AGENCIES

ELECTRONIC RECORDS MANAGEMENT AND ARCHIVES MANAGEMENT POLICY

Guidelines on Electronic Records Management: Managing Electronic Records in the Unstructured Environment

NATIONAL ARCHIVE OF MALAYSIA

ARKIB NEGARA MALAYSIA

Projek Pemeliharaan Rekod Elektronik Sektor
Awam
(e-SPARK)

Project Documentation

Guidelines on Electronic Records Management: Managing Electronic Records in the Unstructured Environment

Managing Electronic Records in the Unstructured Environment

Preface

This Guideline was produced as a result of the e-Spark initiative. Sponsored by the Arkib Negara Malaysia and involving public offices and agencies from across the Government of Malaysia, the purpose of this initiative was to develop policies, standards and practices, technical specifications and training plans to enable the Government of Malaysia to manage records in electronic form. Also included was a strategic plan reflecting the roles and responsibilities of public offices and various central and lead agencies. The Arkib Negara Malaysia, within its legislative mandate to facilitate the management of records in any physical form and to acquire, preserve and make available those of archival value, is the lead public office responsible for facilitating the government-wide management of electronic records. In this capacity and in cooperation with other central agencies and government public offices it is responsible for issuing standards and guidance to government public offices on the management of electronic records.

Managing Electronic Records in the Structured Environment is one of a series of guidelines that have been developed to help government public offices and agencies manage electronic records. This guideline should be used in conjunction with the general guideline, ***Guidelines on Electronic Records Management*** (also available from the Arkib Negara Malaysia). Companion guides are: ***Managing Electronic Records in the Structured Environment*** and ***Managing Electronic Records in the Web Environment.***

These guidelines should also be used in conjunction with ***Electronic Records and the Akta Arkib Negara 2003*** (available from the Arkib Negara Malaysia). This publication supports the implementation of the Akta Arkib Negara 2003 and the requirement by government departments not to dispose of their records without the approval of the National Archivist and to transfer records assessed as having archival value to the control of the Arkib Negara Malaysia.

For additional information, please contact:

Arkib Negara Malaysia,
Jalan Duta,
50568 Kuala Lumpur
Tel. 603-62010688
Fax. 603-62015679
Web Site: http://arkib.gov.my

Table of Content

SECTION 1

Managing Electronic Records in the Unstructured Environment

1. Purpose

The purpose of this section is to provide specific guidance on the management of electronic records generated in the ‘unstructured’ environment. This guide will be of particular interest to program managers and staff, LAN administrators, registry staff, and users of e-mail systems. This guide should be used in conjunction with ***Guidelines on Electronic Records Management*** and ***Electronic Records and the Akta Arkib Negara 2003*** (available from the Arkib Negara Malaysia).

2. The Unstructured Environment

The ‘unstructured’ environment is an environment where e-mail and other electronic documents are generated without the benefit of structured work processes or corporately endorsed procedures. Typically it is a user driven world where the user has autonomy concerning what gets created, how it is transmitted and how it is stored and otherwise managed. The absence of workflow within which records/documents (regardless of their physical form) can be captured in the context of their creation presents a substantial challenge from a record keeping perspective.

Unlike the ‘structured’ environment, issues and strategies associated with the creation, use, and preservation of electronic records in this environment do not have the benefit of an already existing infrastructure for managing the flow of documents (i.e. drafting documents, having them reviewed and approved, disseminating final products, etc.). As a result, and unlike the ‘structured’ environment where record keeping issues tend to focus on retention and disposition, in the ‘unstructured’ environment the entire life cycle of electronic records (i.e. creation, use, maintenance) must be addressed.

Some of the concerns being raised about the management of electronic records in this environment are as follows:

- The confusion over which e-mail messages and other electronic documents should be kept and which should be deleted.
- The difficulty in bringing together the complete “story” behind a decision or event because e-mail messages, their attachments and other related electronic documents may be stored in different locations.
- The difficulty in finding information because of the absence of commonly shared naming conventions for folders, and ad hoc approaches to establishing directory structures.
- The lack of a systematic approach to the retention and off-loading or deletion of files and folders.

- The absence of anyone to help set the business rules for managing work flow and the associated record keeping requirements for the benefit of those generating, exchanging, and using electronic documents.

Electronic Document and Records Management Systems (EDRMS), which are designed to address these issues, provide the most effective means for storing and retrieving electronic records in this environment. A properly implemented EDRMS provides:

- A trustworthy environment for the management of the authenticity and reliability of the records required for decision-making, program delivery, and accountability (though this may not be possible for records classified 'secret' or 'top secret').
- The ability to comply with government laws, regulations, policies, and guidelines.
- The ability to exploit information to serve purposes beyond those for which the information was originally created.
- The achievement of cost savings through the reduction in the time required to search for records, the freeing up of space for storing records, and the economies of scale that can be achieved in sharing records management systems and facilities.
- The ability of departments to maintain their corporate memory and to contribute to the wider archival memory of Malaysia.

Properly implemented, the system will permit records creators to file and retrieve electronic records and other forms of records to and from a trusted environment that meets records management policies and practices.

A Request For Proposal (RFI) has resulted in the identification of prospective vendors of EDRMS. The results of the RFI will be used to develop a prototype in order to better understand the implications of designing and implementing an EDRMS in public offices across the government. Based on the results of the experience gained through the prototype, decisions will be made concerning the establishment of a relevant procurement strategy for an EDRMS for use by public offices.

In preparation for the introduction of EDRMS technologies, two important foundation documents have been produced. Both are included in this Guide (Sections 2 and 3) and both are designed to serve as stepping stones contributing to improvements in the way in which electronic records are managed in this environment and pointing the way toward the introduction of EDRMS technologies. The first is guideline on the management of e-mail (Section 2) while the second is a guideline on the management of shared directories (Section 3).

Section 4 of this Guide is designed as a checklist to help public offices determine if their electronic document management systems can be considered sufficiently robust to serve as record keeping systems.

SECTION 2

Guideline on the Management of Electronic Mail[1]

1. Purpose

This e-mail guide gives guidance and instructions to help public offices identify, create, file and manage e-mail records so that sufficient and accurate evidence of official business and activities will be retained for legal, operational, accountability and archival purposes.

E-mail is increasingly becoming the primary business tool for both internal and external communication and as a result should be treated with the same level of attention given to drafting and managing formal letters and memos. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received. There is a common misconception that email messages constitute an ephemeral form of communication. Government officers should be aware that email messages form part of the corporate record.

The Government of Malaysia is studying the feasibility and implications of developing a properly designed EDRMS. **Pending the findings, Departments should adopt the 'print-and-file' approach to ensure that e-mails of records status are captured and preserved properly in an appropriate recordkeeping system[2]**

This e-mail guide is intended for all e-mail users, registry staff and departmental LAN Administrators. The principles and procedures in this e-mail guide cover all e-mail records unless otherwise specified.

2. E-mail as records

E-mail created or received for official business and kept as evidence of such business are records. They, like all other government records, are subject to the requirements of laws and regulations such as Security Regulations and the *Akta Arkib Negara 2003* and supporting policies and standards.

[1] Much of the guidance in this section was derived from an email guide developed for the Government of Hong Kong by the Government Records Service, 2002

[2] An appropriate record keeping system is one that has been designed and implemented and is under the control of the records management office of the department. See Section 4 of this Guide for the management and functional requirements that systems must respect if they are to be considered as record keeping systems.

To ensure that e-mail records are accurately and adequately documented and are readily retrievable and usable as and when required, they should be captured into a reliable recordkeeping system.

3. Appropriate Use of the Government e-mail System

3.1 Segregation of personal and official e-mail

The government e-mail system is installed for official business communication.

Although government policy permits officers to send and receive personal e-mail messages using the government accounts provided via the government e-mail system, extensive use of the system for private communication that may interfere with the normal work activities must be avoided. Comments or materials that are illegal, inappropriate, offensive or disrespectful to others should not be disseminated through the system.

To facilitate proper management of e-mail records, officers should avoid mixing official and personal e-mail documents in the same mailbox. Personal e-mails should be stored in a separate labelled folder in the local hard drive of an officer's workstation and be deleted or archived as soon as convenient.

3.2 Privacy of personal e-mail

The government does not guarantee privacy of personal e-mail sent or received via the government e-mail system, nor will the government be held responsible for such e-mail. It reserves the right to access all e-mail sent or received via the government e-mail system where circumstances warrant or for the purpose of, for example, system maintenance, guarding against unlawful activities or abusive behaviour.

The departmental LAN Administrator should maintain an e-mail traffic log[3] of the server (in electronic or paper format) that covers all e-mails, including personal e-mail transmitted through the government e-mail system, for security, statistics, diagnostic and other system monitoring purposes. Only authorized officers should have access to the log, which should be disposed of according to operational needs with a records disposal schedule agreed by the Arkib Negara Malaysia.

[3] This log is a record and contains information such as the timestamp and processing time of the event, message ID, sender, recipient and physical size of each e-mail. It may be printed and retained in paper form.

3.3 Ownership of government e-mail records

Official e-mail records are government property and the government has the right to access, read, use, manage and dispose of these e-mail records. Some e-mail records may also be selected as archives for permanent preservation.

3.4 Copyrighted materials

Copyrighted materials, including those downloaded from the Internet[4], should not be stored in the government e-mail system or disseminated to others without the prior permission of the relevant copyright owners.

4. Security of the Government e-mail System

Public offices are responsible for applying adequate security measures to their business routines and protecting government information and computer resources, including e-mail records and the e-mail system, against internal and external fraud and unauthorized access.

4.1 Access to Internet

Unless Internet access is made through an approved departmental Internet gateway, connections to the Internet should be restricted to dial-up connection from either standalone workstations or workstations that have been logged off from the LAN environment.

4.2 Password protection

To enhance the security of the government e-mail system, officers should set up passwords for their workstations and e-mail accounts to prevent unauthorized access and use. Officers should also safeguard and change their passwords regularly. Passwords should be difficult to guess but easy to remember, so that they do not have to be written down.

4.3 Virus Detection

The departmental LAN Administrator should arrange automatic updating of the virus signature or definition files for officers who use the government e-mail system. Officers should make sure that the auto-protection function of the anti-virus software in their workstation is always enabled whenever they use the system to access any document or information.

[4] Software from the Internet should not be downloaded to run on a government computer without permission of the copyright owner and the Head of the Public Office.

Officers should not open any e-mail from unknown or suspicious sources. The departmental LAN Administrator should be informed immediately should any virus be found.

4.4 Security after system logon

After logging on the e-mail system, officers should not leave their workstations unattended unless a password-protected screen saver has been activated.

4.5 Scanned (bit-mapped) signature

Attaching a scanned signature to an e-mail cannot authenticate the identity of the sender as a scanned signature can be easily cut and pasted or manipulated by others to give the appearance that a message was officially signed. Therefore, officers should not put scanned signatures in their e-mail messages or attachments.

4.6 Internet mailing list

Officers should use Internet mailing lists for internal user groups with great care. Exposing these lists to potential public mailing lists, such as newsgroups and web sites, may result in officers on the list receiving unsolicited e-mail from the Internet.

4.7 Backup

To avoid information loss during unexpected system shutdowns or failures, public offices should determine the nature and types of potential risks they may encounter and develop appropriate backup strategies for the e-mail system and e-mail documents.

Where backup procedures are automated with the use of appropriate software, the job logs of such backup runs should be checked to ensure that the backup operation is successful.

4.8 Related regulations and guidelines

In dealing with security issues relating to information systems and classified information in electronic form, Departments should follow the provisions of the Security Regulations and related circulars and guidelines on information technology security.

5. Creating e-mail Records

5.1 Titling email records

The title of an email message does not always reflect the reason for capturing an email message as a record. The problem of email titles not reflecting the reason for capturing the message as a record can, to some extent, be avoided through people following the guidelines for titling emails at the point they are created.

Subject Line

- Ensure the subject line gives a clear indication of the content of the message
- Indicate if the subject matter is sensitive
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required
- Indicate whether an action is required or whether the email is for information only

Subject and Tone

- Greet people by name at the beginning of an email message.
- Identify yourself at the beginning of the message when contacting someone for the first time.
- Ensure that the purpose and content of the email message is clearly explained
- Include a signature with your own contact details.
- Ensure your signature is not unnecessarily long
- Ensure that the email is polite and courteous.
- Tone of an email message should match the intended outcome.
- Make a clear distinction between fact and opinion.
- Proof read messages before they are sent to check for errors.
- Try to limit email messages to one subject per message.
- Include the original email message when sending a reply to provide a context.
- Where the subject of a string of email messages has significantly changed start new email message, copying relevant sections from the previous string of email messages.
- Ensure email messages are not unnecessarily long.
- Ensure that attachments are not longer versions of emails.
- Summarise the content of attachments in the main body of the email message.

Structure and Grammar

- Use plain language.
- Check the spelling within the email message before sending.
- Use paragraphs to structure information.
- Put important information at the beginning of the email message.
- Avoid using abbreviations.
- Avoid using CAPITALS.
- Try not to over-use of bold text.
- Do not use emoticons.

Addressing

- Distribute email message only to the people who need to know the information.
- Using ‘reply all’ will send the reply to everyone included in the original email.
- Think carefully before using ‘reply all’ as it is unlikely that everyone included will need to know your reply.
- Use the ‘To’ field for people who are required to take further action and the ‘cc’ field for people who are included for information only.
- Think carefully about who should be included in the ‘cc’ field.
- Ensure the email message is correctly addressed.

General

- Be aware that different computer systems will affect the layout of an email message.
- Avoid sending email messages in HTML format as if an email recipient is using an email system that does not allow HTML the layout will be affected.
- Be aware that some computer systems might have difficulties with attachments,
- Observe the restrictions on attachment size,
- Restrict the number of addressees,
- Try not to forward message unnecessarily. Put the email into a shared drive or public folder and provide a shortcut link,

6. Identification of e-mail messages

Where there is doubt as to whether an e-mail is a record, the subject officer should consider it a record, and arrange to have it filed in an appropriate manner.

Some typical examples of e-mail records are as follows:

- Correspondence relating to formulation and execution of policies and operating procedures
- Commitments, decisions, or approvals for a course of action
- Documents that initiate, deliberate, authorize or complete business transactions
- Work schedule and assignments
- Agenda and minutes of meetings
- Drafts of major policies or decisions circulated for comments or approval
- Final reports or recommendations
- Documents of legal or financial implications
- Acknowledgements of receipt of e-mail records that document essential transactions

Some typical examples of documents that are not e-mail records are as follows:

- Messages of personal nature
- Copies or extracts of documents that are published or downloaded and distributed for information or reference purposes
- Phone message slips
- Electronic copy of a record of which the paper copy has been filed

Contextual and structural details to be captured

To ensure the completeness and reliability of an e-mail record, in addition to its content, public offices should capture the following contextual and structural details as far as practicable:

- Details of the author (including the author's full name, designation, department, and e-mail address).
- Details of the recipient (including the recipient's full name, designation, department, and e-mail address).
- Transmission and receipt information (including date and, if necessary, time of sending and receiving the e-mail).
- Subject or title of the e-mail.
- File reference of the e-mail.
- Security grading (if applicable).

7. Filing of e-mail Records

7.1 The filing responsibility

To ensure that the record copy of an e-mail record is captured in the recordkeeping system, public offices should adopt the following rules:

- Where the sender and recipient(s) of an e-mail record are using the same file, the sender should designate his copy as the record copy and arrange to have it filed in the recordkeeping system; and
- Where the sender and recipient(s) of an e-mail record are using different files (for example, communication between a bureau and a department or with outside organizations or individuals), the action officer should arrange to have his copy officially filed.

7.2 Filing options

Once the decision has been made to keep a given e-mail (and its attachments) there are a number of options that can be employed for filing it. These include:

- Using Personal Folders in Outlook
- Using Public E-mail Folders
- Using Shared Directories
- Print to File

7.2.1 Using Personal Folders in Outlook

For many users in the Government of Malaysia this is the de facto option. It is based on storing 'in' and 'sent' e-mail messages and their attachments in personal e-mail directories the folders and directory structures of which are typically designed by the individual users. This is a very direct and convenient way to store and otherwise manage e-mail but it does have limitations:

- Access to important email and attachments by others (e.g. in a work group, etc.) may be inhibited if the user is not available to forward them or otherwise make them accessible;
- Important e-mail messages may be inadvertently deleted (e.g. when 'cleaning' out files, etc.);
- Accountability for the proper management of significant e-mail messages and their attachments rests entirely with the user. This could have serious implications if formal access requests require the production of email messages that the user cannot find or that he or she may have deleted;
- The filing structure and naming conventions used for defining folders may not be the same as the structure and conventions used for the shared directory (if is has been established) or the corporate file classification scheme thus inhibiting access to all of the documents related to a given decision, action, etc.

The last limitation can be addressed by setting up folder structures that mimic the shared directory or relevant areas of the departmental file classification scheme. However, this introduces an additional limitation in that the directory structures of individual users must be maintained in parallel with those established for the shared directory and the departmental file system.

7.2.2 Print to File

According to this option the user would print significant e-mail messages and their attachments and forward them to the records management office. This option is normally employed in those situations where the significance of the e-mail message is high enough to warrant its filing in a secure and completely trustworthy environment (i.e. based on paper and managed by the records management office). As explained in Section 3 (Managing Electronic Records in Shared Directories), the storage of electronic documents in public folders or in a shared space environment is not as secure as in an Electronic Document and Records Management System

(EDRMS). In order to maximize the utility of the available technology, however, and in the interests of efficiency (i.e. to reduce duplication) the printing of e-mail messages to paper should be the exception rather than the norm.

The role of the subject officer

The subject officer should confirm the record status of the e-mail sent or received through his mailbox, arrange to print the e-mail and attachment (as applicable) and pass them to the registry staff for filing.

The subject officer or his delegate should check and ensure that sufficient details of the content, context and structure of the e-mail record have been printed or manually marked on the printout.

The subject officer should arrange to:

- Print (and file) the e-mail as soon as possible upon its transmission or receipt;
- Print the e-mail directly from the e-mail client programme. To preserve record authenticity, the e-mail should not be exported or copied to other programmes for printing

If the time of transmission or receipt of the e-mail record is critical to the transaction, check the correct time on the e-mail server.

Where operationally required, identify the full name and designation of the recipient and manually mark such details on the printout.

Store multimedia or non-textual attachments that cannot be printed out to a designated directory on the server, change their attribute to read-only and manually record the full path of the network directory on the e-mail printout. To facilitate cross-referencing, there should be an index showing the details of the attachments stored in the designated directory and the file reference of the corresponding e-mail message.

The role of the registry staff

Similar to the handling of paper records, registry staff should classify, index and code the printout of e-mail records without delay.

Registry staff should ensure that all the necessary information is printed or manually marked on the printout and that all attachments, if any, are filed with the message in processing such records. Where there is doubt about the completeness of the record, advice from the subject officers should be sought.

7.2.3 Public Folders

Public folders are often set up to permit users to share their important email messages and their attachments. Users simply store their ‘in’ and ‘sent’ e-mail messages in their personal e-mail directories and then periodically copy the messages to the relevant public e-mail folders. Similar to the situation for ‘personal folders’ (see above), however, the implication is that two distinct repositories (public e-mail folders and folders on the shared drive) will need to be maintained in parallel. The management of the integrity of both repositories would require support from network services as well as expertise and care that would normally not be available on an ongoing basis in most program areas.

7.2.4 Filing into Shared Directories

E-mail software applications such as Outlook allow users to file their e-mail messages and their attachments directly into existing file folders on the shared directory. By dragging and dropping e-mail into pre-established shortcuts that are linked to favourite file folders within the shared directory structure individual users can easily ensure that all electronic documents supporting the same activity are accessible from a common set of folders accessible from either the user’s e-mail or from the windows file manager. Moreover these folders and the information they contain can be widely shared with anyone who has access to the shared directory. (See *Section 3: Managing Shared Directories* for additional information on managing shared directories)

7.2.5 Electronic filing Using an Electronic Document Records Management System (EDRMS)

An EDRMS can offer an effective and long-term solution to e-mail records management. In this regard, the government is studying the feasibility and implications of developing a properly designed EDRMS for service-wide application. Although detailed functional and management requirements for an EDRMS will be made available, a summary of key functional and management requirements that will be useful in assessing the capabilities of existing systems and/or document management systems procurements are described in *Section 4 - Electronic Document and Records Management Systems: Functional and Management Requirements.*

Departments using computer systems other than the government e-mail system to manage e-mail records are advised to contact the Arkib Negara Malaysia to confirm if their computer systems provide adequate records management functions. Individual departments who are planning to develop or install EDRMS should consult the Arkib Negara Malaysia before proceeding with a procurement initiative involving electronic document management and EDRMS systems.

8. Disposal of e-mail Records[5]

8.1 Destruction of the record copy

Public offices should make arrangements for their officers using the government e-mail system to separate e-mail records from personal e-mail messages and non-records in a timely manner. Identified e-mail records should be properly filed and disposed of when further retention is not required.

As is the case of paper records, public offices should, based on their legal, fiscal and/or operational needs, establish records disposal schedules for e-mail records and obtain the prior consent of the National Archivist before permanent erasure or destruction of the record copy. See ***Electronic Records and the Akta Arkib Negara 2003*** for more information (available from the Arkib Negara Malaysia).

8.2 Deletion of the electronic copy after filing

In general, after the printout copy of the e-mail record has been captured into a recordkeeping system, the subject officer or his delegate should erase or delete the electronic copy, which is no longer a record, from his or her mailbox.

8.3 Destruction of Transitory Records

Officers should check their workstations regularly to delete transitory records. Transitory records such as the duplicate electronic version of e-mail records, convenience or reference copies of e-mail records and personal e-mail messages can be disposed of without separate authorization of the Arkib Negara Malaysia.

8.4 Transfer of archival e-mail records to the Arkib Negara Malaysia

Public offices should transfer those e-mail records appraised by the Arkib Negara Malaysia as possessing archival value to the Arkib Negara Malaysia for permanent retention according to standards issued by the Arkib Negara Malaysia (see ***Electronic Records and the Akta Arkib Negara 2003*** available from the Arkib Negara Malaysia).

[5] Disposal actions may include physical destruction or permanent erasure of records of no residual value, transfer of records to the Arkib Negara Malaysia for inactive storage for a specific period before destruction/erasure, or transfer of records appraised to have archival value to the Arkib Negara Malaysia for permanent retention.

9. Management of Classified e-mail Messages

At the moment, only systems that conform to the requirements stipulated in the Security Regulations may be used to transmit electronically classified documents up to 'confidential' level. Transmission of 'secret' and 'top secret' e-mail should follow the requirements specified in the Security Regulations.

Before using secure systems to transmit classified records, officers must be equipped with the necessary equipment and facilities. In addition, officers should make sure that the recipient(s) are registered users of the secure system and the 'Subject' and 'File Reference' fields of the message to be transmitted do not contain classified information.

9.1 Printing and handling of restricted and confidential e-mail records

In addition to the procedures given elsewhere in this guideline, the subject officer or his delegate should only use a local printer or remote printer in a trusted network to print restricted and confidential e-mail and attachments. Requirements in the Security Regulations should also be observed.

For e-mail records transmitted via secure systems, if the trust validation information is required for the transaction of business or record purpose, the subject officer should sign the corresponding printout to confirm that the identity of the sender is checked and verified correct, and, if required, arrange to also print-and-file the screen dumps used to verify the digital signature.

Registry staff should classify and put the printout of security graded e-mail records on paper files that have the same security classification as the records, and strictly follow the Security Regulations in handling different security graded documents.

9.2 Destruction or erasure of restricted and confidential e-mail records

Public Offices should follow the requirements stipulated in the Security Regulations in disposing of or erasing restricted and confidential e-mail records. All classified information should be cleared from the electronic media before disposal. If the classified information cannot be cleared completely, the media unit should be physically destroyed in a manner that prevents recovery of the information.

Prior consent of the Arkib Negara Malaysia must be sought before any classified e-mail records are destroyed or permanently erased.

9.3 Related regulations and guidelines

In addition to the Security Regulations, Departments should also refer to the most up-to-date guidelines and manuals issued by MAMPU on matters relating to system operation, administration and security.

Section 3

Managing Shared Directories[6]

1. Introduction

The Government of Malaysia is in the process of assessing the introduction of electronic document and records management systems (EDRMS) to support the management of the information required to deliver government programs and services and to meet various accountability requirements.

Until such a system is introduced, interim guidance is required to assist users in leveraging their existing infrastructure to ensure ongoing and timely access to the reliable and authentic documents and records they need.

This guide is designed for individuals in a given organizational unit where there is a requirement for information to be shared and where the members of the unit have access to a shared drive.

This Guide should be used in conjunction with *Section 2: Managing e-mail*.

2. Managing Electronic Documents on Shared Drives

In most organizations the shared drive, or “S” drive, is used as a place to store electronic documents that can be shared with others. Folders are created by individual users to store a wide range of electronic documents including reports, presentations, briefing notes, drafts, etc. Unfortunately, little consideration is often given to setting them up so that the documents they contain are easy to find and use:

- With exceptions, folder names are often created with little regard to commonly shared naming conventions and their locations may not be within the directories already established to store similar or related materials.

- Often, there is little systematic attention to file retention and off-loading, or to the deletion of files that are well beyond their usefulness to the organization. As large volumes of transitory records (i.e. those not contributing directly to the corporate memory) are mixed in with valuable “corporate memory” records and as the volume of the entire file grows, it becomes difficult to find the significant from among the insignificant.

- Rarely has anyone been assigned responsibility for managing shared drives. This leaves the drives open to arbitrary reorganizations or deletions thus compounding the confusion among those using the shared drives.

[6] Much of the guidance in this section was derived from the guide, *Managing Shared Directories*, Industry Canada, 2003

Until the Electronic Document and Records Management System (EDRMS) is introduced, this guide (in conjunction with, *Section 2 - Managing E-mail*) and the shared directory facilities provided within existing networks should be used to enhance the manner in which electronic records are filed and retrieved. It is important to recognize that an enhanced shared directory is not necessarily a record keeping system. Rather it is a stepping-stone that should be employed to set the stage for the introduction of the EDRMS which will be designed to be compliant with record keeping standards and practices.

The major reasons why a shared directory is not a recordkeeping system are as follows:

- Accountability for the integrity of the shared directory normally rests with the relevant program manager. Accountability for the integrity of an EDRMS rests with the records management office. The primary concern of a program manager is the delivery of his or her program. The integrity of the record-keeping environment, while important, is of secondary concern. The primary concern of the records management office, however, is the integrity of the record keeping function across the department and the integrity of the systems supporting this environment. This is why an EDRMS is considered to be trustworthier than a shared directory. The proposed EDRMS will be under the control of the records management office and will reflect sound and generally accepted record keeping standards and practices. The shared directory, while supporting an important sub-set of the functional requirements of an EDRMS is considered to be an interim step at best.
- While the classification scheme employed for a shared directory should be consistent in design with the corporate file classification scheme. However, it may not always be possible to ensure this consistency in an environment where control over the integrity of the shared directory essentially rests with the program head rather than the records management office supported by staff who have the expertise as well as the responsibility for managing the integrity of the classification scheme.
- The corporate file classification scheme is used as the basis for managing the retention and disposition of records regardless of their physical form. If the classification scheme for the shared directory is not consistent with the corporate classification scheme then it may undermine the ability of the program area to comply with the retention and disposition provisions of various laws and policies.
- All of the security and other protection measures normally associated with an EDRMS may not be present in the shared directory environment. This is why the risk to the integrity of electronic records and the potential for records loss is much higher in a shared directory environment than it is in an EDRMS. In situations where highly significant documents are being generated, the risk may be sufficiently great to warrant against using a shared directory.

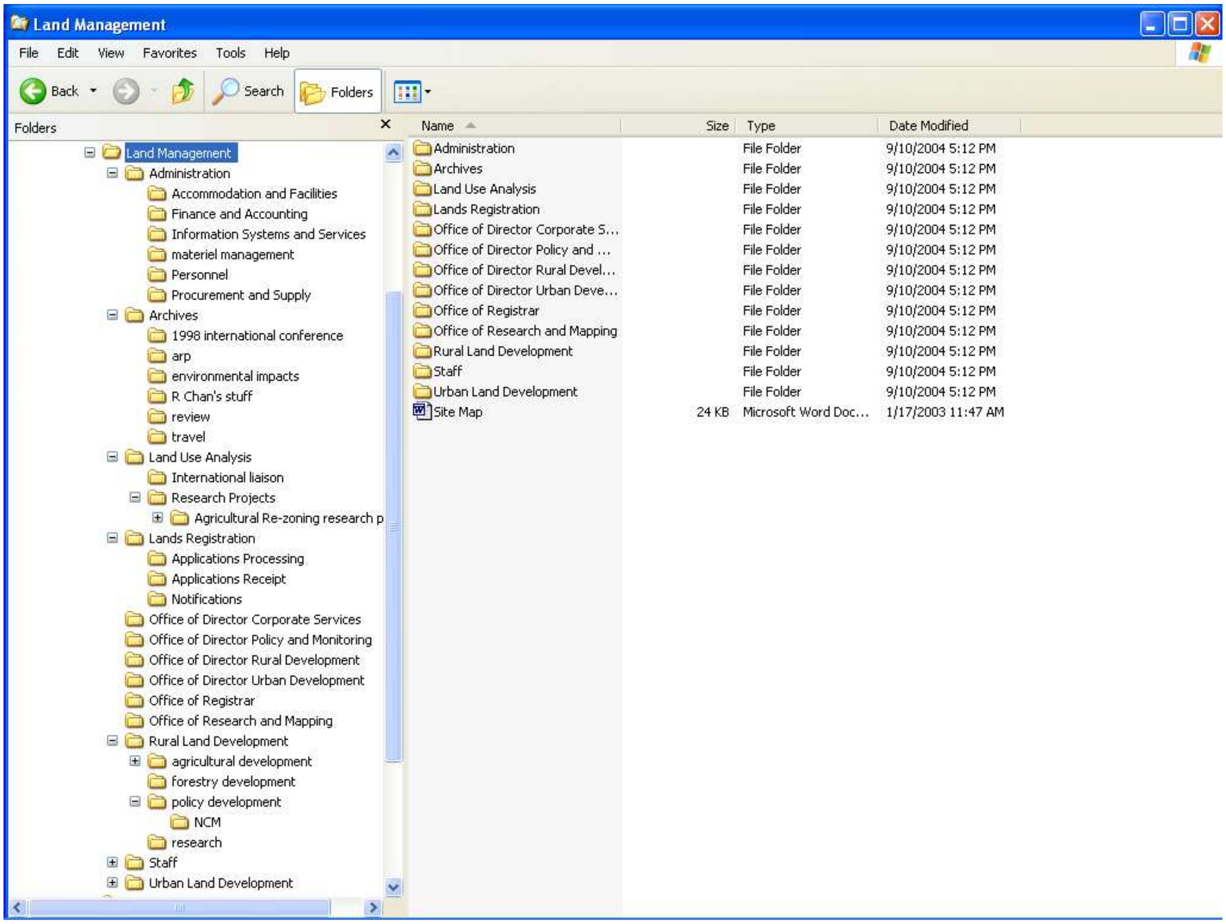
These distinctions between a shared directory and an EDRMS are important because they have an impact on decisions regarding the extent to which a shared directory can serve as a viable record keeping option. In some programs of the department the nature of the activities and the records generated in support of these activities may be of a kind where the risks of using a shared directory are low. In other cases the risk may be much higher. Program managers should consult with their records management offices or the National Archives to obtain advice concerning the extent to which a shared directory may be considered adequate for the management of its records.

2.1 Configuring the Shared Directory

The following steps are designed to help staff in any given organizational unit to migrate to a new directory structure in a manner that minimizes disruption while maximizing the value of the directory to the unit:

- **At the first level below the root of the shared drive (e.g. ‘S:’), create ‘top level’ folders for each of the key lines of business or functional areas of the organizational unit**[7] (see figure 2.1.1 for an example based on a fictional department). These folders should be created in cooperation with records specialists. Under each of the top level folders create sub-folders reflecting key activities, sub-activities, projects, issues, etc. related to the line of business, functional area, etc.

[7] Consistently named records foster collaboration based on mutual understanding of how to name files and use file names (including the file name metadata). Consistently named records also help to meet the legal requirements of being trustworthy, complete, accessible, legally admissible in court, and durable for a slong as your approved retention schedules require. Records that are consistently and logically named are easier to manage to meet these requirements



Folders

- Land Management
  - Administration
    - Accommodation and Facilities
    - Finance and Accounting
    - Information Systems and Services
    - materiel management
    - Personnel
    - Procurement and Supply
  - Archives
    - 1998 international conference
    - arp
    - environmental impacts
    - R Chan's stuff
    - review
    - travel
  - Land Use Analysis
    - International liaison
    - Research Projects
      - Agricultural Re-zoning research p
  - Lands Registration
    - Applications Processing
    - Applications Receipt
    - Notifications
  - Office of Director Corporate Services
  - Office of Director Policy and Monitoring
  - Office of Director Rural Development
  - Office of Director Urban Development
  - Office of Registrar
  - Office of Research and Mapping
  - Rural Land Development
    - agricultural development
    - forestry development
    - policy development
      - NCM
    - research
  - Staff
  - Urban Land Development

Name	Size	Type	Date Modified
Administration		File Folder	9/10/2004 5:12 PM
Archives		File Folder	9/10/2004 5:12 PM
Land Use Analysis		File Folder	9/10/2004 5:12 PM
Lands Registration		File Folder	9/10/2004 5:12 PM
Office of Director Corporate S...		File Folder	9/10/2004 5:12 PM
Office of Director Policy and ...		File Folder	9/10/2004 5:12 PM
Office of Director Rural Devel...		File Folder	9/10/2004 5:12 PM
Office of Director Urban Deve...		File Folder	9/10/2004 5:12 PM
Office of Registrar		File Folder	9/10/2004 5:12 PM
Office of Research and Mapping		File Folder	9/10/2004 5:12 PM
Rural Land Development		File Folder	9/10/2004 5:12 PM
Staff		File Folder	9/10/2004 5:12 PM
Urban Land Development		File Folder	9/10/2004 5:12 PM
Site Map	24 KB	Microsoft Word Doc...	1/17/2003 11:47 AM

Figure 2.1.1: Shared Directory Structure

- **Create additional 'top level' folders** for each of the following:

  - **The offices of senior officials responsible for the management of the organizational unit.** These folders can be used to store those documents that serve as a documentary trail of management decisions taken and a valuable information source for decisions yet to be made by the managers of the organizational unit.

  - **The 'administration' of the organizational unit.** This folder would be broken down into sub folders and sub-sub folders in accordance with the structure and naming conventions used for describing administrative files (consult with the records management office or the National Archives for advice concerning the naming conventions used to describe administrative files). The folders would contain the records of the administrative transactions carried out in support of the functions of the organizational unit. If the organizational unit comprises discrete sub units (e.g. directorates within a Branch) then it may be desirable to create an 'Administration' sub-folder for each sub-unit;

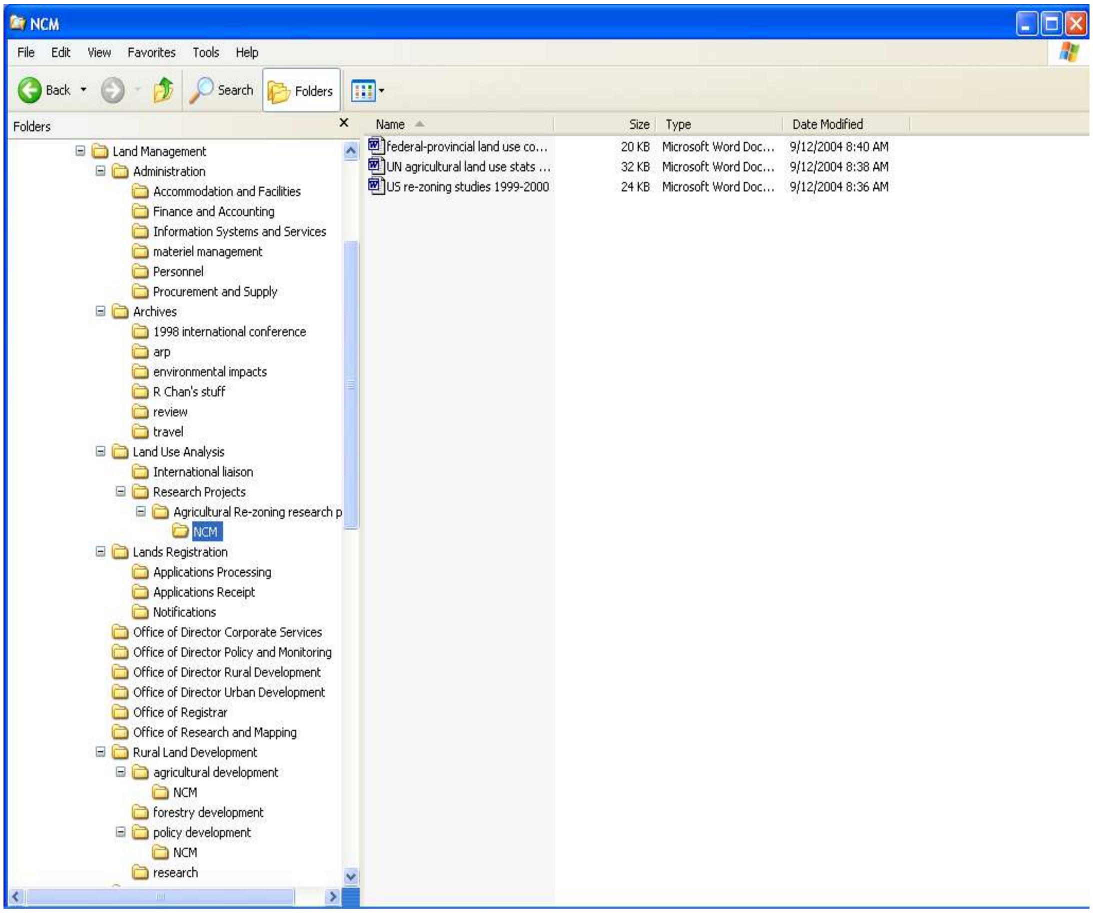
  - **<u>The 'staff' of the organizational unit or work group</u>.** The titles of the sub-folders under the Staff-folder would be the names of the individual staff members in the organizational unit. A staff sub-folder would be password protected and would enable the individual staff member to create, edit, and store documents within the context of a given business activity but without having to worry about the document being accessed by others. Once the document was ready to be shared it would be moved to the appropriate folder on the new shared directory.

  - **<u>The 'archives' containing the directory structure and contents of the 'old' shared directory</u>.** Folders and files considered to be relevant and important to the work of the organizational unit would be migrated to the new directory structure leaving the remainder in the 'archives'.

- **<u>Create a sub-folder called 'NCM" (Non-Corporate Memory) underneath relevant folders in the new directory</u>** for cases where large volumes of reference material or other material not directly supporting corporate memory are being acquired to support a specific activity or project, (see Figure 2.1.2). This will permit valuable corporate documents to be distinguished from related though voluminous reference materials or other records of a transitory nature. This will facilitate access and retrieval as well as disposition (i.e. based on the premise that records not contributing directly to corporate memory may be disposed of earlier than the more significant records that document the activity and contribute directly to corporate memory). In some cases, a non-corporate memory document may become significant when it is used to directly support an important policy decision or business activity. This will change its status and require it to be moved from the NCM folder to the relevant master folder.

- **<u>Use the new folder structure to store electronic documents generated or received in the organizational unit</u>.** Gradually migrate relevant files from the former directory structure (now under the top level folder 'archive') to the appropriate folders in the new directory structure.

  One technique that can minimize the burden on users is to announce a 'new drive' day. On that day (or the night before), key folders used in the existing folder structure on the shared drive would be moved under the relevant high-level folders. The 'fit' (re: the relationship between the existing folders and their new parent folders) may be only approximate and the user defined folder names would not be changed but at least users would be able to see 'their folders' in the new structure. Other folders that are only occasionally accessed would also be moved but any folders that had not been accessed for a considerable period of time would be moved to the new 'archives' folder. Over time, adjustments would be made to the folder titles and structure to ensure that they were in line with the needs of the group and the 'rules of the road' described in the remaining sub-sections of this guide (as augmented by those in, *Section 2: Managing E-mail*).



- Land Management
  - Administration
    - Accommodation and Facilities
    - Finance and Accounting
    - Information Systems and Services
    - materiel management
    - Personnel
    - Procurement and Supply
  - Archives
    - 1998 international conference
    - arp
    - environmental impacts
    - R Chan's stuff
    - review
    - travel
  - Land Use Analysis
    - International liaison
    - Research Projects
      - Agricultural Re-zoning research p
        - NCM
  - Lands Registration
    - Applications Processing
    - Applications Receipt
    - Notifications
  - Office of Director Corporate Services
  - Office of Director Policy and Monitoring
  - Office of Director Rural Development
  - Office of Director Urban Development
  - Office of Registrar
  - Office of Research and Mapping
  - Rural Land Development
    - agricultural development
      - NCM
    - forestry development
    - policy development
      - NCM
    - research

Name	Size	Type	Date Modified
federal-provincial land use co...	20 KB	Microsoft Word Doc...	9/12/2004 8:40 AM
UN agricultural land use stats ...	32 KB	Microsoft Word Doc...	9/12/2004 8:38 AM
US re-zoning studies 1999-2000	24 KB	Microsoft Word Doc...	9/12/2004 8:36 AM

Figure 2.1.2: Use of Non Corporate Memory (NCM) sub-folders

2.2 Naming Directory Folders

The business lines and functions of the organizational unit are normally used as the basis for the names of the directory folders for the first and second levels of the directory.

Example

Land Use Analysis
Research Projects

Before proceeding to establish the upper two levels of the new directory structure, consult specialists in the records management office. They are experts in setting up directory structures and will ensure that the directory structure and naming conventions used to establish the upper two levels will be consistent with others established across the department. As indicated under 'Governance', later in this section, it is proposed that a coordinator be named within the organizational unit or work group to manage the shared directory. Among other roles, the coordinator would work with records management specialists to facilitate the establishment of the upper two levels of the directory structure.

After the upper level directory structure is established, staff in the organizational unit should use the following guidance to create folders at lower levels of the directory structure:

- **Use full, descriptive, easily understood names** that reflect the functions and activities of the organizational unit as well as the subject matter of the files in the folder.

Example

Land Use Analysis
Research Projects
Agricultural Re-zoning Research Project

- **Incorporate the year into the title of the folder.** This will indicate that all files stored in a particular folder pertain to a particular year. Such a convention will make it easier to search through large numbers of files where the date of the file being searched is known. It will also facilitate the management of their future retention and disposition.

Example

Land Use Analysis
Research Projects
Agricultural Re-zoning Research Project 1999

- **Incorporate the date when the files in the folder will no longer be relevant or will have lost their value**. This will help to indicate the relevance of a folder being searched and facilitate decisions concerning disposition of the files in the folder.

Example

Land Use Analysis
Research Projects
Agricultural Re-zoning Research Project 1999
[dispose: 2010]

- **Avoid the use of acronyms** other than those universally understood: such as IC, Min, DM, ADM, DG, UN, USA, etc. This will make it easier to understand the contents of a folder.

Example

Agricultural Re-zoning Research Project (vs ARRP)

- **Use standard terms when establishing the names of folders.** Organizations should ensure that a list of standard terms is made available to users electronically. For instance, the Program/Activity structure supported by the Financial Administration area of the department or the subject file classification systems supported by the records management office could be used as sources of the terms for populating the function/activity driven directory structure. Similarly, the naming conventions developed by the National Archives to describe administrative subject files (i.e. functional records) should be used to generate the names of folders under the high-level folder title "Administration".

- **Add "NCM" to the end of the titles of those sub-folders that have been created to hold records not directly supporting corporate memory.** This will make it easier to distinguish between those folders containing significant documents directly supporting corporate memory from those that do not. It may also be useful to include a "best before date" to facilitate retention and disposition (See Section 2.1 for additional information on the creation of NCM folders).

Example:

Agricultural Re-zoning Research Project
Federal-provincial land use conference proceedings 2003 NCM BB April 2005

- **Have names of sufficient length to make them intelligible to those unfamiliar with the subject area.** 50 characters may prove a maximum reasonable length. However, it is important to note that while some word processing software supports 50 characters, other applications software may be limited with respect to the number of characters they can support.

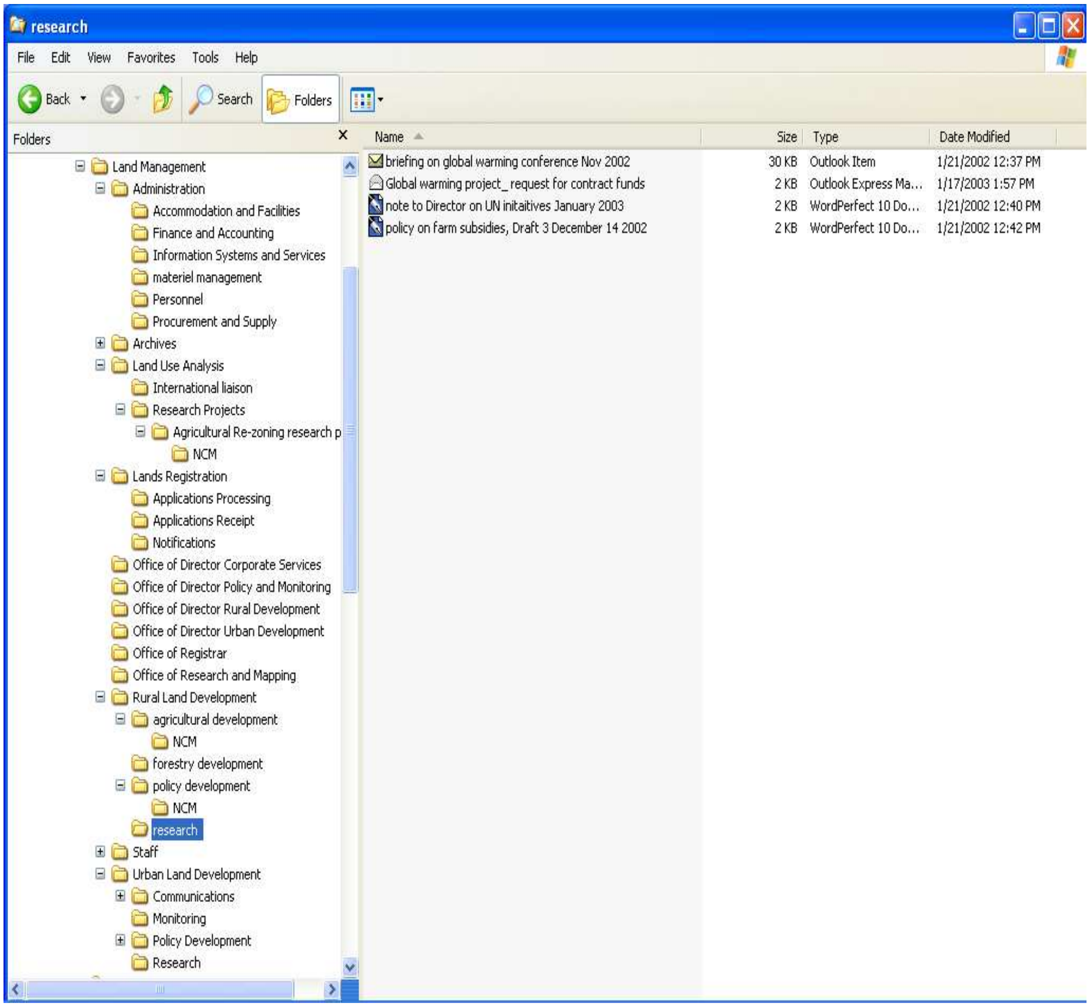
- **Avoid the creation of folders more than five levels below the root folder**. Extended directory structures can make navigation difficult.

- **Ensure that all folders in the new directory are 'read only'.** This will protect valuable documents from being altered or deleted.

2.3 Naming Files

Standard file naming conventions should be used to facilitate shared access and retrieval of electronic files. To this end, the following conventions should be used:

- **<u>Use full names that are descriptive and identify clearly what is in the file</u>** (see Figure 2.3.1). In addition to the title consider adding the following:
    - The document type (i.e. briefing note, policy, guidance, discussion paper etc.).
    - Document status (final, working draft, first draft, copy sent to Chief Secretary, deck, etc.).
    - Date created and or date when the document is no longer relevant, its value has expired, etc.
    - The recipient, originator and/or audience.



- Land Management
    - Administration
        - Accommodation and Facilities
        - Finance and Accounting
        - Information Systems and Services
        - materiel management
        - Personnel
        - Procurement and Supply
    - Archives
    - Land Use Analysis
        - International liaison
        - Research Projects
            - Agricultural Re-zoning research p
                - NCM
    - Lands Registration
        - Applications Processing
        - Applications Receipt
        - Notifications
    - Office of Director Corporate Services
    - Office of Director Policy and Monitoring
    - Office of Director Rural Development
    - Office of Director Urban Development
    - Office of Registrar
    - Office of Research and Mapping
    - Rural Land Development
        - agricultural development
            - NCM
        - forestry development
        - policy development
            - NCM
        - research
    - Staff
    - Urban Land Development
        - Communications
        - Monitoring
        - Policy Development
        - Research

Name	Size	Type	Date Modified
briefing on global warming conference Nov 2002	30 KB	Outlook Item	1/21/2002 12:37 PM
Global warming project_ request for contract funds	2 KB	Outlook Express Ma...	1/17/2003 1:57 PM
note to Director on UN initaitives January 2003	2 KB	WordPerfect 10 Do...	1/21/2002 12:40 PM
policy on farm subsidies, Draft 3 December 14 2002	2 KB	WordPerfect 10 Do...	1/21/2002 12:42 PM

Figure 2.3.1: Examples of names of files

- **Avoid the use of acronyms,** other than those universally understood (i.e. IC, Min, DM, ADM, DG, UN, USA, etc.). This will facilitate understanding of the contents of the file.

  Example:

  Policy on Farm Subsidies, Draft 3 December 14 2002 (rather than PFS)

- **Keep the lengths of the names to no more than 50 characters.**

- **Identify the version of the document.** One approach is to add a field to the name of the file to reflect the version (e.g. *Policy on Emerging Technologies 3*). For those collaborating on a document use a number to reflect the version and a letter code such as "a" to identify one individual and "b" to identify the other. When the documents are listed it will be possible to identify the version and the author.

  Examples:

  Policy on Farm Subsidies 3a.doc
  Policy on Farm Subsidies 3b.doc
  Policy on Farm Subsidies 4a.doc
  Policy on Farm Subsidies 4b.doc

- **Complete relevant fields in the 'document properties' menu.** For WORD, access "file" in the toolbar, then "properties". The default fields can be deleted and augmented as desired. In addition to providing more contextual information regarding individual documents they are also fully searchable thus adding a level of support to future retrieval.

- **Embed the path and file name in the document at the time of storage**. This is an excellent, and highly recommended, practice that will greatly facilitate the identification of the location of the electronic version of a document. This can be accomplished, for example, in a footer which can be displayed at the bottom of each page or at the end of the last page of the document.

  In MS Word first save the file with an appropriate name and location; then insert the path in the document by positioning the cursor at the desired insertion point and clicking on "Insert" in the tool bar, then "Auto Text", then "Header/Footer", then "Filename and Path" (see Figure 2.3.2).

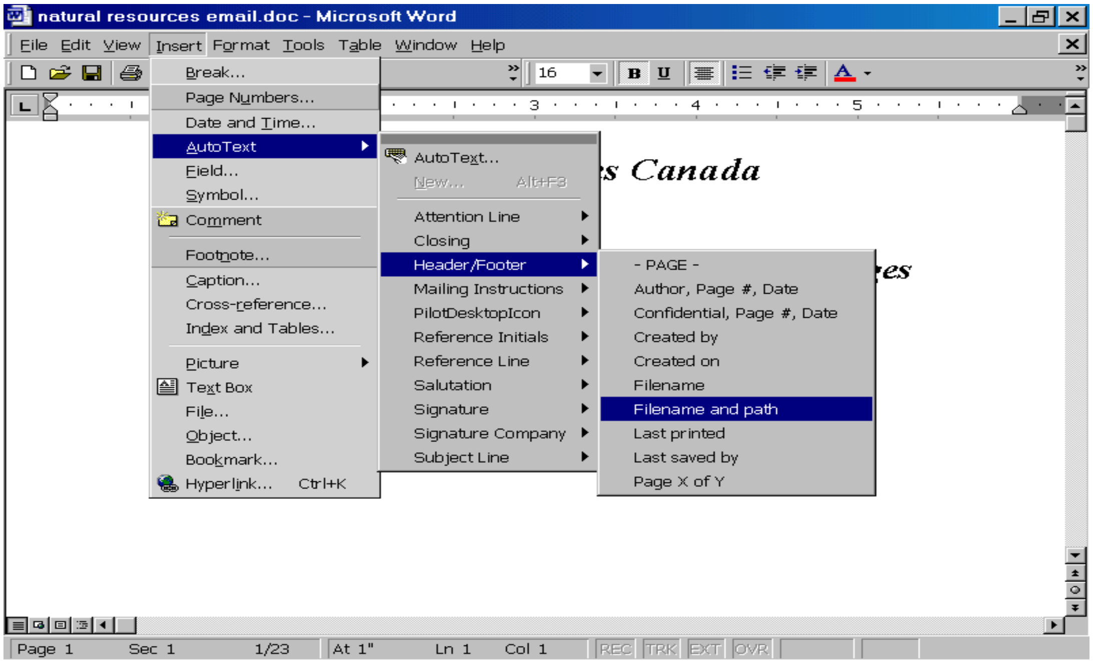


Figure 2.3.2: Inserting path names using Word

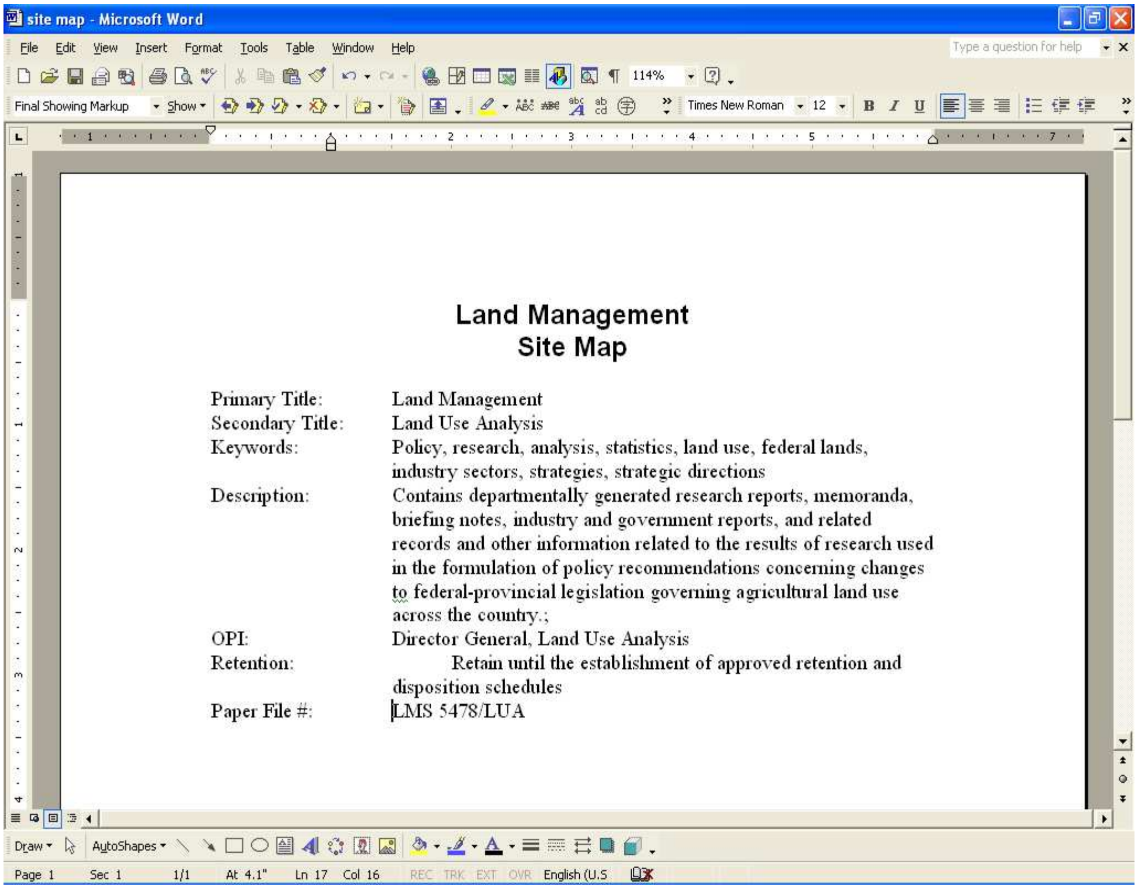
2.4 Creating a Site map For The New Shared Directory

A site map should be created to reflect the first two levels of the Directory structure and stored as a read-only document in the root folder of the new shared directory.

The site map documents and maintains the directory and supports the retrieval of files. The site map will be useful to new staff and others who need to understand the new directory structure in order to use it more effectively. It will also be useful to those who want to know more about the proposed contents of a given high-level folder before filing their documents. For those retrieving files, the site map provides valuable contextual information (e.g. description of the folder; list of sub-folders) that will help guide the search.

Each of the directory folders for the first and second levels of the new shared directory should be described on the site map using the following fields (see figure 2.4.1 for an example of a completed profile):

Title:
Keywords:
Description:
List of sub-folders:
Responsible Officer:
Retention:
Paper File #:


site map - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Type a question for help
114%
Final Showing Markup
Show
Times New Roman
12
Draw
AutoShapes
Page 1 Sec 1 1/1 At 4.1" Ln 17 Col 16 REC TRK EXT OVR English (U.S

Land Management
Site Map

Primary Title:	Land Management
Secondary Title:	Land Use Analysis
Keywords:	Policy, research, analysis, statistics, land use, federal lands, industry sectors, strategies, strategic directions
Description:	Contains departmentally generated research reports, memoranda, briefing notes, industry and government reports, and related records and other information related to the results of research used in the formulation of policy recommendations concerning changes to federal-provincial legislation governing agricultural land use across the country.;
OPI:	Director General, Land Use Analysis
Retention:	Retain until the establishment of approved retention and disposition schedules
Paper File #:	LMS 5478/LUA

Figure 2.4.1: Example of a site map profile

2.5 Finding and Retrieving Electronic Documents

There are a number of ways to retrieve documents from a new shared directory:

- Use the site map of upper level folder descriptions stored in the root folder of the S: drive to browse and search for desired subjects and key words.

- Use the file name or full-text search facility in WORD under “File”, “Search”. Be aware that WORD searches can be rather slow.

- Use the Windows file name or full-text search facility. Use “Start”, “Find”, “Files and Folders”. Users should be aware that this search tool, which is quick and effective when used to identify file names based on specific words, is far less consistent in full-text mode especially in the case of documents prepared in WORD.

3. Filing E-mail Messages into Shared Directories

The guidance provided in this sub-section should be used in conjunction with related guidance in, *Section 2: Managing E-mail*.

The benefits of using a shared directory (rather than other directories such as personal folders) for the filing of e-mail messages and their attachments are as follows:

- Important information in the messages and their attachments can be shared with others.
- E-mail messages can be linked to related documents within the same directory structure.
- Access to all of the information pertaining to a decision, activity can not only be possible, it can be seamless.
- E-mail messages can be stored in their native format and accessed, opened, and used (and re-used) as e-mail.
- Shortcuts can be rapidly re-configured to reflect a user's current set of favourites based on the folders in the shared directory.
- Each user can set up their own customized links without having to rely on network staff.

3.1 Procedures for filing e-mail messages

These benefits of using the shared directory for storing and retrieving e-mail messages can be obtained by following these simple steps (for Microsoft Outlook users only):

- Establish a group of outlook shortcuts:
  - Right click on the Outlook shortcut bar and select *Add New Group*
  - In blank *Group* which appears at the bottom of shortcuts enter the new name of the group (based on the directory structure)
  - Move the new group to the top of the Outlook shortcut bar by clicking anywhere outside the group and then re-clicking on the new group. Add additional groups in line with the directory structure
  - Right click on the renamed group and select O*utlook Bar Shortcut*
  - When *Add To Outlook* bar pops up select the target file system using the radial bar in "*Look In*"
  - Navigate to the desired "S" drive and click *OK* on the folder to be selected
  - *File Folder* will appear under the newly created group in outlook

In order to add additional folders under any established group:

- Click on one of the folders in the group (view of desktop appears in outlook with folder list)
- Drag folders from the folder list and drop under the appropriate shortcut bar

Periodic transfer to the shared directory should be undertaken frequently to ensure that those accessing the relevant folder on the shared directory are able to retrieve the ‘complete story’ including relevant e-mail messages.

3.2 Naming e-mail Messages

The following guidance (for Microsoft Outlook users only) is provided for those situations where e-mail messages and their attachments are to be stored on the “S” drive. See *Section 2: Managing E-mail* for additional information on naming conventions for e-mail messages.

- *E-mails should be saved with the “.msg” extension.* This ensures that an association is made with Outlook so that it will retain it’s e-mail message characteristics (look and feel). When the file is opened in Windows Explorer, Outlook will be launched as the application. Outlook will normally embed the attachments in the saved file when the message is saved with the “.msg” or the “.rtf” extension.

- The resulting “.msg” file is a separate file from the e-mail message stored in an Outlook folder and is treated as such by the operating system (i.e. deleting the e-mail will not delete the S: drive copy and vice versa).

- *E-mail file naming conventions*. The names applied to e-mail filed in the new directory structure should be consistent with the naming conventions applied to other electronic records held by the organizational unit (see *Section 2.3: Naming files*). In addition, one should be aware of the following:

  - Use full descriptive titles in the subject lines for all email messages (these can be used as key words for future retrieval). The inclusion of a creation or “best before” date after the subject in the subject line (based on the format yy-mm-dd) will help organize the material according to date;

  - Saving an e-mail as a file will mean that the e-mail parameters “to” “from” “subject” etc. will no longer be displayed in Windows Explorer or in Outlook. To access that information the file itself must be opened. To see this information directly you must incorporate them into the file name.

  - Saving e-mails as “.msg” files also saves attached files as embedded documents in the file. These will be available in the same way as they are available as e-mail attachments.

- Meaningful titles for attachments should be provided to facilitate understanding of what the attachments are about and to facilitate their future retrieval.

- Large volumes of e-mail messages and their attachments generated for a single activity can lead to a substantial increase in the size of individual folders. This can lead to difficulties in terms of future access and retrieval. One option is to create folders by date range and then to move the e-mail messages and their attachments into the folders according to their date.

3.3 Applying e-mail Protocols

There are a number of rules of the road that can facilitate the future retrieval of e-mail and their attachments as well as the other related documents pertaining to a given decision, topic, issue, project, etc. The following rules, which focus on the filing of e-mail messages, augment those described in *Section 2: Managing E-mail*.

- The author of an e-mail message should be the individual responsible for ensuring that a copy of what he or she sent is saved (i.e. directly into the relevant public folder or the relevant folder in the shared directory, or in their personal e-mail folders for eventual transfer to either the public folder or the shared directory).

- Unless instructed to do so, staff who receive an e-mail from another staff member or executive in the same organizational unit are not required to save a copy of the e-mail as it will be assumed that the e-mail will have already been saved.

- If a staff member receives an e-mail and is directed to take some action based upon the message, the recipient should file the e-mail either directly in the appropriate folder on the new shared directory or in a personal e-mail folder for eventual transfer to the shared directory (or to the relevant public folder).

- While executive level staffs are responsible for filing e-mail they may choose to forward the e-mail to others asking them to file it on their behalf (e.g. “please action and file”).

- E-mail pertaining to subjects, issues, activities, etc. that are not covered in the filing system may trigger the need to create a new folder in the shared directory. This should be undertaken by the person responsible for filing it, whether the author, the recipient of a message from outside the organizational unit, a Director, or their designates (e.g. “Please action - looks like an important new initiative - please create new corporate memory folder”).

- E-mail from outside of the organizational unit directed to multiple recipients’ presents a special problem. Normally the first person on the “to” line or their designate should be the individual responsible for filing the e-mail.

- In forwarding email to others, instructions should be included to guide what should happen to the email (i.e. the desired action, status and disposition of the message (e.g. 'for discussion'; 'for action and file'; etc.).

- When the subject in a chain of e-mail messages changes to another topic, activity, issue, etc., the chain should be stopped, the e-mail messages filed, and a new chain established with the subject line reflecting the new topic, issue, etc.

4. Retaining and Disposing Of e-mail Messages and Other Electronic Documents

E-mail systems are not record-keeping systems which is why this guide emphasizes the importance of moving significant e-mail messages and their attachments to the new shared directory and, eventually to the planned electronic document and records management system.

Consult with records management specialists to determine if a retention schedule has been established for the records generated in the organizational unit.

If a retention and disposition schedule is in place:

- Use it to guide the establishment of retention and disposition specifications for the folders in the shared directory (or public folders if these are being used).

- Store the retention and disposition specifications for the folders in the "1 New Drive" directory structure as folder attributes on the site map.

- Consult with records management specialists on how the retention and disposition specifications can be applied.

If a retention and disposition schedule is not in place:

- Insert the following phrase into the profiles for all folders in the shared directory:

"Retain until the establishment of approved retention and disposition schedules"

- Ensure that this specification is applied to the e-mail messages stored in the related public folders (if these are being used for the storage of corporate memory e-mail messages).

- Consult with records specialists to determine when a retention and disposition schedule can be established.

5. Governance

A coordinator should be named in each organizational unit to be responsible for the following:

- Facilitating understanding and use of the criteria for determining what electronic documents and e-mails should be designated corporate memory and non-corporate memory.
- Facilitating understanding of the folder structure and serving as a point of contact for the creation of new folders, for their respective organizational unit at the first two levels of the new shared directory (in cooperation with records management specialists).
- Ensuring the integrity of the revised S: drive structure and the use of the appropriate shared drive folders for the activities of their organizational unit.
- Ensuring the integrity of the relevant public folders (if these are being used for the filing of corporate memory e-mail messages) and ensuring that linkages between the public folders and related folders on the 'S' drive are maintained; and,
- Co-ordinating the occasional removal of Non-Corporate Memory (NCM) records based on consultation with records management specialists.

Staffs of the public office who want to create a new folder within any one of the two top levels of the directory structure should consult with the coordinator. The steps involved in creating a new folder within the existing two level folder structures are as follows:

- Determine the name and location of the proposed new folder in the directory tree for the 'S' drive.
- Complete an information profile for the proposed folder, indicating the names of sub-folders which you propose to place under it.
- Forward the completed information profile to the coordinator; (the coordinator will consult with the records management office and ensure that the profile information conforms with the rules for establishing new folders at the first two levels of the directory).
- Once the folder appears on the new shared directory add relevant sub-folders in accordance with the guidance described above.

SECTION 4

Core Requirements for an Electronic Document and Records Management System (EDRMS)[8]

1. Introduction

An EDRMS provides the most effective means for storing and retrieving electronic records in the 'unstructured' environment. A properly designed and implemented EDRMS provides:

- A trustworthy environment for the management of the authenticity and reliability of the records required for decision-making, programme delivery, and accountability (excluding records classified 'secret' or 'top secret');
- The ability to comply with government ordinances, policies and guidelines;
- The ability to exploit information to serve purposes beyond those for which the information was originally created;
- The achievement of cost savings through the reduction in the time required to search for records, the freeing up of space for storing records, and the economies of scale that can be achieved in sharing records management systems and facilities; and
- The ability of Departments to maintain their corporate memory and to contribute to the wider archival memory of Malaysia.

Properly implemented, an EDRMS will permit records creators to file and retrieve electronic records and other forms of records to and from a trusted environment that meets records management policies and practices.

Section II presents a set of core functional requirements for an EDRMS. The National Archives is using these requirements as the basis for more detailed requirements that are being used to test the capabilities of existing technologies. The gained experience together with a review of factors such as the availability of resources, the availability of expertise and technical solutions, and the identification of high priority areas warranting EDRMS deployment, will lead to decisions concerning the procurement strategies that should be employed for the acquisition and development of EDRMS across the Government.

For those public offices that have implemented electronic document management systems (EDMS), these requirements may be useful in determining the extent to which their systems reflect the attributes of an EDRMS.

[8] The functional and management requirements described In this section were based on similar requirements developed for the Government of Hong Kong by the Government Records Service, 2003. The functional requirements produced for the Government of Hong Kong were based on related requirements developed for the Government of Canada, the UK Government and the US Department of Defense.

In addition to meeting the functional requirements described below, Departments must establish a management framework that reflects assigned accountability (i.e. to program managers, records managers, IT specialists, etc.) for the integrity and sustainability of the EDRMS through time as well as the records being managed through the use of the EDRMS. An elaboration of the management requirements for an EDRMS is described in Section III.

Departments should contact the Arkib Negara Malaysia before undertaking an assessment of their EDMS or any other application that has the potential to meet the requirements described in the following two sections.

2. Core Functional Requirements

The core functional requirements have been organized according to the broad categories of recordkeeping functions normally supported by public offices. Public offices may choose to augment these requirements in order to secure capabilities beyond those needed to meet their core recordkeeping requirements.

Capture

These requirements address the capability of the system to be able to capture records. They address activities such as collect, receive, create, generate, etc.

The system shall have the capability to:

- Permit users to create new records or edit existing documents (provided that the documents are not finalized) within an authoring application.
- Prompt the user for metadata at the time of creating a record and a new version of a document (provided that the document is not finalized)
- Associate core metadata automatically to the content of an electronic record (including e-mail and attachments, word processing, spreadsheets, images, audio) or to reference, within metadata, non-electronic records (including paper files, microfilm, reports, video, photographs).
- Provide the user with the option to create a new version, replace the existing version (provided the document has not been finalized) or create a new record.
- Automatically link new versions to the original record and earlier or later versions of the record.
- Electronically designate a document as being finalized (authorized by a named authority) thereby protecting the document from modification.
- Attach/link multiple electronic documents to form a single ‘virtual document’ which is subsequently managed as a single entity to ensure its integrity.
- Profile an original hardcopy record.
- Launch the authoring applications (i.e. including associated or generic viewers) from within the retrieval function of EDRMS for the purpose of creating or viewing a record and editing a document (provided that the document is not finalized).
- Permit an authorized individual to apply common metadata values and load records and documents into the repository in bulk (e.g. loading by sub-directory).

Organization

These requirements address the logical structuring of stored documents and associated information (naming, profiling and describing) and the management of the filing and file handling process

The system shall have the capability to:

- Organize and classify both electronic and non-electronic information within a structured subject file classification hierarchy based on function and subject.
- Support pre-defined file classification schemes in a hierarchical structure with at least 4 levels.
- Classify electronic and non-electronic records and capture file titles and numbers in a hierarchical structure with full file number validation.
- Permit authorized individuals to add, modify and delete file numbers/titles both as a single set and globally; includes prompts to confirm the action and messages if the action will affect other levels in the hierarchy or other related records.
- Transfer the file classification scheme and all associated data from a local EDRMS site to a central file classification database.
- Build, maintain and manage the metadata associated with both individual records and the EDRMS users.
- Provide users with the option of filing a document in a selected records or document repository or filing it in the user's work space (outside the EDRMS environment).
- Provide users with the metadata schema, on the profiling screen, that matches the selected repository.
- Cross-reference a record to more than one file number.
- Permit users to file documents directly into the EDRMS or to designate the document as a ‘file-and-send’ for filing by a designated individual.
- File by user activation through a specific action (User Decided Filing) or by forced activation where the filing process is automatically initiated upon receipt or sending of a message (Forced Filing).
- Permit users to select for filing the message currently being viewed in the e-mail client and a message from an e-mail client message list and/or message folder.
- Automatically capture key data elements from the e-mail message and populate the metadata for the e-mail message copy that is to be filed as an EDRMS record.
- Capture resolved distribution lists (i.e., the full e-mail address of the actual recipient), including cc lists in addition to the distribution list name itself.
- Automatically capture e-mail message attachments (sent and received) and enable the attachments to always be relatable to the e-mail message to which they were attached.
- Record the full document name of the e-mail attachment in addition to the system generated name.

Use

These requirements address the retrieval of records by end users (based on pre-established indices) and the ultimate use of the records (viewing, editing, printing, etc).

The system shall have the capability to:

- Permit users to perform requests and retrieve records in an intuitive manner from one or more selected repositories that may contain electronic and related non-electronic records.
- Conduct full text searches on one or a combination of any of the metadata fields (including text descriptions) and on the contents of records.
- Retrieve electronic records and associated attachments from any records repository managed by EDRMS informing the user of the location of the records (e.g. online, offline, etc.).
- Retrieve non-electronic records (e.g. through automatic notification to registry staff) from any records repository managed by EDRMS informing the user of the location of the records, the time by which the user can expect to receive the non-electronic records, etc.
- Permit EDRMS-filed documents from an EDRMS repository to be forwarded to the user as attachments to an e-mail message.
- View electronic records without launching the native or originating application;
- Select and retrieve one or more records from attached/linked multiple electronic records (a single ‘virtual record’).
- Ensure that the default retrieval strategy shall always retrieve only the most recent version of a record.
- Retrieve any or all earlier versions of an electronic record as requested by the user.
- Permit users to check-in and check-out electronic records and to prevent other users from modifying checked-out records while permitting such users to view the records.
- Permit users to charge-in, reserve and charge-out paper records, volumes and records stored in secondary storage containers.
- Perform automatic calculation of recall dates for charge-outs with the ability to override.
- Bring forward files, volumes, enclosures, and/or documents to be sent to users on a specified date.

Storage

These requirements address the physical storage of records in an EDRMS. The objective is to ensure that records, regardless of their physical form, remain authentic, available, understandable and usable for the length of time they are required for business and accountability purposes.

The system shall have the capability to:

- Store and protect records, record indices, record metadata, other associated metadata and all other information required to manage records (regardless of their physical form) in the EDRMS. The storage facility must be flexible, expandable and scalable.
- Support multiple repositories in multiple physical locations for the storage of records, attachments and record metadata (i.e. as distinct from a centralized repository).
- Support replicated repositories (i.e. duplicates of a repository that can be distributed to different geographical locations).
- Permit immediate access to records, attachments and associated record metadata and record indices in:
  - Active (daily/constant) functional use (active-online).
  - Secondary storage for documents and attachments that are no longer in constant use but may be required from time to time (active-offline).
  - Secondary storage for inactive documents and attachments that are no longer in constant use but may be required at some future time (inactive).
- Replicate vital records onto other storage media for off-site transfer and storage.
- Retain records in their native or originating format and software version.
- Update the record metadata to reflect the new software version when a record has been saved to a new version.

Security

These requirements address the protection of electronic records from inadvertent or unauthorized alteration, deletion, access, and retrieval. They also address the management of security-classified records.

The system shall have the capability to:

- Provide proper management of user ID and password information.
- Provide an individual profile for each EDRMS user and a facility for managing ‘permissions’ associated with read, write, modify, delete, and disposal rights and restricting those permissions to designated individuals.
- Control all permissions at the level of the individual, work group, or organization as well as at the record and file classification levels.
- Permit individual profiles to inherit some characteristics of parent organization/group profiles.
- Provide a self-contained security system designed to protect the integrity of records within the EDRMS environment throughout each stage of their life cycle.
- Provide an audit log showing changes made to the security parameters.

- Store in a retrievable manner PKI-based signed and encrypted e-mail and documents.

Retention and Disposal

These requirements address the length of time records are to be retained in an EDRMS and their ultimate disposal based on the specifications described in approved retention and disposal schedules.

The system shall have the capability to:

- Permit an authorized individual to create, maintain, modify and manage retention and disposal schedules indicating the period of time records (regardless of their physical form) are to be retained in an active and inactive state.
- Permit an authorized individual to create, maintain, modify and manage a listing with instructions for the authorized disposition of records (regardless of their physical form) such as destruction, transfer to another government institutions (such as the Arkib Negara Malaysia), or transfer outside government.
- Link the retention periods and disposal actions for records, through the file classification scheme, to the metadata of any record or file.
- Permit an authorized individual to change defaulted retention and disposal designations for individual records and files at any level of the file classification scheme in order to support retention and disposal exceptions.
- Provide assistance and the ability to change record status between active, inactive and archival storage.
- Permit an authorized individual to capture and manage information including record metadata for bulk secondary storage (e.g. boxes, digital media and canisters).
- Permit an authorized individual to identify all records due for destruction according to their authorized disposal schedules.
- Permit an authorized individual to delete records (including e-mail messages and their attachments) from all repository media (including removable media) such that the records cannot be reconstructed.

Auditing and Reporting

These requirements address the activities involved in monitoring the integrity of the EDRMS through time and for providing management information to those responsible for administering the EDRMS.

The system shall have the capability to:

- Maintain charge in/out history for files, volumes, records and secondary storage containers.
- Compile statistics and produce management information.
- Maintain a Document Activity Log/Audit Trail that records and provides information on all information transactions (e.g. access, retrieval, filing, disposal, etc.).

- Maintain and provide reports on revisions to documents, access to documents, and changes to document status.

3. Management Requirements

Problem Definition

- Has the electronic recordkeeping ‘problem’ been defined effectively and has the ownership of the problem been clearly identified?
- Is the problem expressed in terms of the impact electronic recordkeeping is having on the ability of the public office to meet its programme/service delivery and accountability requirements (i.e. is the problem defined clearly within the context of the business of the public office)?
- Does senior management understand the problem and is it prepared to support efforts to find solutions?

Cost-Benefit Analysis

- Has a cost-benefit analysis been performed to substantiate the rationale for acquiring an EDRMS
- Have the benefits of an EDRMS been weighed against the costs to the public office re: technology requirements, financial resources, impact on users, etc.?
- Have the benefits been addressed in terms of risk reduction (i.e. the key factor often used to determine the need for an EDRMS) in addition to cost avoidance, cost savings, and opportunity gain?

Project Initiation

- Has a project charter been established that clearly assigns accountability for the EDRMS among those who will be responsible for its implementation within the public office (e.g. records registry staff, IT specialists, program managers and officers, legal services, etc.)?
- Have approval processes and mechanisms been established to guide the approval of the EDRMS project, its deliverables, and the policies, standards and practices, and technologies that will comprise the supporting infrastructure?
- Has a strong project management framework been established for the design, implementation, and assessment of the EDRMS?
- Has a communication plan been established to ensure that the purpose, benefits, costs, and steps involved in undertaking the EDRMS initiative are understood by all of those involved including, most importantly, the users of the system?

Requirements

- Have user driven functional requirements for electronic recordkeeping been developed?
- Have the business rules and procedures been developed to cover topics such as what gets filed and when, who is responsible for the integrity of the records system, etc.?
- Have the technology requirements been confirmed re: inter-operability, performance, reliability, security, etc.?
- Have the human resource requirements been identified and the capacity of resources such as records management staff, IT specialists, etc. (for which electronic recordkeeping may be quite new) been assessed?
- Have the requirements for facilities such as off-site storage, 'archiving' facilities, etc. been expressed?
- Have funding and procurement strategies been established that are appropriate in terms of the objectives of an EDRMS, the availability of the technologies, and the procurement objectives of the Government of Malaysia?

Design

- Have data and process models of the system been designed that account for the recordkeeping realities (e.g. centralized, decentralized, etc.), specifications (e.g. classification schemes, retention and disposition, etc.), and objectives of the public office?
- Has the system been designed to account for the evolution of the technology platform of the organization and its evolving organizational culture (re: user readiness for an EDRMS)?
- Have performance measures been established to ensure that the EDRMS meets the specified requirements and that it is able to do so through time?

Implementation

- Have awareness and training requirements been identified and relevant programmes established to facilitate user acceptance of an EDRMS?
- Has a comprehensive site readiness study been undertaken to account for the way people work, existing records management practices, existing technology platforms, potential areas for re-engineering, etc.?
- Has a comprehensive site readiness study been undertaken to account for the way people work, existing records management practices, existing technology platforms, potential areas for re-engineering, etc.?
- Within the context of the site readiness study, has an understanding been gained of how information is created, used, and preserved (This will consume the greatest amount of effort outside the effort to develop the functional requirements)?
- Has a migration strategy been established to migrate from a paper-based to a mixed paper-electronic based recordkeeping environment?

- Has a prototype been developed to test the EDRMS requirements in a ‘live’ area of the public office and has an acceptance test been conducted to confirm that the system is ‘EDRMS compliant’?

Maintenance

- Have mechanisms been established to ensure system compliance with the requirements through time and has a change management procedure been established?
- Is a mechanism in place that accounts for the impact on recordkeeping (and supporting systems) of changes to the organizational structures and the functions of the public office through time?
- Is a mechanism in place for monitoring the security of the system and the integrity of the records?
- Have processes been established for managing system upgrades and for managing the migration of electronic records to account for changes to the technology upon which the records may be dependent?
- Have processes been established for anticipating emerging gaps in areas such as the recordkeeping rules supporting the EDRMS, the knowledge and skills required by the human resources specialists managing the system, etc.?

Review and Evaluation (Quality Assurance)

- Have performance standards and other evaluation criteria been established to ensure that the EDRMS meets the specified requirements?
- Have mechanisms been established to audit and evaluate over time the quality and integrity of the system and especially the records generated through the use of the system?
- Have strategies for conducting audits and evaluations of the capability, availability, reliability, and survivability of the EDRMS been established (e.g. should separate recordkeeping audits be conducted or should this be accomplished by reflecting recordkeeping considerations in the systems audit process? Or both?)?
- Have the roles and responsibilities of those involved in the design, testing, implementation, and evaluation of the EDRMS been clearly defined (e.g. records registry staff, audit and evaluation, etc.)?