UNITED NATIONS
Archives and Records Management Section

Guidelines

November 2015

Managing Electronic Information and Records in Shared Drives

Drafted by: Ian Meldon
Approved by: Bridget Sisk
Approval date: November 2015
Contact: sisk@un.org
Office: Department of Management
Review date: November 2017

Contents

A. Purpose

1. The purpose of this document is to provide guidance to personnel in relation to the usage, organisation and management of information and records in United Nations shared drives as required by the Secretary General's bulletins *ST/SGB/2007/5 Record-keeping and the management of United Nations archives* and *ST/SGB/2007/6 Information Sensitivity, Classification and Handling*. This guidance should be used to clean-up legacy information and records, and for day-forward reorganisation of shared drive content in preparation for migration to enterprise document and records management systems.

B. Scope

2. This document is intended to serve as a guide for United Nations personnel that use, administer or are accountable for shared drives on United Nations Information and Communications Technology (ICT) networks.

C. Rationale

3. The United Nations is implementing technology to manage documents and records. During the transition offices will continue to use shared drives. These guidelines are designed to help better prepare for this transition.

4. Benefits of following these guidelines include:

   Records and information are easier to find

   - Records are filed according to a File Classification Scheme and, in turn, an approved Records Retention Schedule
   - Folders and files are appropriately and consistently named

   Trust in information is increased and co-ordination improved

   - Final version records are clearly identified and are distinct from non-record drafts
   - Controls are implemented to protect the trustworthiness of records and related metadata

   Costs may be better controlled

   - The growth of information and records storage is managed
   - The migration of information and records to other systems is improved
   - The identification of information or records to be deleted is improved

5. Pending the deployment of fit-for-purpose electronic records management systems, these guidelines will enable Offices to better align records management practice with United Nations policies *ST/SGB/2007/5 Record-keeping and the management of United Nations archives* and *ST/SGB/2007/6 Information Sensitivity, Classification and Handling*.

D. Roles and responsibilities for managing shared drives

6. All United Nations personnel are accountable for the appropriate use of shared drives, depending on their role, specific accountabilities are outlined in Table 1.

Table 1: Roles and responsibilities for managing shared drives

Role	Responsibilities
Head of Office	• Promulgates these Guidelines, emphasising accountability • Assigns roles and responsibilities, provides executive support • Ensures all personnel are aware of their responsibilities vis-a-vis records management
Information Management Officer (IMO) (or designated focal point)	• Manages the implementation of these Guidelines and acts as a focal point for personnel • Co-ordinates with personnel regarding the implementation of these guidelines • Acts as an ICT focal point with the Office of Information and Communications Technology (OICT) • Ensures folder structures implemented throughout the Office reflect a File Classification Scheme • Ensures security and access rights are applied to shared drives and folders within them, in keeping with the Office's approved access rights plan • Establishes and promotes naming conventions applicable at the folder, sub-folder and file level • Introduces new personnel to these guidelines and works with those leaving to ensure information is deleted and records retained • Plans for and oversees the migration of records in coordination with OICT • Develops and manages File Classification Schemes and liaises with the Archives and Records Management Section (ARMS) to develop Records Retention Schedules • Ensures the routine disposition of records using the Records Retention Schedule
Office of Information and Communications Technology (OICT)	• Works with the IMO or designated focal point to determine an appropriate technical configuration for shared drives[1] • Provides network and technical support, including service availability, security, capacity, migration and backup

[1] See OICT service catalogue

	• Ensures security, sensitivity and access rights are applied to servers, software and systems used to manage shared drives
All Personnel	• Correctly files records in the correct folder structures • Names information and records as per naming conventions • Separates non-record drafts from final version records and files them correctly • Regularly deletes out-of-date, duplicate or unnecessary information • Ensures sensitive information is appropriately handled as per *ST/SGB/2007/6 Information Sensitivity, Classification and Handling*. • Ensures suspicious files are not stored, and does not open those with suspect filename extensions
United Nations Archives and Records Management Section (ARMS)	• Develops and disseminates Secretariat-wide records management policy and guidance • Provides subject matter expertise on records management, including Records Retention Schedules

E. Folder structures and filing

7. Offices use shared drives to store a mix of records, working files and reference material. In order to identify records offices should have two distinct folder structures:

   - a formal folder structure to store and classify the records of the Office; and,
   - an informal folder structure to share non-record drafts, other working files and reference material.

8. The benefits of segregating content are:

   - allows personnel to distinguish records from other content;
   - helps personnel and IMOs to delete working files; and,
   - improved migration to more suitable systems.

9. The Information Management Officer (IMO) or designated focal point should develop protocols for the creation and deletion of folders in both the formal and informal folder structures.

10. Heads of Offices should require at least an annual clean-up of both folder structures. The objectives should be to correct misfiling, move records to the formal records folder structure and delete redundant content. Redundant content must be deleted two years after creation.

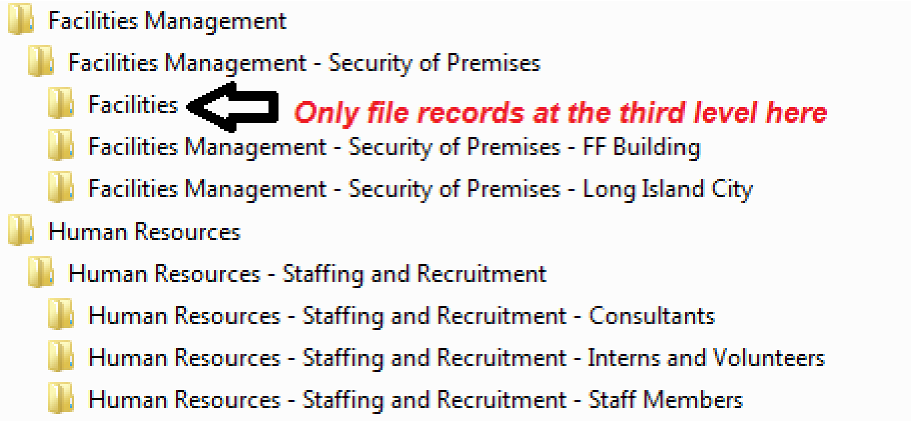
Personnel must not store records on: Local Disk (C:), H Drives, removable media, or with third-party online storage vendors such as Dropbox or Google Drive. The use of these should be restricted to genuinely personal or publically available information. *ST/SGB/2004/15 Appropriate Use of United Nations ICT Resources and Data* provides for limited personal use of ICT resources

Formal records folder structure

11. Records should be filed in appropriately named and structured folders using a File Classification Scheme reflects the substantive functions of the office and the activities within these functions. Folders for administration operations should be structured using the File Classification Scheme for Administrative Functions Common to all UN Offices.

12. A three-tier folder structure is recommended, with upper-level folders used for File Classification Scheme structure and to apply access controls. Records should be filed at the third level as illustrated in Figure 1, below.

Figure 1: Sample formal records folder structure



- Facilities Management
  - Facilities Management - Security of Premises
    - Facilities ⇦ *Only file records at the third level here*
    - Facilities Management - Security of Premises - FF Building
    - Facilities Management - Security of Premises - Long Island City
- Human Resources
  - Human Resources - Staffing and Recruitment
    - Human Resources - Staffing and Recruitment - Consultants
    - Human Resources - Staffing and Recruitment - Interns and Volunteers
    - Human Resources - Staffing and Recruitment - Staff Members

Informal folder structure

13. Personnel may create their own folders here using a one or two-level folder structure. For consistency and to make it easier to identify records or dispose of content, naming conventions should still be applied.

F. File and Folder Naming conventions

14. Each office should develop and apply locally applicable naming conventions to folders and files aligned with the best practice described in Table 2, below. The IMO or designated focal point should produce this guidance and implement it with the support of the Head of Office.

15. Folders that contain records must be named in accordance with the applicable hierarchy of functions and activities defined in the File Classification Scheme.

16. Benefits include:

- improved retrieval use and re-use of information and records;
- better sorting, browsing and ability to distinguish information and non-records drafts from records; and,
- simplified appraisal and deletion of information and records.

Table 2: Folder and file naming conventions

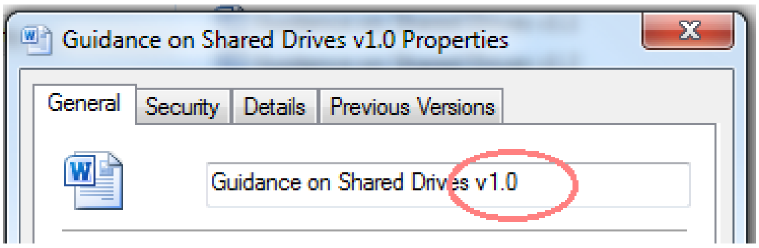
• Use consistent, short, clear, meaningful and well-defined names. For example, avoid vague names like “Jane’s Files” or “2015 Misc.”
• Use two digit numbers, i.e. 01-99 unless they represent a year as this makes it easier to maintain numeric order of files
• For dates put years first, i.e. YYYYMMDD, as per the International Standard ISO 8601 2001. This ensures records can be viewed chronologically
• Version numbers should be shown in file names as “v”, then an appropriate number. For example v1.0 or v2.0 for major changes and v1.1 or v.1.2 for minor edits. Indicate drafts and final versions by writing “Draft”, or “Final” at the end of file names *(see also, section G, Version control)*
• Put surnames before initials or forenames as this ensures correct alphabetical sorting when similar surnames exist in the same folder
• Avoid unhelpful or common words at the *start* of file names, for example “draft” as these will appear altogether in search results
• Do not mark files with their sensitivity or security in titles. Using terms such as ‘confidential’ could compromise content by publicising this in the name. Use access controls to prevent unauthorised access instead (*See Information Security)*
• To describe organisational structure, put relevant information in reverse hierarchical order (most general first): *Department, Office/Division, Section/Unit*, for example, OCHA, Emergency Liaison Branch
• Avoid using unfamiliar abbreviations or acronyms, especially if the information or records might be widely shared
• Document types may be included, as long as there is a standard format used. For example: TPs (Talking Points), RS (Routing Slip), CC (Code Cable), etc.

G. Version control

17. Specialist records management systems provide for documents and records version control. Shared drives, however, provide limited capability for this and versioning must be done manually. Personnel should therefore follow the best practice outlined below.

18. Figure 2 shows how the addition of ‘v1.0’ in the title indicates the draft status of this record. The use of small decimal increments to indicate minor revisions, and whole numbers for major revisions, will allow personnel to identify current drafts or final version records.

Figure 2: Version control in file titles

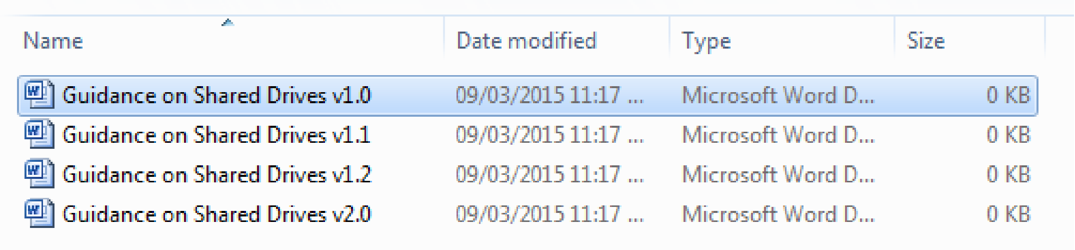


Guidance on Shared Drives v1.0 Properties

Guidance on Shared Drives v1.0

19. Figure 3, shows how consistently applying this approach allows different versions to be identified within folders in the shared drive.

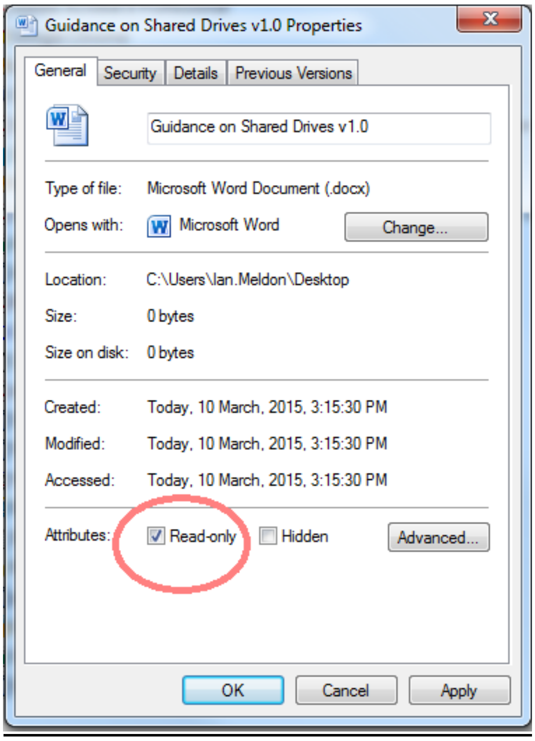
Figure 3: Version control differentiation



Name	Date modified	Type	Size
Guidance on Shared Drives v1.0	09/03/2015 11:17 ...	Microsoft Word D...	0 KB
Guidance on Shared Drives v1.1	09/03/2015 11:17 ...	Microsoft Word D...	0 KB
Guidance on Shared Drives v1.2	09/03/2015 11:17 ...	Microsoft Word D...	0 KB
Guidance on Shared Drives v2.0	09/03/2015 11:17 ...	Microsoft Word D...	0 KB

20. Setting documents as read-only prevents users from editing earlier drafts. This can be done by right clicking on the document and selecting the read-only option as shown in Figure 4. This can also be done for folders as shown in Figure 5.

Figure 4: Selecting read-only at the file level


Guidance on Shared Drives v1.0 Properties

Guidance on Shared Drives v1.0

Type of file: Microsoft Word Document (.docx)

Opens with: Microsoft Word

Location: C:\Users\Ian.Meldon\Desktop

Size: 0 bytes

Size on disk: 0 bytes

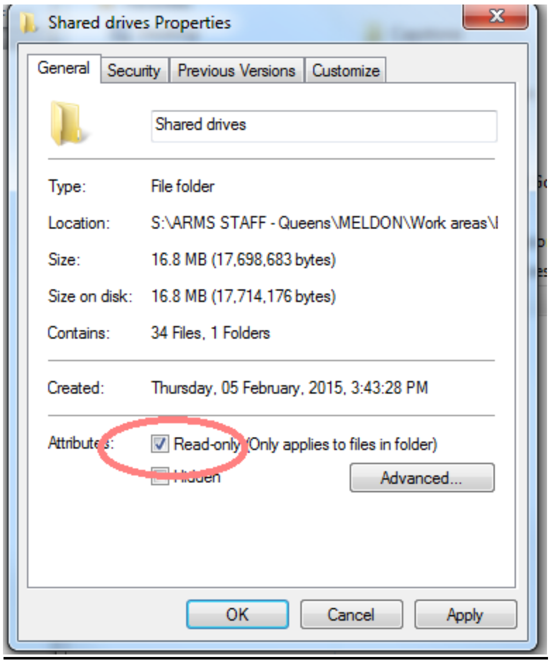
Created: Today, 10 March, 2015, 3:15:30 PM

Modified: Today, 10 March, 2015, 3:15:30 PM

Accessed: Today, 10 March, 2015, 3:15:30 PM

Attributes: ☑ Read-only □ Hidden

Figure 5: Selecting read-only at the folder level


Shared drives Properties

Shared drives

Type: File folder

Location: S:\ARMS STAFF - Queens\MELDON\Work areas\I

Size: 16.8 MB (17,698,683 bytes)

Size on disk: 16.8 MB (17,714,176 bytes)

Contains: 34 Files, 1 Folders

Created: Thursday, 05 February, 2015, 3:43:28 PM

Attributes: ☑ Read-only (Only applies to files in folder)
□ Hidden

H. Information security

21. In accordance with *ST/SGB/2007/6 Information sensitivity, classification and handling*, the guiding principle for classifying information - including that on shared drives - is based on the understanding that the work of the United Nations should be open and transparent. However, there will be situations where sensitive or confidential content can only be made available on a need-to-know basis; therefore it will be necessary to implement access controls to secure information.

22. Information management systems provide robust information security management, while only basic access controls can be set in shared drives. ST/SGB/2007/6 provides a framework for identifying and managing United Nations sensitive information, and there is extensive guidance on ARMS website to support this.

Setting access controls

23. Table 3 outlines all roles and responsibilities for information security and access administration.

Table 3: Information security and access administration

Role	Responsibilities
Head of Office	• Approves shared drive security and access rights plan • Accountable for ensuring access to sensitive information is controlled
IMO (or designated focal point)	• Responsible for the management of access controls and acts as a focal point for personnel • Consults with personnel to develop a plan for shared drive security and access controls • Configures and applies security and access controls
All Personnel	• Notifies the IMO or designated focal point of permission and access control requirements • Ensures information and records are correctly marked and filed in accordance with their sensitivity
OICT	• Accountable for ensuring access to sensitive information is controlled • Ensures security, sensitivity and access rights are applied to servers, software and systems used to manage shared drives • Ensures back-end access is on a need-to-know basis • Provides information on how shared drives are managed at the back end and, on a case-by-case basis, who has access
ARMS	• Provides advice on managing access to confidential or sensitive content, files or records, as determined by *ST/SGB/2007/6 Information sensitivity, classification and handling* and communicated in guidance on ARMS website

I. Managing retention

24. In accordance with *ST/SGB/2007/5 Record-keeping and the management of United Nations archives* offices are required to determine what records must be retained, deleted or archived according to a Records Retention Schedule. The Records Retention Schedule should be applied to all folders in shared drives. Non-records drafts, working files or content in the informal folder structure will have a short retention of maximum two years.

25. Retention should be managed in shared drives in order to:

- accountably dispose of records in a timely manner;
- reduce the volume of information and records stored;
- dispose of outdated, irrelevant or duplicate information or records; and,
- prepare for migration to another shared drive or more suitable system.

Applying a Records Retention Schedule

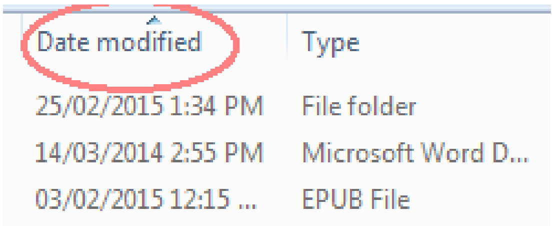
26. Retention can only be applied manually in shared drives; therefore roles and responsibilities must be assigned and followed. The Records Retention Schedule should be applied annually.

Table 4: Roles and responsibilities for applying a Records Retention Schedule

Role	**Responsibilities**
Head of Office	• Accountable for the implementation of the Records Retention Schedule • Supports the IMO or designated focal point in implementing the Records Retention Schedule
IMO (or designated focal point)	• Takes responsibility for the application of the Records Retention Schedule and acts as a focal point for personnel • Ensures the Records Retention Schedule is up-to-date • Plans the application of the Records Retention Schedule on an annual basis • Deletes information and records as per a Records Retention Schedule
All Personnel	• Files United Nations records in the formal records folder structure so retention can be easily applied
ARMS	• Approves Records Retention Schedules in compliance with Organization-wide requirements

27. To identify time-expired and redundant information when applying a Records Retention Schedule, or during a clean-up, information and records can be sorted within folders by when they were last modified. This can be done by clicking the “date modified” column in any folder in Windows Explorer as shown in Figure 6.

Figure 6: Sorting by date modified



Date modified	Type
25/02/2015 1:34 PM	File folder
14/03/2014 2:55 PM	Microsoft Word D...
03/02/2015 12:15 ...	EPUB File

Shared drive clean-up

28. A shared drive clean-up will enable the one-off deletion of duplicate and redundant information and non-record drafts. A shared drive clean-up campaign should be done:

- the first time these Guidelines are applied to an unmanaged shared drive;
- immediately prior to restructuring a shared drive, typically when implementing a new File Classification Scheme;
- before implementing a new Records Retention Schedule; and
- prior to migrating records or information to more suitable systems.

29. Signs of where content may need to be moved to the formal records folder structure or can be deleted as per a Records Retention schedule, include:

- folders named after or created by personnel who have left or moved to other Offices; and
- folders relating to closed projects or completed tasks.

30. All personnel have a role in a shared drive clean-up. For example, individuals are responsible for cleaning-up and moving records from their own folders in informal folder structures, the IMO, or designated focal point should develop and implement a clean-up plan for formal records folder structures containing records. Table 5 shows typical roles and responsibilities for the clean-up process.

Table 5: Roles and responsibilities for a shared drive clean-up

Role	Responsibilities
Head of Office	• Supports the clean-up initiative and the IMO or designated focal point in planning, announcing and implementing a clean-up • Approves and signs-off on clean-up plans • Ensures that a clean-up occurs at least every year
IMO (or designated focal point)	• Manages the shared drive clean-up • Develops a clean-up plan and oversees its implementation • Acts as a focal point for personnel
All Personnel	• Identifies records stored in the informal folder structure and moves them to an appropriate place in the formal records folder structure • Delete duplicate, unneeded, or outdated personal content

31. The clean-up plan developed by the IMO or designated focal point will typically include:

    - a review of existing File Classification Scheme(s) or Records Retention Schedule or the development of new ones;
    - notifying personnel of the clean-up plan including the rationale behind it, benefits, plan and their roles;
    - discussing information and records currently stored on shared drives with personnel;
    - ensuring records not duplicated elsewhere are moved to the formal records folder structure;
    - deleting outdated, irrelevant or duplicate information or records as per input from all personnel and the Retention Schedule. This should ideally be done at the folder level; and,
    - cleaning-up content from personnel who have left or moved to other offices, as well as content relating to closed projects or completed tasks.

J. Preparing for a migration to other systems

32. Moving records or information from one system to another while maintaining their authenticity, integrity, reliability and usability is referred to as *migration.* Migration from a shared drive should only be done after a clean-up or the application of a Record Retention Schedule, and to a more suitable enterprise system. As content must be first cleaned-up and volume reduced, migrating everything should never be considered an option. There are two ways to approach a migration:

    - migrate content based on its value, for example, the last two years or substantive records only; and,
    - migrate nothing and take a day-forward approach, typically by cleaning-up the shared drive, setting it to read-only and requiring personnel to file into the new system after a chosen date.

33. A migration plan should outline the approach taken and rationale behind the approach. It should be developed, communicated and implemented by the IMO or designated focal point with the approval of the Head of Office; it typically includes:

    - a shared drive clean-up and application of an approved Records Retention Schedule;
    - notifying all personnel of the migration and their role in the process;
    - reconfirming or developing a new access matrix to ensure continuity in the protection of sensitive materials and communicating this to personnel;
    - creating folder structures in the new system which reflect a File Classification scheme and in turn have an approved Records Retention Schedule applied to them;
    - deciding cut-off and migration dates, timescales for any read-only access, and a disposition date for old content if required (typically after around six months); and,
    - providing personnel with a mapping of the current shared drive to the new system.

Table 6: Roles and responsibilities for migration

Role	Responsibilities
Head of Office	• Supports the IMO or designated focal point and personnel in planning and implementing the migration • Signs-off on migration plans
IMO (or designated focal point)	• Manages the migration and acts as a focal point for personnel • Develops a clean-up plan, oversees its implementation and reports on progress • Acts as a focal point for personnel
All Personnel	• Deletes duplicate, unneeded, and outdated personal content • Identifies information and records for migration
OICT	• Provides technical support as required, especially when migrating to a new system

K. Other ARMS resources for managing United Nations records

34. There is extensive guidance on managing United Nations records on ARMS website

L. Definitions

35. The following definitions are applicable to these guidelines; a full records management glossary can be found on ARMS website

Disposition: A range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments. *International Standard ISO/TR15489-1, Clause 3.9*

File Classification Scheme: A system that describes standard categories and that is used to organise records with common characteristics. *ARMS Glossary of Recordkeeping Terms*

File Plan: A plan or scheme developed by an Office, Department or Organisation to organise and arrange different types of files. See *File Classification Scheme* above

Metadata: Data that describes data such as the context, content and structure of records and their management through time. *International Standard ISO/TR15489-1, Clause 3.12*

Migration: The act of moving information or records from one system, software configuration or technology to another while maintaining their authenticity, integrity, reliability and usability. *Glossary of Records Management Terms. National Archives of Australia, 2007*

Read-only: Documents that can be opened and viewed but not edited, e.g. saving changes. In other words, the document can only be read from, not written to.

Record:

i) Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. *ISO 15489-1:2001 Information and documentation - Records management*

ii) Any data or information, regardless of form or medium, maintained by the United Nations as evidence of a transaction *ST/SGB/2007/5 Record-keeping and the management of United Nations archives.*

Records Retention Schedule: A comprehensive instruction covering the disposition of records to ensure that they are retained for as long as necessary based on their administrative, fiscal, legal and historic value. *ARMS Glossary of Recordkeeping Terms*

Recordkeeping system: Information systems which capture maintain and provide access to records through time. *International Standard ISO/TR15489-1, Clause 3.17*

Shared drive: Shared drives, also known as network drives, or file shares, are typically used to store, access and share digital content such as documents, images, audio, video, spreadsheets, presentations, and databases. *NARA Bulletin 2012-02.*