PROVINCIAL ARCHIVES OF SASKATCHEWAN

Information Management Services

Guidance for Managing Electronic Records in Shared Drives

Effective Date: December 11, 2018

This page intentionally left blank

Table of Contents

Introduction 4

1. Establishing Structured Shared Drives 5
    1.1 Identify the Stakeholders Involved 5
    1.2 Determine the Scope of Work 6
    1.3 Establish the Drive Structure 6
    1.4 Develop Naming Conventions 11
    1.5 Implementation of the Drive Structure 11

2. Policy and Procedures for Structured Shared Drives 12
    2.1 Roles and Responsibilities 12
    2.2 Explanation of Drive Structure 12
    2.3 Use of Personal Drives 13
    2.4 Shared Drive Auditing and Compliance 13
    2.5 Inventory of Records in the Shared Drive Structure 13
    2.6 Transferring Records From the Active Folder to the Retention Folder 14
    2.7 (Year-End) File Maintenance 14
    2.8 Disposal of Records 14
    2.9 Other Repositories (SharePoint, etc.) 15
    2.10 File Formats and Migration 15

Appendices

Appendix A – Tools to Assist the Transfer to a New Drive Structure 16

Appendix B – Shared Drive Roles and Responsibilities 17

Appendix C – Certificate of Destruction – Electronic Records 19

Introduction:

Shared drives, which may also be referred to as network drives, are network storage locations that are accessible to defined groups of users. Shared drives are made up of folders where electronic records, such as Word documents, Excel spreadsheets, digital photographs, PDF documents, audio files, video files, etc. are stored and accessed.

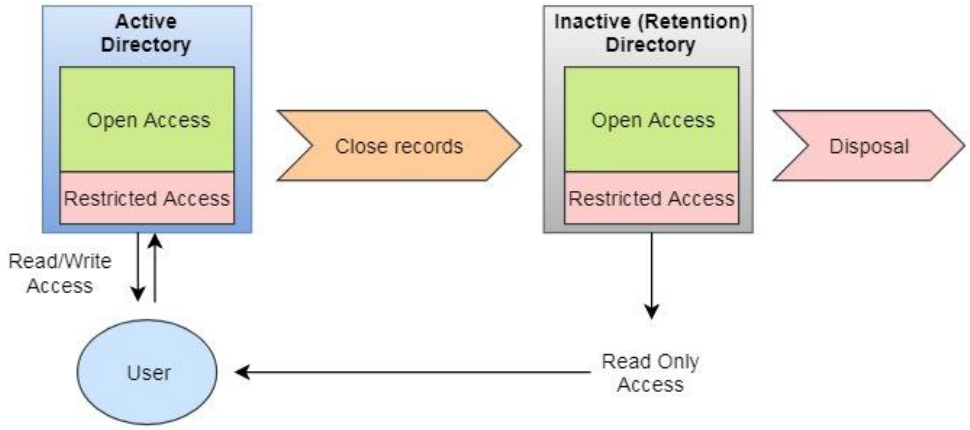
The management of shared drives presents a number of challenges:

- Unlike an EDRMS (a software application designed to manage digital information), shared drives have no automated recordkeeping functionality, such as auditing controls, security controls, the ability to easily add metadata to records, or the ability to track the retention and disposal of records. This means that an ongoing, manual effort by the institution will be required to manage the records in its shared drives.
- The lack of auditing controls, security controls and metadata can make it difficult for the institution to demonstrate the authenticity and integrity[1] of its electronic records, which is necessary if the records are to serve as evidence in legal proceedings.
- Shared drives that have no imposed structure and no rules regarding the creation or naming of folders or documents may be poorly organized, and employees may have difficulty locating and retrieving needed information.

This document provides guidance on the development and management of structured shared drives. *The Archives and Public Records Management Act* requires that government institutions utilize records schedules for the classification and disposal of government records. Therefore, the Provincial Archives proposes that government institutions base the structure of their shared drives on the approved records schedule(s) applicable to them. The structure will take into account the need to apply access controls to records that contain personal, sensitive or confidential information. The folder structure will then be replicated as a set of read-only folders into which closed records will be moved to wait out their required retention periods so that they can then be disposed of through the Provincial Archives' disposition procedure for government records. Policy and procedures will be developed to accompany the new drive structure in order to ensure that it is properly managed, used, and maintained by the institution's staff.

[1] Authenticity – an authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have sent it, and to have been created or sent at the time purported.

Integrity – the integrity of a record refers to it being complete and unaltered. *The Evidence Act* states that where the best evidence rule applies to electronic records it is satisfied by proof of the integrity of the system that recorded and/or stored the record. Therefore, it is necessary to demonstrate that the system operates properly and that measures are in place to prevent accidental or deliberate alteration to documents recorded by and/or stored in it.



The implementation of a structured shared drive, with dedicated folders for retention and procedures for its management, is intended to:

- make records easier to locate, identify, and retrieve throughout their lifecycle and reduce the risk of important information being lost;
- control the growth of shared drives and help reduce unnecessary duplication of records;
- help safeguard sensitive records, including those which contain personal information, through the use of access controls;
- allow the institution to demonstrate the authenticity and integrity of its electronic records in the event they are required to produce the records as evidence;
- facilitate disposal of records in accordance with *The Archives and Public Records Management Act.*

Institutions must keep in mind that these benefits will only be gained if a dedicated, ongoing effort is made to monitor and maintain the drive structure, and to train staff to use it according to the procedures set out by the institution.

1. Establishing Structured Shared Drives

1.1 Identify the Stakeholders Involved

The development, implementation and maintenance of an institution's shared drives will require the expertise of and cooperation from a number of different groups:

- Senior management for an institution-wide project, or branch level management for a project limited to a certain branch. Support of management is necessary to ensure the allocation of adequate time and resources for the project, and buy-in from staff.
- Records Management Coordinator/staff will ensure that the drive structure and policy and procedures meet records management requirements.
- Input from all staff may be necessary in order to determine if the proposed drive structure and/or its accompanying policy and procedures will impede the work of staff in any way.

- Information Technology professionals (either from the Information Technology Department or the institution's own IT staff) will set up the agreed upon drive structure and assign access permissions as necessary. They will also provide advice concerning any technical issues encountered during the development of the drive structure and in the future.

Other individuals, such as the institution's privacy officer, may be called on to provide advice if needed. The Provincial Archives' Information Management Services can also be contacted to provide assistance.

1.2 Determine the Scope of the Work

In order to allocate adequate time and resources to the development and implementation of a new drive structure, it will be necessary to determine the scope of work that needs to be done. The following questions may help with this assessment:

- Is the new drive structure limited to a single branch, or will it be done on a larger scale (e.g. division wide or institution wide)? If the latter, will you develop and implement the new drive structure for the entire division or institution at once, or divide the work into smaller segments?
- Who will be responsible for the initial set-up of the new folder structure and movement of records into it? Who will be responsible for maintaining the structure going forward?
- Once the new drive structure is in place, does the institution intend to use it on a "go-forward" basis (meaning that on a certain date active records will be moved into the new structure and the institution will begin saving new records in this structure, while existing inactive records remain in the institution's old drive) or will all records be moved into the new drive structure, including inactive (legacy) records?
- Will the institution undertake a clean-up of records in its existing shared drives to identify and remove transitory records (such as duplicate copies) and non-work related records prior to moving records into the new drive structure?
- If the institution does not intend to move inactive (legacy) records into the new drive structure, does it have a plan for their management? How will the institution monitor and, if necessary, migrate these records to ensure that they do not become inaccessible due to format obsolescence? How does the institution intend to classify these records so that they can be legally disposed of through the Archives' disposition process?
- What file formats are currently found in the institution's drives? Are there any file extensions that you do not recognize? Are there files in versions of software that may soon become inaccessible and will the institution need to migrate these files to the new version? Are there files in versions of software that are already inaccessible and how will the institution address this?

1.3 Establish the New Drive Structure

The Provincial Archives recommends that each institution's shared drive structure be based on the approved records schedule(s) applicable to that institution. For executive government, this means the Administrative Records Management System 2014 (ARMS 2014) and one or more Operational Records

Schedule (ORS), while for CIC crown corporations and certain other institutions, this means a comprehensive corporate-wide schedule. There are a number of reasons for this recommendation:

- Records schedules are composed of groupings of records that relate to the same function, activity, or business process; these groupings are referred to as records series. Within the retention schedule the records series are arranged into broad sections (for example, Human Resources), and each records series is assigned a classification number. Therefore, basing the drive structure on applicable records schedules should ensure that records in the drive structure are organized in a logical way and that related records are kept together.
- Attached to each record series is a retention period or periods. This is the minimum length of time that the records found within that records series must be kept by the institution. Basing the institution's drive structure on applicable records schedules means that records with the same retention period will be found together. This will help facilitate the eventual disposal of the records, as the institution will be able to identify batches of records that will be eligible for disposal at the same time.
- *The Archives and Public Records Management Act* specifies that no government record may be disposed of unless it is done pursuant to an applicable approved records schedule. This means that all government records must be classified using the appropriate schedule and records series number when they are submitted to the Provincial Archives for disposal. It is easier to classify records at their creation or receipt rather than retroactively apply classification numbers to records, as the latter often requires significantly more effort on the part of the institution.

Institutions that do not have an approved ORS or comprehensive corporate-wide schedule should contact Information Management Services for advice before beginning the process of establishing their drive structure.

In addition to applicable records schedules, two other factors will influence how the drive structure is set up. The first of these is the institution's need to restrict access to certain records; the second is the technical limitations that determine how access permissions that restrict the records can be applied. Access to records may need to be restricted for a number of reasons. The records may contain personal information, as defined by *The Freedom of Information and Protection of Privacy Act*, or personal health information, as defined by *The Health Information Protection Act*, or they may contain information that the institution considers sensitive or confidential. In these situations access to the records will need to be restricted to those employees who require the information in order to perform their duties.

However, certain technical limitations can make implementing access permissions challenging and must be considered when developing the drive structure. For those government institutions that receive IT services from the Information Technology Department (ITD), a limiting factor is that access permissions cannot be set any lower than the third level of the drive structure. Institutions that do not receive services from ITD should consult their IT provider/staff to determine if the same limitation applies. The institution must ensure that in their drive structure access permissions can be applied at the records series level or lower, where documents begin to be found. This means that the records series level must not be lower than the third level of the institution's drive structure.

The following are examples of possible drive structures, as well as an example of a drive structure that should be avoided.

Example 1

The following drive structure allows a records series to be restricted if necessary, while allowing others to remain open to all users. However, if there are situations in which only specific information within a records series needs to be restricted, this structure may restrict more information than is necessary and could hinder the work of employees.

Level 0	Level 1	Level 2	Level 3 (last permission level)
G:/	Branch/	ARMS/	Records Series *(e.g. 1000_Building Maintenance)*
		ORS/	Records Series

Example 2

As an alternative, the structure below gives the institution more flexibility when restricting access to records, as it is possible to restrict some, rather than all, of the records within a records series.

Level 0	Level 1	Level 2	Level 3 (last permission level)
G:/	Branch_ARMS/	Records Series *(e.g. 1000_Building Maintenance)*	Folders/files within the records series *(e.g. Building A Folder, Building B Folder, etc.)*
	Branch_ORS/	Records Series	Folders/files within the records series

Example 3

By contrast, the following structure would be problematic for an institution when access permissions need to be applied to records. In this structure, the institution would be unable to apply access permissions to either individual records series or to specific folders within a records series.

Level 0	Level 1	Level 2	Level 3 (last permission level)	Level 4
G:/	Division/	Branch/	ARMS/	Records Series *(e.g. 1000_Building Maintenance)*
			ORS/	Records Series

Once you have established a folder structure for active records, a set of duplicate folders with the same structure will be added, into which closed records will be moved in order to wait out their required retention periods. These will be read-only folders, so that staff can view the records and, if the need arises, copy them back to the active folders, but cannot move records into these retention folders or delete records from them. The retention folders will be assigned an administrator or administrators (ideally not more than two or three people) who will have permission to move records into and delete records from these folders. This is intended to help prevent the unauthorized alteration and destruction of official government records.

Example of Full Drive Structure

The example below shows a drive structure currently used by an institution of the Government of Saskatchewan. All of the branch's electronic records are stored within the G:\Branch folder in 6 main subfolders at the second level: ACT_ARMS, ACT_ORS, ACT_RESTRICTED, RET_ARMS, RET_ORS, and RET_RESTRICTED.

- The ACT (active) folders contain all records that are in development or are actively in use, including records that were created some time ago but are still actively used for reference (e.g. policies).
- The RET (retention) folders contain all records which are closed and being held for their retention period before they can be disposed of. Please note that in cases where the retention period for a records series includes a condition, records are not considered closed and moved into the retention folder until the condition has been met. These folders are read-only for most employees to prevent modification or deletion of records.
- The RESTRICTED (Restricted Access) folders hold all ARMS and ORS series containing records that require access be restricted because they include personal, confidential or sensitive information. This institution decided to include the restricted folders so that records with access restrictions can be housed without needing to create special permissions within the ARMS or ORS folders.

At the third level are the folders for each record series.

At the fourth level, under each record series, are the active files (in the Active folders) and a "Closed" folder for placing closed records. This is the level at which employees are able to begin creating folders/documents. Employees who work with the records are in the best position identify records that are considered closed (e.g. records of projects that have been completed) and are expect to move the records into the "Closed" folders within each series. The "Closed" folders are periodically reviewed by an individual with administrator access to the retention folders, who then moves the closed records into the retention folders. In the Retention folders, the fourth level contains a folder for each fiscal year of file closure for easy tracking and organization of closed records.

The fifth level within the Retention folders mimics the fourth level in the Active folders with the exception of the Closed folders. All of the records that were closed in a specific series in a given fiscal year are stored in these folders to await their retention period and eventual disposal.

Level 0	Level 1	Level 2	Level 3 (last permission level)	Level 4	Level 5
G:/	Branch	ACT_ARMS (Read/Write for all users)	All active ARMS series folders	Folders/files within each ARMS series	
				Folder for identification of closed records within each series	
		ACT_ORS (Read/Write for all users)	All active ORS series folders	Folders/files within each ORS series	
				Folder for identification of closed records within each series	
		ACT_RESTRICTED (Read/Write for specified users)	Any active ARMS and ORS series folders with special user access	Folders/files within each series	
				Folder for identification of closed records within each series	
		RET_ARMS (Read Only for all users)	All inactive ARMS series folders	Folder for each fiscal year	Folders/files from the ARMS series closed in the fiscal year indicated
		RET_ORS (Read Only for all users)	All inactive ORS series folders	Folder for each fiscal year	Folders/files from the ORS series closed in the fiscal year indicated
		RET_RESTRICTED (Read Only for specified users)	All inactive ARMS and ORS series folders with special user access	Folder for each fiscal year	Folders/files from the ARMS or ORS series closed in the fiscal year indicated

Archivists from Information Management Services are available to assist government institutions to develop their drive structures.

1.4 Develop Naming Conventions

Naming conventions are a set of rules created by the institution that help to ensure that employees title folders and files in a standardized, consistent and understandable way so that users of the drive structure can browse and retrieve records easily and efficiently. For advice on developing your institution's naming conventions, please consult the *Naming Conventions* document found on the Provincial Archives' website.

1.5 Implementation of the Drive Structure

The following suggestions may be helpful during the implementation of a structured shared drive:

- Ensure that employees are aware of the upcoming change, the reasons for it, and the importance of adhering to the new drive structure and its procedures.
- Provide employees with training and informational material before they are expected to begin using the new drive structure. Employees who are familiar with records schedules and basic records management concepts will be better able to understand and effectively use the institution's shared drive. Helpful records management resources will include:
    - a glossary of records management terms
    - the records schedules applicable to the institution, on which its shared drive structure has been based
    - naming conventions
    - online records management training developed by the Provincial Archives. This training can be accessed through LEARN by those institutions who have access to it. The training is also available through the Provincial Archives website for institutions without access to LEARN.
    - Records management policies and guidelines on the Provincial Archives' website
    - Additional records management policies, procedures, manuals, etc. developed by the institution
- Ask employees to review the folders they use to identify transitory records so that these can be removed before records are moved into the new drive structure.
- Analyze the institution's current folder structure and map the existing folders into the new drive structure before beginning to move records.

2. Policy and Procedures for Structured Shared Drives

The Provincial Archives recommends that if an institution has not already developed an Overarching Records Management Policy, that it do so as part of the process of establishing the shared drive and associated policies and procedures. Within the institution's Overarching Records Management Policy or in its policy and procedures for the management of the shared drives, each government institution should identify the format (paper or electronic) in which the institution expects employees to retain official records. It is likely that government institutions will find that some exceptions will need to be made no matter which format they select. An institution that decides that official records should be retained electronically may determine that certain records must still be kept as paper because there is a legal requirement to do so, or because long term retention requirement will make it difficult to keep the records accessible electronically. An institution that chooses to keep its official records in paper will find that in the case of certain records (for example, records held in databases, audio and video records, CAD files, etc.) it is difficult or impossible to print and file them in a paper filing system. Each institution will need to create a list identifying records which must be retained in the format other than the one that is considered the default for its official records. This list may be incorporated into the chosen records management policy or added to it as an appendix.

The declaration of a default format for official records and list identifying exceptions is important, as it provides clear direction to employees. Please note that designating paper records as the institution's default for retaining official records does not negate the need for well-designed and properly managed shared drives. Prior to being printed and filed, the records need to be logically arranged and clearly identified so that they can be located and used by employees, and so that proper access controls can be applied to records containing personal, confidential or sensitive information.

The following items should be addressed in an institution's shared drive policies and procedures.

2.1 Roles and Responsibilities

Managing records in shared drives requires ongoing effort and commitment from various levels of the institution. An institution's shared drive policy and procedures should clearly define the roles and responsibilities of employees at all levels of the institution in regard to the use, maintenance and management of the shared drive structure. For an example of roles and responsibilities for the management of a shared drive, please refer to Appendix B.

2.2 Explanation of Drive Structure

Procedures should provide employees with an explanation of the layout of the institution's drive structure, and how the structure is intended to be used. Items that may need to be explained include:

- the difference between the active folders and the retention folders, and the purpose of each

- at which levels of the folder structure users may create their own folders and at which levels only designated individual(s) may create folders
- at which levels of the folder structure users may file records
- where restricted folders are located, why access to certain folders is restricted, which users have access to these folders, and what employees should do if they have not been given access to records that they require in order to perform their job.

2.3 Use of Personal Drives

Government records stored in personal drives are inaccessible to other employees who may require them, and may be forgotten or lost if the individual in question does not move them to the shared drive when departing the institution. The institution's procedures should clearly define how personal drives should be used by employees. It should outline the circumstances (if any) in which it is acceptable to save work in a personal drive, and ensure that employees understand that any government records must be transferred to the shared drive. Since the institution's shared drive structure will place access restrictions on records containing personal, confidential or sensitive information, the presence of such information should not typically be one of the circumstances in which it is acceptable to save records in a personal drive.

2.4 Shared Drive Auditing and Compliance

Periodic auditing of the drive structure will be necessary to ensure that it is being properly used. For the individual(s) assigned the responsibility of auditing the shared drive, the procedures should outline what to look for to determine that the drive is being used appropriately. This includes ensuring that folders and files are being created at the appropriate levels of the drive structure, the folders and files are saved under the correct item (classification number) in the drive structure, that naming conventions are followed when folders and files are created, and that folders and files are not being unnecessarily duplicated. The individual(s) responsible for auditing will also need to identify if there are employees who are not using the shared drive. Further, the procedures should outline what action the individual(s) responsible for auditing the drive structure are expected to take if employees are not using the drive structure appropriately, or not using it at all. Such action may include reminders to use the drive structure, or additional training/assistance in its use. For repeated misuse or refusal to use the drive structure, action may include reporting the behaviour to the individual's supervisor.

2.5 Inventory of Records in the Shared Drive Structure

The institution should maintain an inventory of its electronic records. This inventory will include the records in both the active and retention folders. The shared drives procedures should identify the information that the individual(s) responsible must keep as part of this inventory. This should include a file name/description, the schedule to which the records relate, the item number within that schedule under which the file is classified, the applicable retention period, the date of file closure, the fiscal year in which the record will be eligible for disposal, the file format, and the size of the file. The inventory may also include any other information concerning the records that the institution considers valuable to collect.

2.6 Transferring Records from the Active Folders to the Retention Folders

Once records are considered closed, they will need to be moved to the retention folders to wait out their required retention periods. Because access to the retention folders is limited, the transfer can only be done by an individual who has been assigned administrator privileges. The institution's shared drive procedures will need to establish a method for employees to identify records that have been closed so that the designated individual(s) can move them to the retention folders. In the example of a drive structure provided in section 1.3 of this document, we've proposed including a "closed" folder under each record series into which employees are directed to place closed records. However, institutions may develop their own alternatives to this proposal. The procedures should also provide the individual(s) responsible for transferring the records to the retention folders with an explanation of how this is to be done.

2.7 (Year-End) File Maintenance

The institution's shared drive procedures should provide direction for the maintenance of records in the folder structure. Staff should be advised to regularly remove transitory records from folders in the shared drive structure. At the end of the institution's fiscal year, all staff should be asked to review the records they create and use in order to identify those that are no longer active or have met the closure conditions identified by their retention period, and move these records into the "closed" folders. The designated individual(s) should then move these records into the retention folders, and update the institution's inventory of records. This suggestion for maintenance of files in the shared drive is again based on the use of 'closed' folders within the filing structure. Institutions may develop their own alternatives to this proposal. Prior to moving the records, the individual(s) responsible may also wish to audit the records to ensure they are correctly classified and titled in accordance with the institution's naming convention. Please note that this may be done periodically throughout the year, rather than only once. In large institutions, or institutions that find they have a large volume of records, it may be preferable to do this quarterly or bi-annually. However, at minimum, this should be done at year-end.

2.8 Disposal of Records

The shared drive procedures should ensure that employees are aware that they must not delete government records from the drive structure. They may, however, delete transitory records, so the institution's procedures and/or employee training should explain the difference between these two types of records.

Deletion of government records from the shared drive structure must be done in accordance with the Provincial Archives' disposal process. The same process that is followed to authorize the disposal of physical government records must be followed in order to dispose of electronic government records. The records may only be disposed of (deleted) after the institution has received permission to do so from the Provincial Archivist. For a full explanation of the Provincial Archives disposal process, please refer to the Archives' Records Disposal System on our website. The procedures should also outline or refer to any internal disposal requirements developed by the institution.

Once the institution receives permission to dispose of electronic records the individual(s) assigned this responsibility will delete the records from the retention folder. The individual(s) will sign a certificate of deletion to confirm that destruction of the records was carried out. This certificate, along with all other documentation pertaining to the deletion of the records, must be retained in accordance with the applicable retention schedule.

2.9 Other Repositories (SharePoint, etc.)

Many institutions create and hold records in other repositories, such as SharePoint. The institution's procedures may need to address how government records created in these repositories will be handled. In some cases, it may be possible to adequately manage the records within the repository. However, if this is not possible the procedures may instruct users to move the records from the repository into the appropriate folder in the shared drive structure.

2.10 File Formats and Migration

Institutions which manage official government records electronically must give consideration to the file formats in which the records will be retained. File formats become obsolete over time, and electronic records that are not migrated into new versions of software can become inaccessible. This is of particular concern when records have long-term retention requirements. To reduce the risk of records becoming inaccessible due to file format obsolescence, the shared drive procedures should identify the file formats in which it is acceptable to retain records with long-term retention periods (i.e. retention periods longer than 10 years). Employees should be directed to create and save records in these formats whenever possible. If the records cannot be created in one of the file formats identified, the procedure may direct the creator, or a designated individual, to migrate the records into one of these formats as soon as possible. The procedures should also ensure that the institution monitors records in the shared drive to identify any records that are at risk of becoming inaccessible due to file format obsolescence, and outline the action that the individual(s) responsible are expected to take when such records are identified. Further information on file formats may be found in the Archives' document *File Formats for Long-Term Preservation and Transfer to the Provincial Archives*, which is available on the Provincial Archives' website.

Appendix A
Tools to Assist the Transfer to a New Drive Structure

The following are some tools which may be helpful as an institution makes the transition to its new drive structure. The Provincial Archives does not endorse any specific tool, and we recommend that an institution consult its IT provider before it downloads and installs anything for use in its drive structure transfer/clean up. Your IT provider may be able to suggest other tools and may need to be notified that a tool will be in use.

- File naming tools can batch process and modify the document name to help adhere to the institution's newly established naming conventions, and can also be used to transfer information from parent folders to document names.
- File management tools can assist in moving documents, as they allow you to open multiple folders next to each other, drag and drop between them and report on the contents of the folder structure.
- Link management tools can be used to preserve links between documents when moving files around.
- Tools are available for managing the transfer of email into folders within shared drives so that they can be managed alongside the records to which they relate.
- Duplicate finder tools can be used to locate copies of records within the shared drive so that duplicates that meet the definition of a transitory record can be identified and disposed of. Please note that duplicate finders should be used with caution. At times, copies of records may be found in more than one place because the information is required to support separate functions/business process; therefore, neither copy of the document should be considered a duplicate.

Appendix B
Shared Drive Roles and Responsibilities

The following is an example of roles and responsibilities that may be assigned to employees at various levels of an institution in order to manage its structured shared drive. Each institution should adjust these roles and responsibilities to fit its circumstances.

Records Management Coordinator and/or Shared Drive Working Group/Leads

Ideally, the implementation and management of an institution's shared drives should be overseen by its Records Management (RM) Coordinator. The RM coordinator will likely not have the time to handle the day-to-day management of the institution's shared drives, particularly in large institutions. It will be necessary to establish a shared drive working group and/or appoint Shared Drive Leads at a level considered appropriate within the institution (e.g. at the division level, branch level or unit level, depending on the institution's size) to assist the RM Coordinator. A shared drive working group and shared drive leads may also be used in cases where an institution has no RM Coordinator.

The RM Coordinator and shared drive working group/shared drive leads will be responsible for:

- providing training on the organization of the shared drive folder structure and use of the shared drives to the institution's employees
- communicating any changes in the folder structure or associated policy and procedures to the institution's employees
- ensuring appropriate access controls are in place, that incoming employees are provided access to restricted folders if necessary, and that access is removed from employees who no longer require it or are leaving the program area
- monitoring the shared drives to ensure employees are correctly classifying records and are adhering to the naming conventions established by the institution
- transferring files that have been identified as closed from the active drive into the retention drive
- maintaining an inventory of active, inactive and deleted files
- submitting requests for disposal of electronic records to the Provincial Archives and carrying out the deletion of the records once permission is granted

Management

Executive management must demonstrate their commitment to the initiative to implement and manage a structured shared drive, and their support of the RM Coordinator and others assigned to work on this task. It is the responsibility of executive management to:

- allocate appropriate resources to the implementation and management of the shared drive
- approve the shared drive policy and procedures, and any subsequent changes to them
- promote the use of the shared drive and the shared drive policy and procedures developed by the institution

- ensure employees receive training in the use of the shared drive

Information Technology Department/Internal Information Technology Staff

Ongoing involvement from the institution's IT provider/staff will be required in order to maintain the shared drives. It is their responsibility to:

- assign the required access permissions to the institutions staff, as requested by the RM Coordinator, shared drive working group, or shared drive lead
- provide technical advice on any issues related to the management of the shared drive to those responsible

All Staff

Cooperation of staff who create and access files in a shared drive is necessary for the maintenance of an effective shared drive. It is the responsibility of all staff to:

- file records in the appropriate location in the shared drive folder structure established by the institution
- follow all procedures established by the institution for the shared drive, including naming conventions
- safeguard records filed on the shared drive that contain personal, sensitive or confidential information
- request clarification or assistance from a shared drive lead or the institution's records management coordinator if needed

Appendix C

Certification of Destruction – Electronic Records

This document confirms that the electronic records indicated in the attached inventory have been approved for destruction by the Provincial Archivist and have been destroyed/deleted from all electronic storage systems. All copies including backups and printed versions of the indicated records have also been identified and destroyed.

This form should be filed along with all other documentation related to the destruction of the indicated records. An inventory or inventories of the records must be attached to this form.

Institution: _____

Branch: _____

Location: _____

Internal disposal record ID (if applicable): _____

PAS disposal authorization file #: _____

PAS disposal authorization date: _____

Inventory of destroyed records is attached _____

Method(s) of destruction _____

Notes:

Records destroyed by: _____ (Print) _____ (Signature)

Witnessed by: _____ (Print) _____ (Signature)

Destruction Date: _____