruction: To eliminate records identified for destruction, and provide documentation about the records destroyed.

Disposition: The actions taken with regard to non−current records following their appraisal and the expiration of their retention periods as provided for by legislation, regulation or administrative procedure.

Document: information created, received, and maintained which can be treated as a unit regardless of medium or characteristics.

Draft: A preliminary form of a document sometimes retained as evidence.

Electronic document management system: system that produces, processes, or stores documents electronically

Electronic document: document generated in electronic form

Electronic records management system: system that preserves security, authenticity, context and integrity of electronic records

Electronic record: record generated and stored in electronic form

Electronic signature: A digital mark, code, or other symbol that identifies an individual and indicates responsibility for or consent to the content of the material to which it is affixed.

Encryption: The conversion of data into a secret code for transmission over a network.

Export: a disposal process, whereby copies of a digital record (or group of records) are passed with their metadata from one system to another system. The record remains on the ERMS after export unlike during transfer.

File format: a standard or specification for the encoding of information in a file

File: An organized unit of documents accumulated during current use and kept together because they deal with the same subject, activity or transaction.

Filing: The systematic organization of records in groups or categories according to methods, procedures, or conventions represented in a filing system

Hybrid file: a set of related electronic records and/or physical records stored partly in an electronic file within the ERMS and partly in a related paper file outside the ERMS.

Information system: a system for generating, sending, receiving, storing or otherwise processing data messages and capable of being used in conjunction with external files.

Interoperability: The ability of one application, system, or metadata schema to communicate, work, or interface with another; the ability to provide services and accept services from other systems, enabling information that originates in one context to be used in another in ways that are as highly automated as possible.

Metadata: Data associated with either an information system or an information object for purposes of description, administration, legal requirements, technical functionality, use and usage, and preservation through time and within and across domains in which the data is created.

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 to ensure continued access to the information as the system or media becomes obsolete or degrades over time.

National Archives: Institution mandated by the Archives Act (1992) and responsible for the regulation, execution and administration of matters related to the custody and care of all public records.

Preservation: The processes and operations involved in the storage, stabilization and protection of documents against damage and deterioration and in the treatment of damaged or deteriorated documents and may also include the transfer of information to another medium.

Record creation: The first phase of a record's lifecycle in which a record is made or received and then set aside for action or reference.

Record: information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business.

Records lifecycle: the phases through which records pass, including creation, use and maintenance, and disposition (destruction or permanent preservation).

Records management: field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of record, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Refreshment: (of digital objects) conversion storage of digital components from one medium to another or otherwise ensure that the storage medium remains sound.

Reliable record: record whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Retention schedule: a set of instructions allocated to a series or file to determine the length of time for which its records should be retained by the organization for business purposes and the eventual fate of the records on completion of this period of time.

Retrieval system: A set of rules governing searching and finding records in a system, and the tools and mechanisms used to implement these rules.

Standard; Rules established to prescribe qualities or practices in order to achieve common goals of uniformity within or across a sector or system.

Systems administrator: a person responsible for the day to day operations of the institutional records management system.

Technological obsolescence: The process of becoming inaccessible or unusable through technological change.

Transfer: the disposal process consisting of confirmed export of digital records and folders followed by their destruction within the exporting ERMS

User: Any person utilizing an information system

Version control: The ability to track and manage the history of a particular piece of content including: the ability to rollback to a previous version of a document, the ability to track major and minor revisions of a document, and the ability to purge earlier versions of a document

Part D

Functional Requirements for Electronic Records Management Systems

Part D

Functional Requirements for Electronic Records Management Systems

Table of contents

Document first created: **July 2006**
Document last modified: **19 October 2007**

Executive summary

The ***Functional Requirements for Electronic Records Management Systems*** provides Namibian government ministries, offices and agencies with a set of generic requirements for ensuring adequate records management functionality within electronic records management systems (ERMS) software. This document supplements the ***E-Records Policy for E-Governance*** as well as ***E-records guidelines*** in meeting the objective of the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities in ministries, offices and agencies for as long as they are required.

Ministries, offices and agencies are required to make use of the ERMS Specifications when designing or purchasing new, or upgrading existing, ERMS software. The Specifications may also be used when auditing, assessing or reviewing an agency's existing ERMS software.

These generic requirements are not intended to be a complete specification, but rather provide a template of key functional requirements that ministries, offices and agencies may incorporate into their tender documentation when preparing to select and purchase new ERMS software. Agencies using the Specifications must assess and amend the functional requirements, and select requirements that best suit their own business and technical requirements and constraints.

1.0 Introduction to functional requirements

1.1 Background and purpose

In a report published in 2004, the review process revealed that while there is "extensive use of PCs to store key information by officials and private secretaries", no policies or standards exist to manage records produced by the electronic systems. Among the key recommendations from this assessment was the need to "ensure that

the electronic information systems selected for implementation include electronic record management standards".[2]

These E-records functional requirements for ERMS systems are a specific response to the need to provide direction when designing or purchasing new, or upgrading existing, ERMS software. They contain generic requirements for electronic records management systems software and sets out the records management functionality that is essential for a system to support business and accountability requirements and meet public expectations. They also present desirable requirements that may further enhance the records management functionality of an agency's ERMS software.

The functional requirements set out in the E-records functional requirements for ERMS systems were developed for Namibian ministries, offices and agencies and will help them:

- • build a business case to support the review, design or purchase of ERMS software;
- • review the performance of existing ERMS software;
- • develop requirements for adequate recordkeeping functionality for inclusion in a design specification when building or purchasing ERMS software, or when upgrading existing systems software;
- • evaluate the recordkeeping capability of proposed customised or commercial off-the-shelf software intended to manage digital records; or
- • undertake a recordkeeping audit or compliance check of agency ERMS software to verify that such systems have adequate recordkeeping functionality.

1.2 Effective date, version, ownership and revisions of the E-records functional requirements for ERMS systems

These E-records functional requirements for ERMS systems take effect….

[2] [Namibia] Ministry of Basic Education, Sport and Culture (2004) **Library and Archives Consultancy Report**, Namibia Library and Information Service pg. 75-76

Document first created: **July 2006**
Document last modified: **19 October 2007**

These E-records functional requirements for ERMS systems will be reviewed annually from the date of its approval.

These E-records functional requirements for ERMS systems are mandated by the Archives Act and owned by the National Archives, which is responsible for its further development.

These E-records functional requirements for ERMS systems will be maintained in line with The E-Governance Policy for the Public Service of Namibia published by the Office of the Prime Minister in 2005.

1.3 Acknowledgement

The E-records functional requirements for ERMS Systems are based on similar publications developed internationally. The Specifications has been modified to suit the records management environment of the Namibian Government, in accordance with the requirements of the National Archives Act as well as The E-Governance Policy for the Public Service of Namibia (2005) and the Draft E-records management policy for E-governance in Namibia (2006).

The National Archives would like to acknowledge the following publications in the development of the ERMS Specifications

- AIIM and ARMA's Technical Report: Framework for Integration of Electronic Document Management Systems and Electronic Records Management Systems (2004)
- Australia's Functional specifications for Electronic Records Management Systems Software (2006)
- EU's Model Requirements for the Management of Electronic Records (2001)
- International Standards Organization's ISO 15489 standard on records management (2001)
- International Standards Organization's draft guidelines for drafting an RFP for electronic document systems
- South Africa's Electronic Records Management Guidelines (2004)

- UK National Archives' Requirement for Electronic Records Management Systems (2002)
- US Department of Defence's Design Criteria Standard for Electronic Records Management Software Applications (2002)

1.4 Purpose and scope of this specification

This specification describes functional requirements for the Management of Electronic Record. It focuses on functional requirements for the management of electronic records by an Electronic Records Management System (ERMS).

This specification is written to be equally applicable to public and private sector organisations which wish to introduce ERMS, or which wish to assess the ERMS capability they currently have in place.

While the specification focuses on functional requirements, it recognises that non-functional attributes are central to the success of an ERMS, as with any information system. However, these non-functional attributes vary enormously between environments. Accordingly, they are identified but described only in outline.

Other closely-related requirements, such as document management and the electronic management of physical records (e.g. paper files and microfilm) are also addressed, but in less detail. For example, the specification includes guidelines on the requirements for managing physical records; but it does not include all the detailed functionality associated with tracking physical locations, bar coding, etc.

1.5 Typical ERMS Functions

Typical ERMS functions include:

• Marking an electronic document as a read-only electronic record

• Protecting the record against modification or tampering

• Filing a record against an organizational file plan or taxonomy for categorization

• Marking records as vital records
• Assigning disposal (archival or destruction rules) to records
• Freezing and unfreezing disposal rules
• Applying access and security controls (security rules for electronic records may differ from the source electronic document in the EDMS)
• Executing disposal processing (usually an administrative function)
• Maintaining organizational/historical metadata that maintains the business context of the record in the case of organizational change
• History/audit trail

1.6.Standards for ERMS

Because records management as a business practice/profession is relatively mature, a number of ERMS standards exist.

1.6.1 International Standard: Information and documentation—Records Management (ISO 15489)

ISO 15489 was published in 2001 to provide guidance on determining the responsibilities of organizations for records and records policies, procedures, systems, and processes. It applies to the management of records, in all formats or media, created or received by any public or private organization in the conduct of its activities, or any individual with a duty to create and maintain records. ISO 15489 provides guidance on the design and implementation of a record system, but does not include the management of archival records within archival institutions.

1.6.2 U.S. Department of Defense Standard: Design Criteria Standard for Electronic

Records Management Applications (DoD 5015.2-STD)

DoD 5015.2 was first published in 1997 to set forth mandatory baseline functional requirements for records management applications (RMA) software for US Department of Defense components in the implementation of their records management program, defines required system interfaces and search criteria to be

supported by RMAs and non-mandatory features, and describes the minimum records management requirements that must be met, based on US National Archives and Records Administration (NARA) regulations. DoD 5015.2 also identifies non-mandatory features that are deemed desirable for RMA software. Version 2 of the standard was published in June 2002 to incorporate requirements for security classification markings, access controls, declassification and downgrading instructions, and other issues.

1.6.3 United Kingdom Public Records Office (UK PRO)

The UK PRO ERMS *[sic]* standard was originally published in 1999 to form a baseline of generic functional requirements necessary for a credible electronic records management system. The 2002 revision was published as a three-part document. Part 1—*Functional Requirements* identifies the functional requirements for ERMS *sic]* in two sections. Section A defines the core requirements for an ERMS in some detail. Section B defines additional features that are closely related to an ERMS and which some products may offer. Part 2—*Metadata Standard* defines the core metadata elements referenced in Part 1. Part 3—*Reference Document* provides a glossary of terms, description of entities and their relationships, user roles, access control model, and example disposal schedules.

1.6.4 Model Requirements for the Management of Electronic Records (MoReq)

The Interchange of Data Between Administrators (IDA) program of the European Commission sponsored the development of *Model Requirements for the Management of Electronic Records* or MoReq in 2000-2001. MoReq describes functional requirements for the management of electronic records by an ERMS. The specification was written to be equally applicable to public and private sector organizations that wish to introduce an ERMS or to assess the ERMS capability they currently have in place. Other closely related requirements, such as the electronic management of physical records (e.g. paper files and microfilm), are also addressed.

2.0 Functional requirement statements

2.1 Core functional requirements

2.1.1 Records management

2.1.1.1 Control - The ERMS must allow folders and records to be organised, so that they can be managed, found and understood.

2.1.1.2 Capture - The ERMS must formally capture records regardless of their technical characteristics.

2.1.1.3 Access and security - The ERMS must have the ability to assign rights and restrictions on the use or management of particular records in order to facilitate security.

2.1.1.4 Disposal - The ERMS must be able to control the retention and disposal of records held by the system, in accordance with disposal authorization.

2.1.1.5 Searching and retrieval - The ERMS must be able to retrieve digital records and folders by a variety of search methods, and render the results on-screen.

2.1.1.6 Metadata - The ERMS must support the use of metadata to describe digital records and to enable automated records management processes.

2.1.1.7 Compliance - The ERMS must meet relevant local, national and international requirements for recordkeeping and records management.

2.1.2 Systems management and design

2.1.2.1 Usability - The ERMS must be logical to operate and simple to learn, taking into account the differing needs and abilities of potential users.

2.1.2.2 Reporting - The ERMS must be able to produce reports on system activities and the status of objects within its control, for management, statistical and general purposes.

2.1.2.3 Systems administration - The ERMS must provide facilities for the ongoing maintenance and support of the system, and the data it manages. Some of these functions may be provided by the operating system, database management system or other applications linked to the ERMS.

2.1.2.4 Systems design - The ERMS design must support response times and levels of system availability that meet current and projected user requirements.

2.2 Additional functional requirements

2.2.1 Online security - The ERMS must be able to manage digital records which have been subjected to online security procedures, and ensure that such processes do not impair the ability of the ERMS to meet the core requirements of this specification. These processes include encryption, electronic signatures, digital watermarks and other authentication processes.

2.2.2 Document management - The ERMS must be able to provide, or integrate with, document management facilities to ensure records management functions are seamlessly supported.

2.2.3 Workflow - The ERMS may provide or be integrated with a workflow facility to support business and records management tasks in a controlled manner. The ERMS must ensure that such processes do not impair its ability to meet the core requirements of this specification.

2.2.4 Hybrid system management - The ERMS must support the management of markers, physical folders and hybrid folders in a manner consistent and fully integrated with the management of digital records and folders.

3.0 Access matrix[3]

This section contains a simple generic model of user roles. In order to make it generic, it consists of a matrix which recognizes just two user roles. The roles of user and Administrator are defined in terms of access to ERMS functionality.

The role Administrator represents a simplification. Especially in large organizations, the tasks attributed in this specification to Administrators may be divided between several roles, with titles such as Administrator, Records Manager, Records Officer, Archivist and Data Manager or IT manager etc.

Note that the Administrator role is in many cases only implementing, from a system perspective, decisions taken by more senior management based on laws and regulations, such as information laws, data security laws, archival laws and industry regulations. This matrix is not intended to imply that Administrators must take management decisions, though in some environments that may be the case

In broad terms, users have access to facilities which an office worker or researcher needs when using records. This includes adding documents, searching for and retrieving records; their interest is in the contents of records. Administrators take actions related to the management of records themselves; their interest is in records as entities rather than their content. They also manage the ERMS hardware, software and storage, ensuring backups are taken and the performance of the ERMS.

In the following table,

- • YES indicates the ERMS must allow this combination of roles and functions;

[3] Cornwell Management Consultants [for the European Commission Interchange of Documentation between Administrations Programme] (2001), Model Requirements for the Management of Electronic Records, Pg 115

Document first created: **July 2006**
Document last modified: **19 October 2007**

- • NO indicates the ERMS must prevent this combination of roles and functions;
- • OPTIONAL indicates that the ERMS may allow or prevent this combination of roles and functions, and that the using organization must determine whether its procedures allow or prevent this combination.

Note that this matrix is divided into sections. These sections group, for convenience, the functions normally associated with files, records, records management and administration.

This matrix is best viewed as a starting point, and as the formal basis for assigning rights. Users of this specification will need to consider additional requirements which are specific to their environment. For example, some environments may have "records reviewer" roles which are separate from the Administrator roles; in this case there will be a need to specify access controls for this role.

	User	**Systems administrator**
Create new files	OPTIONAL	YES
Maintain filing system and files	NO	YES
Delete files	NO	YES
Capture records	YES	YES
Search for and read records[4]	YES	YES
Change content of records	NO	NO[5]
Change record metadata	NO	YES
Delete records	NO	YES
Retention schedule & disposal transactions	NO	YES
Export and import files and records	NO	YES

[4] Subject to access rights of individual documents
[5] Except for redaction (the process of legally hiding sensitive information in a record)

	User	Systems administrator
View audit trails	OPTIONAL	YES
Change audit trail data	NO	NO
Move audit trail data to off-line storage media	NO	YES
Perform all transactions related to users and their access privileges	NO	YES
Maintain database and storage	NO	YES
Maintain other system parameters	NO	YES
Define and view other system reports	NO	YES

4.0 Approved systems and suppliers

The list below of approved systems identified as capable of meeting both the ERMS functional requirements in these document and have been tested internationally.

Product	US DOD approval[6]	UK approval[7]	SA approval[8]
Documentum Records Manager v5.2.5 (EMC Corporation)	Expiry 21st Jan 2007		Expiry 1st May 2006
Hummingbird Enterprise 2005 DM/RM 6.0 (Hummingbird)	Expiry 8th April 2007	Expiry 30th April 2008	Expiry 1st May 2006
Livelink Records Management (Open Text) http://www.opentext.com	Expiry 11th Nov 2006	Expiry 31st Oct 2006	Expiry 1st May 2006
SharePoint Portal Server 2003 integrated with Meridio, Inc.'s Meridio v4.2 EDRM Accelerator (Microsoft) http://www.microsoft.com	Expiry 22nd July 2006	Expiry 30th June 2006	
SAP Records Management for Public		Expiry 30th Nov	

[6] http://jitc.fhu.disa.mil/recmgt/register.html
[7] http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/approved.htm
[8] http://www.sita.co.za/TendersAdministration/ViewAwarded.asp?tenderid=56

Product	US DOD approval[6]	UK approval[7]	SA approval[8]
Sector http://www.sap.com/uk/publicsector		2007	
TRIM Context v6.0 (Towersoft)	Expiry 18th June 2007	Expiry 30th Sept 2007	Expiry 1st May 2006

Considering that there are different suppliers for these products within the region, the National Archives has adapted ISO standards in order to be able to identify, assess and approve suppliers best placed to provide systems in the approved systems. The assessment criterion is shown in the figure below.

Qualifications and Experience

1. Provide company history
2. Provide company financial data for three years
3. Provide most recent annual report
4. Current number of people employed
5. Current number of locations including sales, service, training locations
6. Nearest service location to proposed installation
7. Describe service locations including number of personnel, management organization, escalation policy
8. Provide specific industry background
9. Current number of systems in specific industry
10. Current number of systems installed including those installed within the last two years as well as pilot systems
11. Provide references for three installed systems similar to the system proposed including account name and address, project manager name, project manager's telephone number, and description of system
12. Site visit (provide on request the availability of one of the sites described in item 11 as a reference account)

Pre-Award Demonstration

1. Vendors will be required to provide a pre-award demonstration plan with their proposals to include
   - description of demonstration facilities
   - hardware and software demonstrated
   - hardware and software configuration
   - performance measurements
   - communications capabilities

   2. Vendors will be required to demonstrate functional requirements of equipment proposed.

   3. Vendors will be required to process actual documents. These documents will be supplied on request.

   4. Functional demonstrations

Disaster Recovery

1. Discuss the types of disasters that could affect the system such as
   - fire and smoke damage
   - water damage
   - earthquake damage
   - potential fatal system problems
   - internal personnel-induced disasters (sabotage)
2. Provide detailed preventive plans for the scenarios outlined in the preceding item 1
3. Provide detailed recovery plans for the scenarios outlined in item 1 and include
   - on-site recovery
   - off-site recovery
   - dedicated recovery sites
   - shared-use recovery sites
   - vendor-supported recovery sites
   - third-party-supported recovery site
4. Provide details for reestablishing existing sites
5. Provide details for establishing physical security
   - preventive
   - post-disaster

Following the above vendor selection criteria drawn from ISO standards, the National Archives will identify an approved list of system suppliers within the region in order to provide direction for ministries, offices and agencies.

The use of an approved list of both systems and their suppliers is intended to ensure reduce the risk of having questionable businesses without a proven track-record trying to lure ministries, offices and agencies into purchasing their systems.

Government ministries, offices and agencies are encouraged to develop pilot projects and use a modular or incremental approach to implementation. Electronic records management is a relatively new application area for the government, and an incremental approach will support an ability to learn from experience, and to avoid pitfalls often inherent in large single-rollout projects.

The current e-Governance policy requires baseline information on e-readiness in order to establish the gap between the objectives and current situations. This gap analysis will be used to refine action plans. The strategy specifically mandates the Head of National Archives with these activities. Before implement ERMS application, each ministry, office or agency should have an e-readiness assessment conducted by the National Archives in order to determine the possible risks and opportunities in the process.

5.0 Glossary

Access: The right, opportunity, or means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any of the resources of the computer system.

Application: Computer software that allows the user to process data or perform calculations necessary to achieve a desired result, as opposed to the operating system designed to control the computer's hardware and run all other programs.

Archives: records of enduring value selected for permanent preservation

Attachment: An item added or appended to a document.

Audit trail: Information about transactions or other activities which have affected or changed entities, held in sufficient detail to allow the reconstruction of a previous activity.

Authentic record: record one that can be proven: To be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported. Authenticity is conferred on a record by its mode, form, and/or state of transmission and/or manner of preservation and custody

Backup: A duplicate copy of all or portions of software or data files on a system made for safety purposes.

Capture: Registration, classification, addition of metadata and storage of a record in a system that manages records.

Conversion: Changing the medium and/or physical form of the record, leaving intact the intellectual form, for purposes of security, disaster prevention, conservation, overcoming technology obsolescence, or compacting the information while preserving the record's reliability and authenticity. This includes migration, refreshment, reproduction, etc.

Copying: making reproduction of a record in any state of transmission for business purposes.

Data: electronic representations of information in any form suitable for transmission, interpretation or processing

Database: Any grouping of data for a particular purpose or for the use of a particular set of end users, usually organized via fields, which enables manipulation of the data such as sorting, grouping and extraction.

Destruction: To eliminate records identified for destruction, and provide documentation about the records destroyed.

Disposition: The actions taken with regard to non−current records following their appraisal and the expiration of their retention periods as provided for by legislation, regulation or administrative procedure.

Document: information created, received, and maintained which can be treated as a unit regardless of medium or characteristics.

Draft: A preliminary form of a document sometimes retained as evidence.

Electronic document management system: system that produces, processes, or stores documents electronically

Electronic document: document generated in electronic form

Electronic records management system: system that preserves security, authenticity, context and integrity of electronic records

Electronic record: record generated and stored in electronic form

Electronic signature: A digital mark, code, or other symbol that identifies an individual and indicates responsibility for or consent to the content of the material to which it is affixed.

Encryption: The conversion of data into a secret code for transmission over a network.

Export: a disposal process, whereby copies of a digital record (or group of records) are passed with their metadata from one system to another system. The record remains on the ERMS after export unlike during transfer.

File format: a standard or specification for the encoding of information in a file

File: An organized unit of documents accumulated during current use and kept together because they deal with the same subject, activity or transaction.

Filing: The systematic organization of records in groups or categories according to methods, procedures, or conventions represented in a filing system

Hybrid file: a set of related electronic records and/or physical records stored partly in an electronic file within the ERMS and partly in a related paper file outside the ERMS.

Information system: a system for generating, sending, receiving, storing or otherwise processing data messages and capable of being used in conjunction with external files.

Interoperability: The ability of one application, system, or metadata schema to communicate, work, or interface with another; the ability to provide services and accept services from other systems, enabling information that originates in one context to be used in another in ways that are as highly automated as possible.

Metadata: Data associated with either an information system or an information object for purposes of description, administration, legal requirements, technical functionality, use and usage, and preservation through time and within and across domains in which the data is created.

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 to ensure continued access to the information as the system or media becomes obsolete or degrades over time.

National Archives: Institution mandated by the Archives Act (1992) and responsible for the regulation, execution and administration of matters related to the custody and care of all public records.

Preservation: The processes and operations involved in the storage, stabilization and protection of documents against damage and deterioration and in the treatment of damaged or deteriorated documents and may also include the transfer of information to another medium.

Record creation: The first phase of a record's lifecycle in which a record is made or received and then set aside for action or reference.

Record: information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business.

Records lifecycle: the phases through which records pass, including creation, use and maintenance, and disposition (destruction or permanent preservation).

Records management: field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of record, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Refreshment: (of digital objects) conversion storage of digital components from one medium to another or otherwise ensure that the storage medium remains sound.

Reliable record: record whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Retention schedule: a set of instructions allocated to a series or file to determine the length of time for which its records should be retained by the organization for business purposes and the eventual fate of the records on completion of this period of time.

Retrieval system: A set of rules governing searching and finding records in a system, and the tools and mechanisms used to implement these rules.

Standard; Rules established to prescribe qualities or practices in order to achieve common goals of uniformity within or across a sector or system.

Systems administrator: a person responsible for the day to day operations of the institutional records management system.

Technological obsolescence: The process of becoming inaccessible or unusable through technological change.

Transfer: the disposal process consisting of confirmed export of digital records and folders followed by their destruction within the exporting ERMS

User: Any person utilizing an information system

Version control: The ability to track and manage the history of a particular piece of content including: the ability to rollback to a previous version of a document, the ability to track major and minor revisions of a document, and the ability to purge earlier versions of a document