Information
Management

Managing Shared Electronic Workspace

(Non-EIM Environment)

Business Rules

December 2005

Alberta
Government

Produced by:

Information Management Branch
Government and Program Support Services
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web Site:
www.im.gov.ab.ca

ISBN 0-7785-3689-0

Contents

1. Introduction

Everyday, staff create and manage electronic information to support their work. In fact, it is estimated that 92% of all new information is stored on network servers. The network servers storing this information are divided up into what is commonly called "shared drives" or "common drives."[1] In addition, some servers may also permit staff to store electronic information on a "personal" or "individual" drive which is accessible only to the individual. Managing all of this information efficiently and effectively can greatly improve business performance.

About this guide

This guide is intended for information management professionals within ministries who are charged with improving productivity through improved management of electronic information.

Most organizations today find themselves in transition. That is, most information is created electronically, yet recordkeeping systems are largely paper-based.

The solution lies in implementing Electronic Information Management (EIM). In an EIM environment, information can be managed to meet both work productivity and the ministry's recordkeeping requirements. If your ministry is beginning to implement EIM, you should consult Implementing Electronic Information Management: A Planning Guide.

If your ministry is not preparing to implement EIM in the near future, this guide can provide assistance in establishing business rules to improve the management of electronic workspace. These business rules can begin to establish discipline and common practices related to the creation, storage, use, and maintenance of electronic information. However, without EIM, shared drives do not provide a means to meet government recordkeeping requirements. Thus, the advice provided in this guide is meant only to support more efficient work practices. Ministries will still need to capture information on shared drives into their recordkeeping systems, as required by the Records Management Regulation.

The focus of this guide, then, is on managing electronic workspace on shared drives for the storage, use, and protection of common office documents (including spreadsheets and presentations.) It is not meant to cover the management of web sites or electronic mail, which are covered in other guides that are available at www.im.gov.ab.ca.

[1] Throughout this guide, the term "shared drive" is used to refer to this common electronic workspace.

Purpose

In most organizations there are few rules to guide employees on how to effectively manage electronic information on network drives. As a result, several issues emerge which impede business performance and reduce productivity. These issues include:

- information stored on personal drives that is not accessible to those who need it when the individual is ill or away from the office;
- the need to e-mail attachments of files to workgroups because not all people in the workgroup have access to the same part of the shared drive;
- duplication of files when the same file is stored in different locations under different names (often as a result of sending the same file to multiple e-mail recipients);
- increase in the number of directories and sub-directories created by employees without any guidance on optimal structure and organization of the information;
- difficulty knowing what is the appropriate version of a document as a result of the lack of naming standards and version control;
- information being "orphaned" when it is stored in an individual drive and the individual leaves the organization or changes jobs without passing control of the information on to someone else; and
- the need to protect personal and sensitive information.

All of these issues lead to increased costs for the organization (e.g., increased storage and backup costs for the servers) and increased frustration for staff.

Establishing effective business rules around managing this electronic workspace can increase efficiency and support collaboration. Specifically, clear business rules around managing shared electronic workspace can:

- reduce the duplication that occurs when multiple people store the same file in multiple locations on the ministry's servers;
- increase access to information by ensuring all information related to the business of the ministry is stored in an accessible location where all who need to get access to it can access it;
- improve the maintenance of corporate memory by ensuring that responsibility for information content is transferred when an individual responsible leaves the organization (thus reducing the amount of "orphaned" information); and
- facilitate the protection of personal and sensitive information.

Guiding principles

To improve business performance, ministries should establish clear guiding principles on the management of shared electronic workspace. These principles will establish a foundation on which to manage shared electronic workspace on an ongoing basis. Principles that have been adopted in several organizations include:

1. All electronic office files (e.g., Word, PowerPoint, Excel) that are related to the business of [ministry name] will be stored on the shared drive.
2. The shared drive will become the common workplace for all staff. The default is that folders will be "open" to all staff, unless specifically restricted. If functional areas determine a need to restrict access to the entire folder, the reasons for the restriction should be documented. Individual documents stored in "open" folders can be protected as "read-only" if necessary.
3. Individual drives and "My Documents" are to be used for an employee's own personal (private) files only (i.e., information that does not pertain to the business of the ministry). Individual drives and "My Documents" should NOT be used for information that others may need to access if you are away from the office.

Getting started

Effectively implementing improved management of electronic information on shared drives will require significant planning and the implementation of a number of prerequisites. The plan should include:

- **File Management:** Protocols should be developed for the naming of files, version control, and document labelling.
- **Classification Structure:** While the shared drive is not a recordkeeping system, it can facilitate recordkeeping by being structured similarly to the ministry's recordkeeping system. Structuring the shared drive by business function (often called a functional approach) is consistent with the direction of Government of Alberta (GoA) records management and can also avoid problems related to using organizational names (i.e., Division Name or Branch Name), especially when the ministry undergoes re-organization.
- **Metadata:** If you are able to capture document-level metadata on the shared drive, an approach and metadata elements will need to be defined.

- **Security Strategy:** Access rights on the shared drive will be driven by your security strategy and security classification for personal and sensitive information.
- **Responsibilities and Stewardship:** Clearly articulated roles and responsibilities for information (i.e., staff know what they are responsible for managing and know how to do it) and processes to transfer stewardship when employees change positions or leave the organization will be needed.
- **Business Rules:** Business rules codify the common practices you are trying to achieve in the shared electronic workspace.
- **User Guidance and Training:** Because employees have been left to organize their own electronic workspace for so long, there will be considerable guidance and training needed, in addition to change management, to ensure staff understand what is expected of them.

In the next section of the guide, a core set of business rules is presented for the management of electronic information on shared drives.

2.
Business Rules for Managing Information on Shared Drives

Business rules are a synthesis of an organization's policies, directives and standards for managing information in support of its business functions. They provide a basis for developing the methods and practices for managing information within the workgroup and by the individual. Business rules provide clear direction for consistent practices for managing information throughout the organization and establish roles and responsibilities.

Information life cycle elements

These draft business rules are organized into four categories that follow the information life cycle:

- creation, collection and receipt
- organization, use and retrieval
- storage and protection
- retention and disposition

Throughout the remainder of the guide, the term "file" is used to refer to content stored on shared drives, whether it is a traditional document or another type of information content such as a spreadsheet, presentation, photograph or graphic image.

Responsibilities

Business rules help to establish roles and responsibilities. The responsibilities outlined in this document are consistent with the roles and responsibilities defined in Accountability for Information Management: A Model. Namely, four roles have been used in the business rules. These are:

- **Controllers**[2] are ultimately responsible for the information to support their business objectives. Controllers are often the business managers, although specific responsibilities of the Controller might be assigned to workgroups or to individuals.

[2] In some organizations, the Controller is referred to as the information owner. The term owner has not been used here because information is not owned by individual employees – it is owned by the government. It is a Crown asset.

- **Stewards** create, collect, receive information to support business activities. Stewards also update, edit, ensure the accuracy of information and manage its use and disclosure. Finally, stewards ensure appropriate categorization of information to support sharing, future reference and reuse. Stewards are usually individual employees or workgroups.
- **Administrators** design, implement and maintain the environment in which information is organized and stored. Examples of administrators are records management personnel, network administrators, Internet and intranet administrators, and library professionals.
- **Users** need information to make decisions or complete tasks. While users may be internal or external to the ministry (the public, clients and stakeholders), the focus in this document is on the roles and responsibilities of internal users.

NOTE: These responsibilities are not mutually exclusive. That is to say, a single individual may have more than one of these responsibilities in relation to any particular file. For example, say you have created a spreadsheet for your own use. In this case, you will fulfill most of the roles identified above. You are likely the **user** (making decisions from the information), the **controller** (you define the information needed), and the **steward** (you create and update the information). In this case, the **administrator** role is shared by records management and information technology (IT) systems (they helped you define the folder and classification structure that helps you know how to name the spreadsheet and where to file the spreadsheet as well as maintain the servers on which the spreadsheet resides).

More examples of how these roles and responsibilities are applied can be found in Accountability for Information Management: A Model.

Creation, collection and receipt

In a shared drive environment, most files will be created electronically or, in some cases, scanned into an electronic format from hard copy. Employees may also collect information (e.g., download files from Internet sites) or receive information (e.g., attachments through e-mail).

1. Business-related information

The shared drive is a place to organize, find, and maintain the ministry's information to support its work. This information needs to be accessible to all who need it, regardless of whether the author or creator is available or not.

Business Rule: All electronic documents (files) that pertain to the ministry's business will be maintained on the shared drive (and not individual drives or in "My Documents").

Responsibility: Stewards

2. Non business-related content

Employees often keep information that is not business-related, but is of a purely personal nature.

Business Rule: Information that is of a purely personal nature should be maintained in "My Documents" or an individual (private) drive.

Responsibility: Steward

3. Authoring or creating files

Responsibility for managing files rests with the author or designated individual.

Business Rule: The author/or designate will be responsible for:

- **managing the file on the shared drive;**
- **ensuring the file is integrated into the ministry's recordkeeping system; and**
- **setting and removing access restrictions (in consultation with IT Administrators).**

Co-authors will have full access and editing rights to the file, and share responsibilities for:

- **creating new versions as appropriate; and**
- **deleting the file if declared a transitory record.**

Responsibility: Steward

4. Draft files

Drafts of electronic files created in the conduct of official ministry business should be managed on the shared drive. More than one individual can author or contribute to a draft file.

Business Rule: Draft files should be managed on the shared drive.

Responsibility: Steward

5. Naming electronic files

Standard formats for naming files can:

- facilitate better access to and retrieval of electronic files;
- allow sorting of files in logical sequence (e.g., version #, date); and
- support the ability to recognize the content of a file from a list.

Business Rule: The following naming standard is recommended for all files managed on the shared drive:

Title_version_date.ext

The subject is the title of the file. The version is the version number (e.g., v01, v02, v03). The date is the date the file is created or updated and should be in the international date standard (YYYY-MM-DD). The extension identifies the program in which the file was created (e.g., Word, Excel, PowerPoint, etc.).

Responsibility: Steward

Note: Further guidance can be found in Naming Conventions for Electronic Documents. Also, business units may want to establish additional naming standards, especially in cases where the folder structure on the shared drive does not provide sufficient information to easily find information.

6. Profiling files – metadata

[Ed. Note: This business rule would only apply in those ministries that have adopted common metadata standards and have a system to manage metadata.]

Metadata can make information significantly easier to find and to manage over the long-term.

Business Rule: The following metadata elements must be included when files are created and saved on the shared drive:

- **title,**
- **author,**
- **subject,**
- **description,**
- **date created, and**
- **security classification (if protection is necessary).**

Note: A metadata standard for the GoA is currently under development that will guide ministries on this business rule.

Responsibility: Steward, with assistance from Administrators

7. Versions of files

Many files undergo revisions through their creation. Standards around versioning of files can make them easier to manage and help users find the "right" version they are looking for.

Business Rule: Versions of electronic files are to be identified and managed on the shared drive.

Note: There is no limit on the number of versions that can be created. The author can delete unneeded versions of an electronic file if the record is transitory. For guidance on when versions should be maintained as official records, refer to Official and Transitory Records: A Guide for Government of Alberta Employees.

Responsibility: Steward

8. Collaborative authoring

Where files are created by multiple authors, clearly designating responsibility for managing these files is needed.

Business Rule: For files authored collaboratively, i.e., by two or more people, one person will be assigned the responsibility for:

- **managing the file on the shared drive;**
- **ensuring the file is integrated into the ministry's recordkeeping system; and**
- **setting and removing access restrictions (in consultation with IT Administrators).**

Co-authors will have full access and editing rights to the file, and share responsibilities for:

- **creating new versions as appropriate; and**
- **deleting the file if declared a transitory record.**

Responsibility: Steward, IT Administrators

9. Date functions

Many dates relate to a file throughout its life cycle: creation date, date last modified, date printed. Standard practices around the date function can reduce uncertainty when accessing and using electronic files.

Business Rule: Date functions (e.g., automatic dating feature in MS Office) should not be used in electronic files. Dates should be in standard text format, following the international date standard of YYYY-MM-DD. The date of creation (or new version) should be in the file name. Other dates may be captured by the system or captured by metadata.

Responsibility: Steward

10. Dynamic links

A file containing dynamic links to other files can be managed on the shared drive, but there is no guarantee that the linked file will be the same upon each use, particularly if control of the linked file rests with another workgroup or with someone outside the ministry.

Business Rule: It is the responsibility of the person who makes a decision based on a file containing dynamic links, to manage a copy of the complete file (e.g., original file and information contained in the linked file) on the shared drive as it existed at the time the decision was made.

Responsibility: Steward

11. Receipt of information by numerous people

Often, documents are received by more than one person in the ministry at the same time. Responsibility should be established so that these documents are managed once.

Business Rule: If a document is received by more than one individual in the ministry, the first name on the distribution list (e.g., e-mail transmittal, distribution list) will be responsible for managing the document in electronic workspace.

Responsibility: Steward

Organization, use and retrieval

Shared drive folder structures should be intuitive. Your ministry's records management personnel can provide guidance on folder structure that is consistent with a functional classification of information. This will facilitate access and later integration of files into the ministry's recordkeeping system.

12. Folder structure

Active management of the folder structure on the shared drive will help ensure information is accessible across the ministry, while adequately protecting personal and other sensitive information (i.e., restricting certain folders to workgroups or functions).

Business Rule: Level 1 (directories) will be managed by a departmental team, co-led by [insert appropriate coordinating group name here]. The team will also monitor the evolution of other levels. It is recommended that functional business areas establish a small team to coordinate and manage levels 2 and 3 of the folder structure. This will facilitate common approaches. Levels 4 and beyond will be managed by branches and individuals within those branches.

Responsibility: Administrator (Level 1), Controllers (Level 2-3),
Steward (Level 4)

13. Information access

One of the objectives of shared electronic workspace is to improve access to information assets and encourage the leveraging of the value of these assets as well as the protection of personal and sensitive information.

Business Rule: Files managed on the shared drive will be, by default, shareable and accessible to any ministry employee. The Controller, a delegate or the Administrator is responsible for ensuring items that must have restricted access are adequately protected (based on security classification). This may include limiting access to specific workgroups or specific users. *(See Business Rule 16: Access Restrictions)*

Responsibility: Controller, Administrator, Steward

NOTE: The GoA Information Security Classification Guide identifies types of sensitive information, including personal information, that need protection and practices related to controlled access to the information.

14. Linking to files

A common practice today is to e-mail a file to multiple people. This practice not only requires all recipients to manage the file, but increases costs by increasing duplicate information on the shared drive. Placing files in shared electronic workspace can reduce the amount of unnecessary duplication of files.

Business Rule: When distributing a file to individuals within the ministry, where possible, insert a link to the file in the e-mail rather than attaching the file to the e-mail.

Responsibility: Steward

NOTE: This is only practical where all individuals on the distribution list have access to the location of the linked file.

15. Modifying files

An open shared drive environment promotes access. At the same time, all staff should have the expectation that files will only be altered by authors or members of a workgroup involved with the file.

Business Rule: A file managed on the shared drive may be modified by the original author of the file (steward) or delegate. Other users attempting to modify a draft file not authored by them will be required to save it as a new file. Exception: When a draft electronic file is authored collaboratively, i.e., by two or more people, the users granted co-authoring rights will be permitted to modify the file. *(See Business Rule 8: Collaborative Authoring)*

Responsibility: Administrator

Storage and protection

Appropriate practices for storage and protection will be applied to ensure the integrity of recorded information. This includes the continued readability of electronic information. Special measures will be taken for the security of confidential and restricted information, which will be reflected in recordkeeping procedures.

16. Access restrictions

Certain information will require protection, based on its security classification.

Business Rule: Controllers (in consultation with IT Administrators) can establish access restrictions to folders on the shared drive. Access can be restricted to individuals or to groups.

Responsibility: Controller/IT Administrator

17. Transferring access rights to different users

To accommodate reorganization and personnel changes, transferring rights for files will be necessary.

Business Rule: The IT Administrator may, at the direction of the workgroup manager, transfer access rights to folders to another workgroup or other users.

Responsibility: IT Administrator/Controller

Retention and disposition

Records retention and disposition schedules developed by individual ministries and approved by the Alberta Records Management Committee (ARMC) govern the retention and disposition of all records. These schedules set out designated retention periods to ensure that records are maintained and protected for as long as they are needed (for their operational, fiscal and/or legal value and in accordance with privacy requirements). The schedules will also identify records deemed to have archival value and, as such, are subject to transfer to the Provincial Archives of Alberta at the end of their retention period. Related procedures and directives for scheduling and disposition will be maintained.

18. Managing official records

Retention periods are established in records retention and disposition schedules approved by the Alberta Records Management Committee (ARMC).

Business Rule: All records on the shared drive must be managed according to their retention requirements and integrated into the ministry's recordkeeping system. Once a document has been integrated into the ministry's recordkeeping system, a note should be added to the electronic document identifying the date the document was filed into the ministry's recordkeeping system (e.g., in properties, or as part of the header or footer of the document).

Note: Without Electronic Information Management (EIM), this will usually mean producing a paper copy and integrating the record into the paper-based recordkeeping system. The shared drive is NOT a recordkeeping system.

Responsibility: Steward/Senior Records Officer

19. Transitory records

Effectively managing transitory records can improve operational efficiency of the shared drive and reduce risk to the ministry associated with keeping unnecessary information.

Business Rule: Files managed on the shared drive that are transitory in nature should be deleted when they are no longer needed for business purposes. Duplicate files (e.g., duplicates of records that have already been integrated into the ministry's recordkeeping system) may continue to be managed on the shared drive as long as they are needed to support work.

Responsibility: Steward

3.
Conclusion

Electronic Information Management (EIM) provides a way for ministries to integrate and manage both recordkeeping and work functions. However, for ministries that have not implemented EIM, improved management of the shared electronic workspace can still improve productivity and reduce costs.

The shared drive is not a recordkeeping system, but rather, is a work environment. This guide proposes some basic business rules to effectively manage information in this work environment to support the business. These business rules can be used in conjunction with other recordkeeping procedures established within the ministry.

These business rules will be supplemented by additional business rules that will need to be developed when implementing EIM. In the interim, they can be used in a shared drive environment to begin developing discipline and consistent practices for managing electronic information across the ministry.