

Managing Official Electronic Records Guidelines

Application and Scope of Guidelines

These guidelines are meant to assist Government Institutions in understanding responsibilities and concerns that must be taken into consideration when choosing to designate electronic records as official public records. This applies to all Government Institutions subject to *The Archives and Public Records Management Act*. These guidelines do not apply to transitory records, which should be managed and disposed of according to *The Transitory Records Guidelines*, or non-work related material, which should be removed or deleted from the government records keeping systems on a regular basis.

Definitions

An **electronic or digital record** is any item of information that is created, recorded, or stored on any medium in or by a computer system or other similar device. These records must be managed in the same manner as records in other formats. Electronic records that are subject to records management requirements include e-mail and other electronic messages, social media, websites, and records stored on cloud computing services, in addition to word processing documents, databases, photos, and all other digital media formats.

The Archives and Public Records Management Act defines a **Public Record** as

- (a) a record made or received by a government institution in carrying out that government institution's activities;
- (b) a ministerial record;
- (c) a record made or received by the Legislative Assembly, the Legislative Assembly Service or an Officer of the Legislative Assembly;
- (d) a court record; or
- (e) an administrative record of a court;

The Archives and Public Records Management Act defines a **record** as:

Information Management Unit

“a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or other mechanism that produces records.”

Requirements

As *The Archives and Public Records Management Act* is media neutral, the management of electronic records (including e-mail) should be integrated with other records management practices for records in the custody or under the control of each institution. Having a unified Records and Information Management program is grounded by comprehensive policies and procedures which establish control over records, including the creation and implementation of all applicable records schedules (ARMS2014, Operational Records Schedules, or Corporate-wide Records Schedules).

Records retention schedules that are at the heart of a well-established RIM program allow institutions to have control over their information resources by:

- Providing an organizational structure based on common functions which can be applied to a digital environment such an EDRMS (Electronic Document Records Management System) or network drive
- Ensuring that electronic and paper records management systems work together
- Providing records retention requirements for long-term system and record migration planning
- Providing a legal method for disposal of records

As outlined in *The Archives and Public Records Management Act* and the Saskatchewan Records Disposal System, public records must maintain their usability, accessibility, legibility and transferability throughout their lifecycle. In addition, records must be authentic, complete, and maintain their integrity as outlined by *The Electronic Documents Act* and *The Evidence Act*, which presents a number of additional concerns when designating and managing electronic records as official records of a government institution. The following are some major issues to address:

- Appropriate records management procedures and policies must be created to ensure standards for the management of electronic records. This includes an

- approved retention schedule(s), in addition to the procedures and policies established as part of the RIM program
- Public records must be disposed of in accordance with *the Archives and Public Records Management Act*, either by transfer to the Provincial Archives of Saskatchewan or securely destroyed with the permission of the Provincial Archivist. Any existing copies of the public official records that exist within your institution must also be deleted as per *The Transitory Records Guidelines*
 - Procedures and controls must be in place to prevent the accidental deletion or alteration of records, tampering with data, etc.
 - Adequate back-up procedures to mitigate risk, including periodic checks to ensure long term records viability
 - Implementing adequate access and security protocols, including access permissions and safeguards for individual records and the system
 - Metadata capture and control
 - Migration strategies that take into consideration software and system upgrades as well as records retention dates so that records managed by the system remain accessible, legible, usable, and are not affected by the obsolescence of software and hardware.

Please consult your organization's IT Unit/staff for more information regarding information technology infrastructures that affect your organization, in addition to facilitating discussions between records management staff and individual business units. It is very important that your IT Unit is aware of records management requirements applicable to your electronic records in order to maintain the records properly. Also, consult your legal counsel regarding legal requirements concerning the records and to ensure that your official records can be kept electronically. Certain classes of official records must be retained in physical form. Communication between these groups is integral so that all requirements are taken into account and appropriate solutions are applied consistently.

Working with Electronic Records

Any electronic records management solution heavily relies on the successful implementation of a robust RIM program. When choosing to work with electronic records there are three possible ways to implement a successful electronic records management system: an Electronic

Document Records Management System (EDRMS), a non-EDRMS environment, and the print-and-file system.

- 1. Electronic Document Records Management System (EDRMS)** is by far the most effective way to manage electronic documents as it will facilitate the implementation of adequate controls, which ensure the authenticity and integrity of digital records and their proper maintenance and disposal; but it does come with costs and still requires planning and preparation. Please see *the Electronic Document and Records Management System (EDRMS) Acquisition Strategy*, developed by the Provincial Archives for more information about choosing, implementing, and working with an EDRMS.
- 2. A non-EDRMS environment** (or shared/network drive system) is the most common way to manage electronic documents in the absence of EDRMS. This approach to electronic records management can quite efficiently address all of the aforementioned concerns but it may require the implementation of additional security, records management protocols, and technical programming to ensure consistent and complete control of records. The following appendix shows examples of how a shared/network drive can be structured using records series from ARMS2014.
- 3. The print-and-file system** is the default way to manage electronic records if no policy exists to designate electronic records as official public records and there are no other solutions in place to manage digital records (see point 1 and 2 above). This method may work well within the scope of already established paper records management systems, but may become problematic when dealing with complex types of electronic records (such as databases, spreadsheets, images, videos, websites, etc).

Additional Documents for Consultation

These guidelines comply with and support the following legislation: *The Archives and Public Records Management Act*, *The Electronic Information and Documents Act (2000)*, *The Freedom of Information and Protection of Privacy Act (FOIPP)*, *The Health Information Protection Act (HIPA)*, and *The Evidence Act*.

Information Management Unit

Please consult the following documents produced by the Provincial Archives of Saskatchewan for basic records management requirements that affect all records, including electronic documents:

- *Saskatchewan Records Management Policy*
- *Basic Records Management Practices for Saskatchewan Government*
- *Email Management Guidelines*
- *Transitory Records Guidelines*
- *Source Records Guidelines*
- *Records Management Policy Model*
- *Naming Conventions*
- *Electronic Document and Records Management System (EDRMS) Acquisition Strategy*

For further information and international standards regarding electronic records consult the following:

- *The Electronic Records As Documentary Evidence standards, by the Canadian General Standards Board and the Standards Council of Canada*
- *ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments*
- *MoReq2010 Modular Requirements for Records System*

If you have any further questions or concerns, please contact the Information Management Inquiry Line at recordhelp@archives.gov.sk.ca or 306-787-0734.

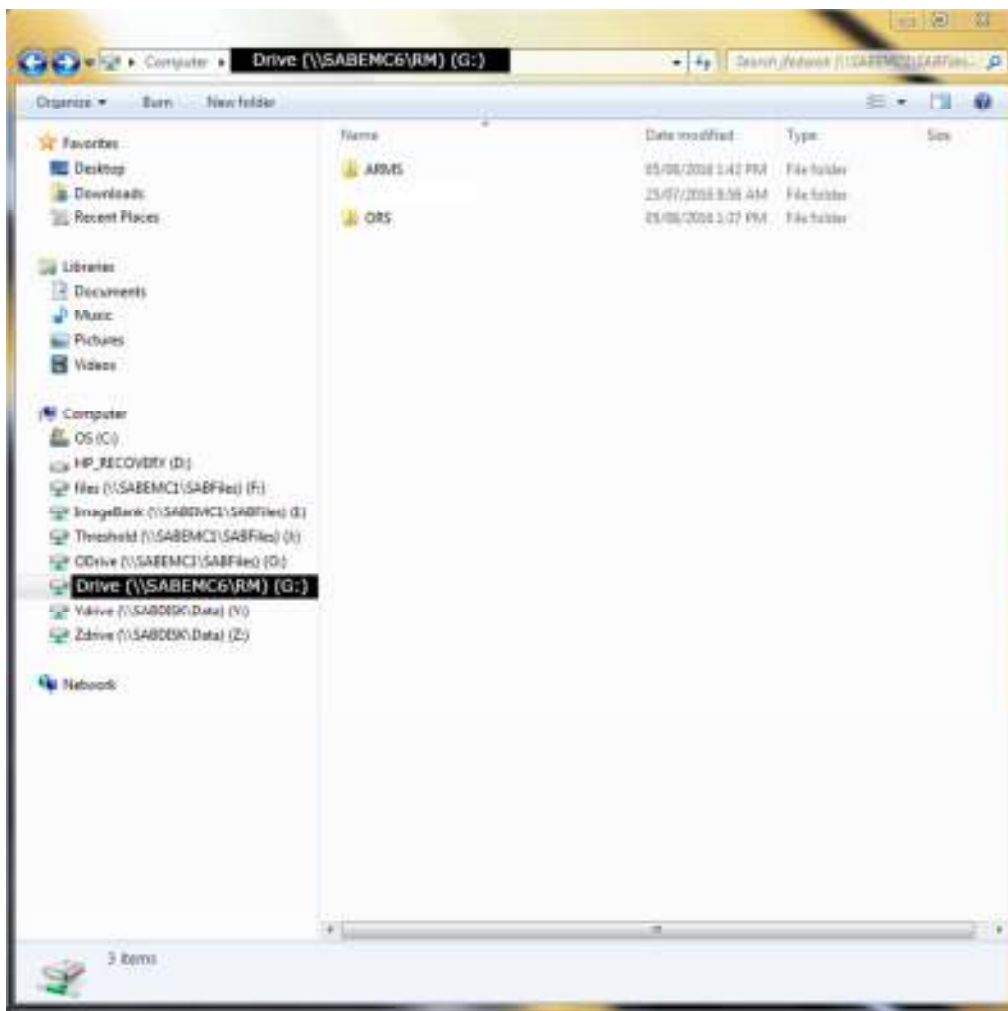
Appendix: Working with Electronic Records in a non-EDRMS Environment

A shared directory is a directory created on a computer hard drive that is accessible to many users in a network environment, and can be formatted based on ARMS2014, an Operational Records Schedule, or a Comprehensive Records Schedule to facilitate good records management practices without the use of an Electronic Documents Records Management System (EDRMS).

Level 1:

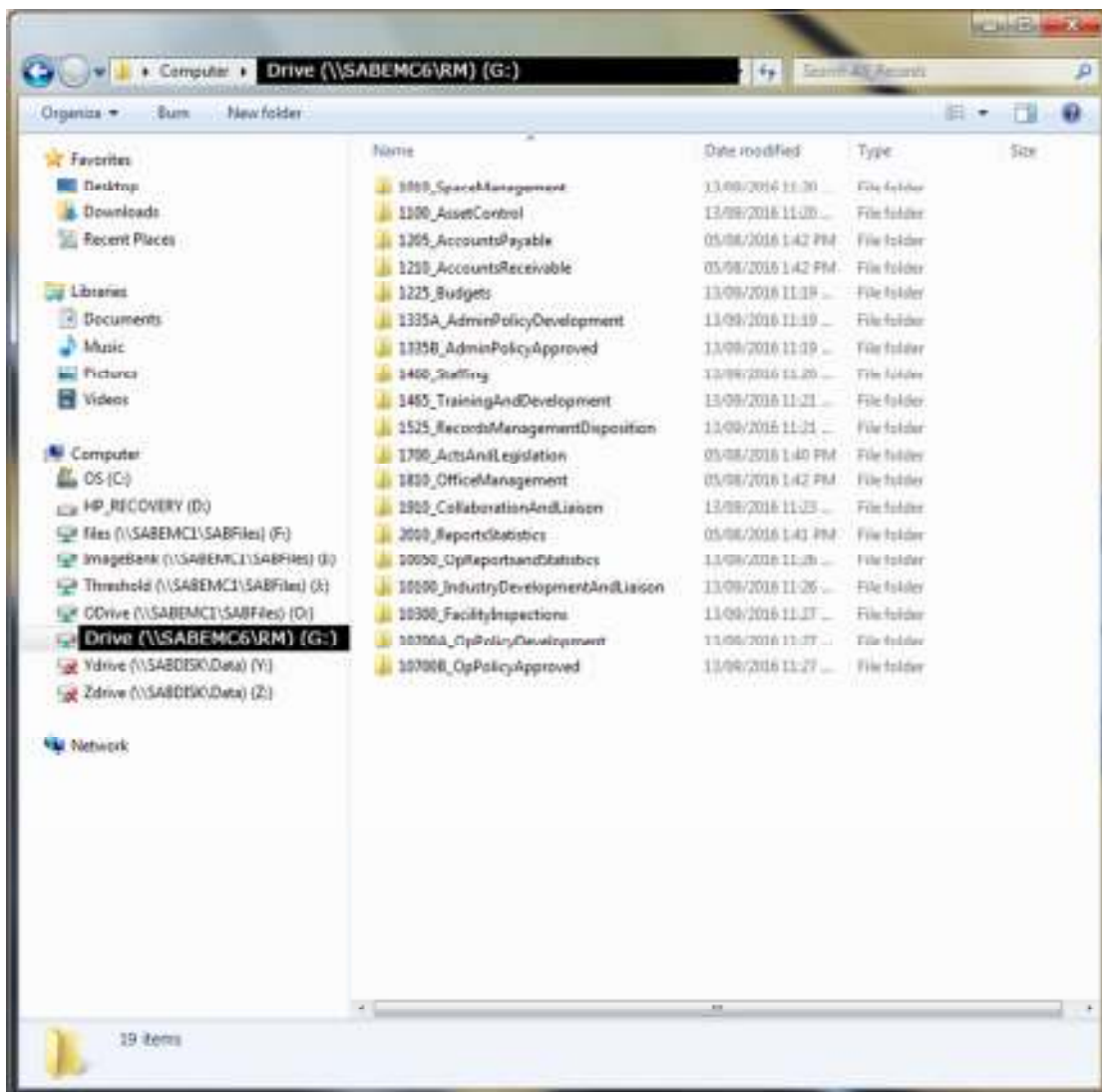
Within a shared drive it is often useful to separate Administrative Records and Operational Records based on their records schedule to easily delineate the functions of those records. Additional directories may also be added at this level for groups of records which require additional security as a whole (such as Executive Management, Deputy Minister, etc).

Information Management Unit



If an organization is small or a limited number of record series are used an organization may not choose to separate Administrative and Operational records series at the first level. The differing styles of numbers (ARMS2014 series are numbered with 4 digits, while ORS usually have 5 digits) will facilitate an intellectual distinction between these two types of records, but make sure to differentiate between series which have similar functions but relate to only Administrative Records or Operational Records (such as we have shown with the Policy Development series from ARMS2014 and the ORS).

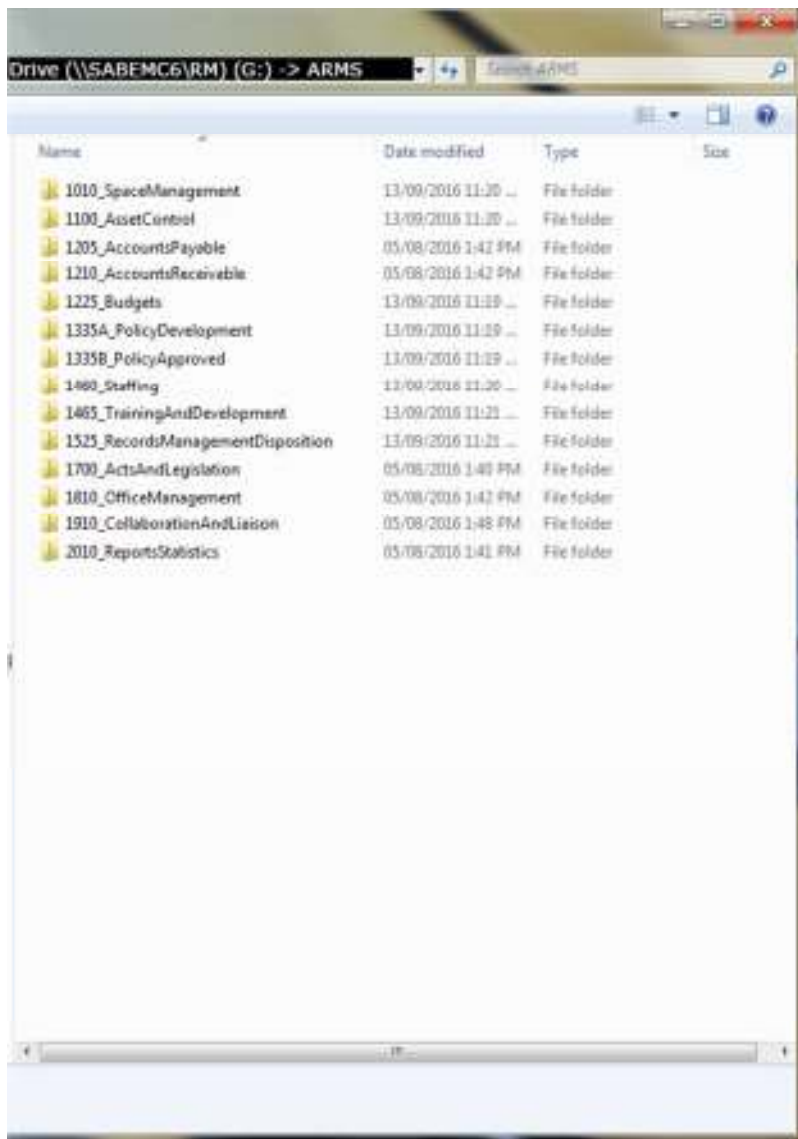
Information Management Unit



In the following examples we will explore how to apply the records series from ARMS2014 to a shared directory. Any records series from ARMS2014 or an Operational Records Schedule can be applied similarly.

Information Management Unit

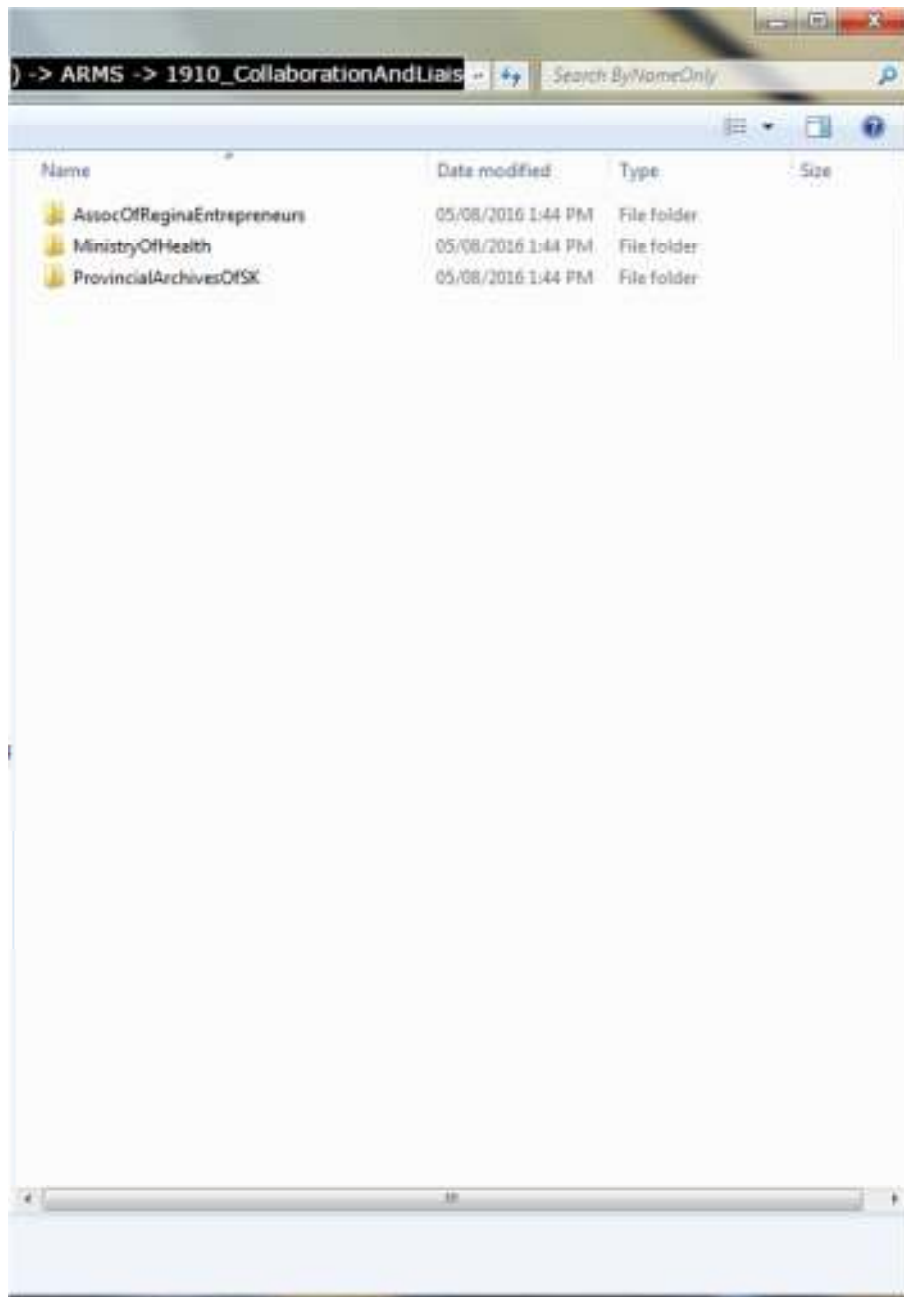
Level 2: Within the Administrative Records section of the directory we have created folders based on the record series within ARMS2014, with item numbers included to facilitate numerical filing order. In this example we have not chosen to shorten the names of the records series, but you may decide to abbreviate the lengthier names of records series. Besides abbreviation, the names and item numbers from the schedule may not be changed, since these come from an approved records schedule (ARMS2014 in this case).



Information Management Unit

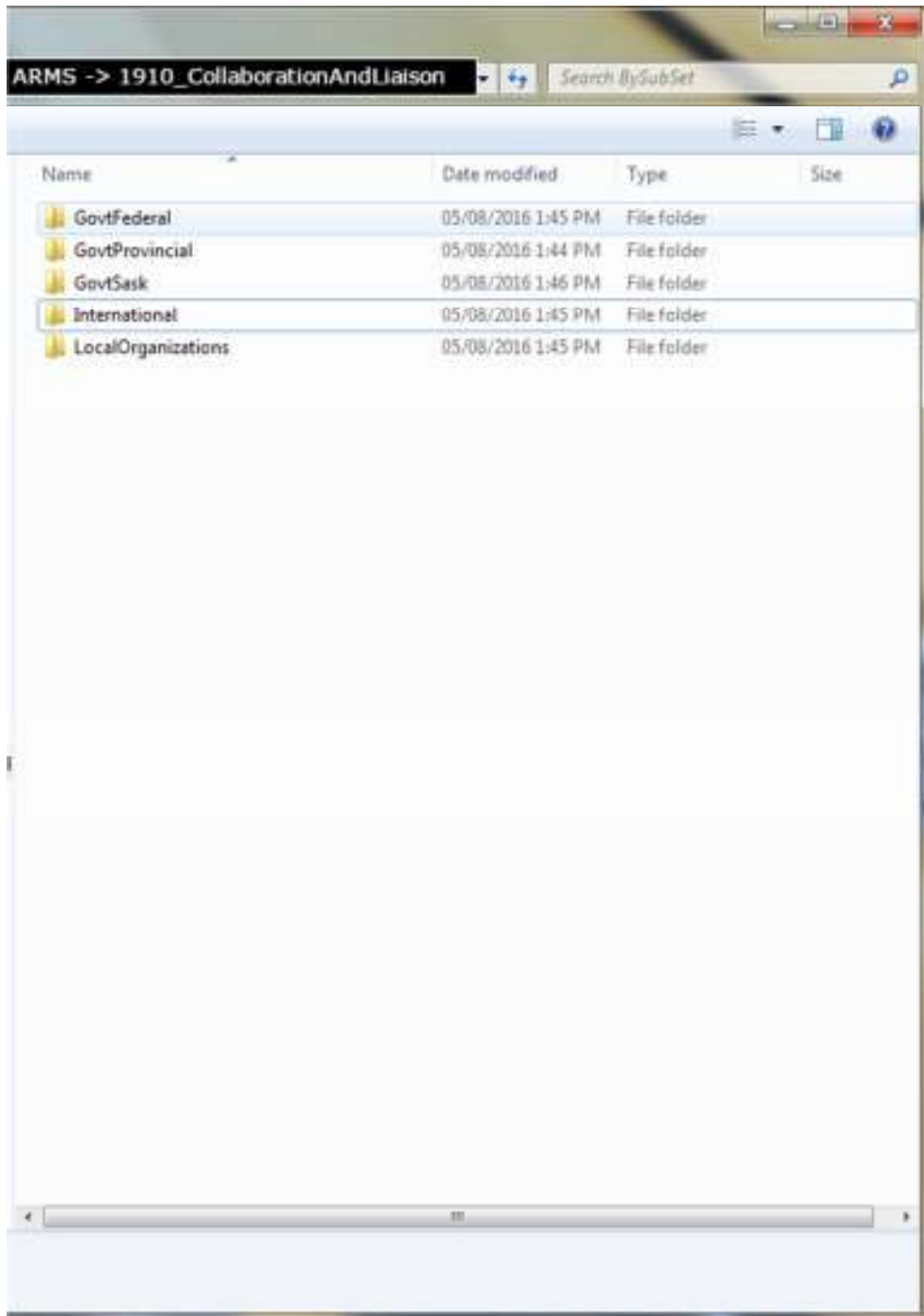
Level 3: Within each record series defined by ARMS2014 it is likely that you will need to organize records with further divisions. The following show examples of how records within the 1910 Collaboration & Liaison series can be further organized.

Organized by name of collaborating organization: This is the simplest method of organization, as it simply groups records based on the external group that the Ministry is collaborating/liasing with.



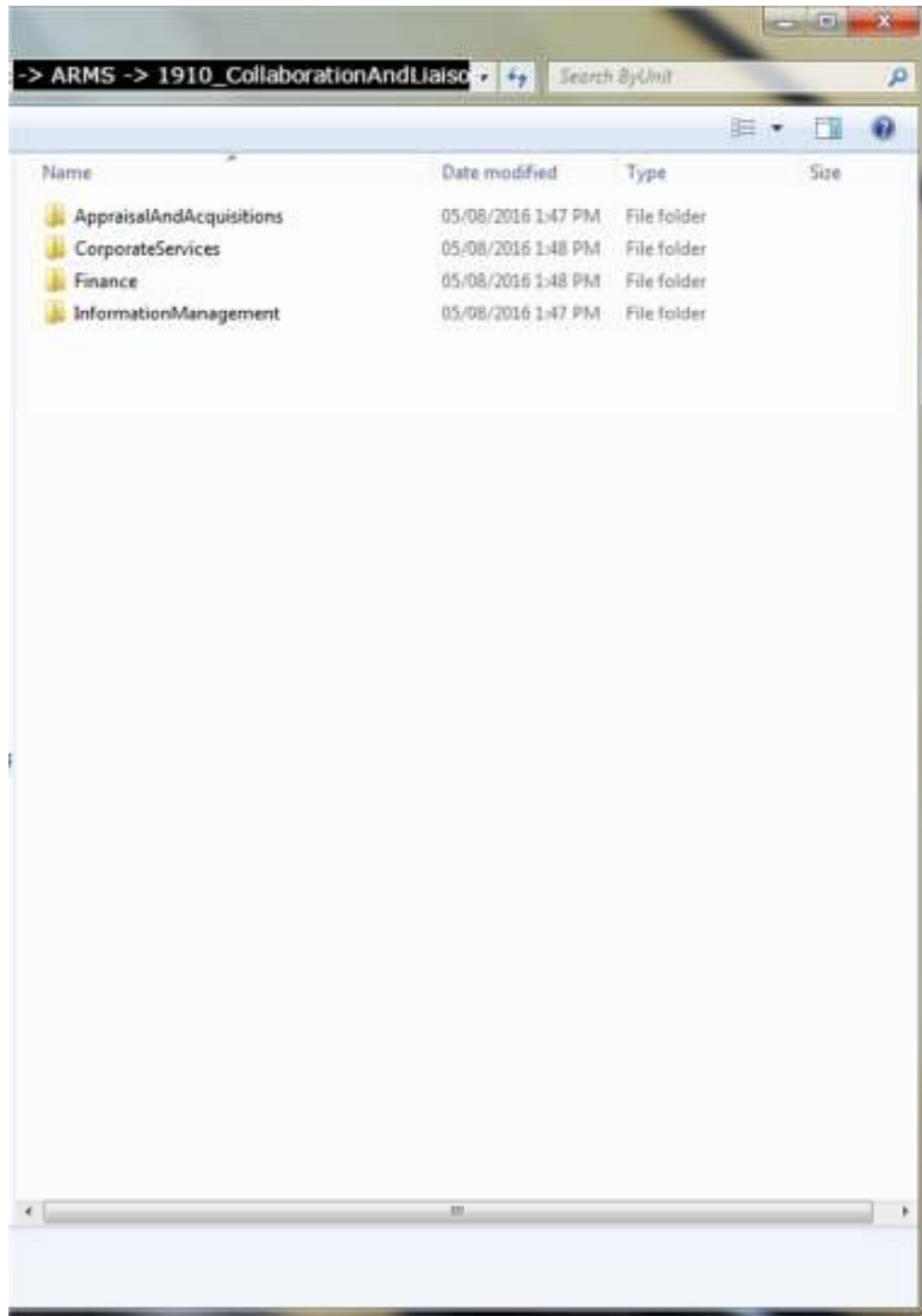
Information Management Unit

Organized by type: If there are many external groups that the Ministry collaborates/liases with it may facilitate filing to group similar external organizations together.



Information Management Unit

Organized by unit/department/division: Since many Ministries are divided by unique units, departments, and divisions, it may be logical to group records relating to each individual unit together. This method allows for privacy and autonomy between units and for easy identification by the employees of where they should file their records.



Level 4: If you choose to implement the second and third examples above, it may be necessary to create another level of organization within these groupings to separate the documents by the name of the external collaboration/liaison group.

All electronic documents (including spreadsheets, databases, images, Word documents, emails, etc.) should then be filed in the lowest level of this directory, and given meaningful names to identify their contents. It is suggested that structures not exceed 6 levels of folders (including the originating Drive and final document) or for the total file path to exceed 250 characters, as this may cause problems for the IT system or for users' ease of use. See the Naming Conventions document for further advice on creating useful and functional electronic records naming procedures. Naming Conventions should be established, implemented, and enforced throughout your organization and monitored regularly to ensure consistent application and use.