Redundant Source Information

Replacing original "source" records with copies needs to be done right. This interpretation guide will help you:

- **work with your Records Officer to ensure the copies will serve your ministry's needs,**
- **determine what you need to do before destroying the originals,**
- **follow a defensible process as required in the Redundant Source Information Schedule (RSIS) when you replace originals with copies, and**
- **meet the Managing Government Information Policy (MGIP) requirements for ministries to copy or move records and data using formats that maintain their authenticity, are stable and accessible, and according to applicable standards.**

If you just need a basic overview or want to know whether you need to complete an RSIS defensible destruction form, see Redundant Source Information Quick Tips.

Contents

A.	What is Redundant Source Information (RSI)?	page 1
B.	When to Replace Originals with Copies	page 2
C.	Categories of Redundant Source Information	page 3
1.	Digital Communications	page 3
2.	Encrypted Records that have been Decrypted	page 4
3.	Migrated and Converted Information	page 4
4.	Digitized Information	page 5
D.	What is a Defensible Process?	page 6
E.	RSI Checklist	page 7

A. What Is Redundant Source Information (RSI)?

The term Redundant Source Information (RSI) covers original records and data that have been replaced by authoritative copies. You can only make this replacement after using a defensible process to ensure the copies are accurate, authentic, authorized, documented, and saved/filed in an appropriate system. Only then can you determine that the originals are no longer needed (i.e. the source information is redundant).

The requirements for replacing redundant source information with authoritative copies are established in the Redundant Source Information Schedule (RSIS). Authoritative copies have the following characteristics:

- they have been produced using a defensible process to ensure they are authentic, reliable, and usable;
- they provide evidence and historical proof of government actions and/or decisions; and
- they are managed in appropriate systems.

For digital communications and encrypted records that have been decrypted (categories 1 and 2) the defensible process is simple. Just save the information in an appropriate system according to ministry procedures. Make sure you follow naming conventions and don't lose relevant metadata along the way.

The defensible process is more involved for migrated and converted information and digitized information (categories 3 and 4). For these you will need to ensure you are authorized under applicable standards and guidance, including:

- the Migration Guide<under development>, and
- the Digitizing Government Information Standard and Guide.

See "What is a Defensible Process?" (Section D) to learn more.

B. When to Replace Originals with Copies

You need to replace originals when they cannot serve recordkeeping needs due to the limitations of their format and/or storage location. Some common examples that correspond with the four categories of redundant source information are when you need to:

1. copy email from a personal mailbox into a shared location (digital communications)
2. read and file encrypted records (encrypted records that have been decrypted)
3. move data to a new system (migrated and converted information)
4. file paper records in a digital system (digitized information)

See "Categories of Redundant Source Information" (Section C) to learn more.

Once you have made authoritative copies and filed them in an appropriate system, do you need to keep the source records? Most of the time this is unnecessary, but you may be required to retain some digitized information (category 4) in its original form to meet business, legal, audit, or archival requirements. Identifying any source information that does need to be kept is part of the process.

Some examples of source information that you may need to retain:

- the records have original signatures or other features that are needed for legal or archival reasons
- the records have been scheduled for full or selective retention in the government archives, and have not yet been assessed to determine if the copies would be adequate for this purpose
- the information is unscheduled and has not yet been assessed by a Government Records Service (GRS) archivist to determine its long-term value

The process of establishing a defensible process will lead to a final determination of whether the source information needs to be retained (see section D).

Source Information that is Not Redundant

Some source records cannot be replaced, even if your office has made digital copies that serve well for day to day operations. There may be a legal, archival, or other reason why the originals should be retained for a period of time or permanently. Check the applicable information schedule and be aware of relevant ministry policy before destroying originals.

Some specific examples of source information that is NOT redundant even after it has been digitized are:

- original paper birth registrations are fully retained [FR]) under the *Vital Statistical Services ORCS* (Schedule 163600, secondary 24070-30)
- original archaeological permit reports that are deemed unsuitable for copying are fully retained under the *Archaeology ORCS* (Schedule 170415, secondary 11150-25), while other similar reports may be destroyed after being digitized/microfilmed.

Find these schedules in the ORCS Library.

C. Categories of Redundant Source Information

1 Digital Communications

Government uses a variety of business applications to create and receive messages (e.g., Outlook, SharePoint, MS Teams, instant messaging). Most of these do not have adequate controls to ensure the messages are accessible and secure. Therefore, you need to copy any messages required to serve ongoing business needs into an appropriate system. For help, see:

- the Email Guide (see especially the "Saving Email Records Outside of Outlook" section under the Managing Your Email tab), and
- the Collaboration Tools Guide.

Examples of originals	Destroy them when you've confirmed that:
○ Emails ○ Instant messages ○ MS Teams messages ○ Social media messages ○ Text messages	The authoritative copies, including attachments, have been made, classified and filed in the appropriate system.

2 Encrypted Records that have been Decrypted

These are source records that are temporarily encrypted (i.e. transformed into an unreadable format) for secure transmission, or to restrict unauthorized access. Once sent or received, they are decrypted by a recipient with proper authorization, and the encrypted version is no longer needed. For further requirements relating to encryption of BC Government information, see the Information Security Policy and the Cryptographic Standards 6.10.

Examples of originals	Destroy them when you've confirmed that:
Messages and documents that are: ○ sent or received by government laptops, smartphones, or tablets ○ stored on portable media (e.g. thumb drives) ○ encrypted for other security purposes.	1. They have been properly decrypted and verified. 2. The decrypted authoritative copies have been filed in the appropriate system.

3 Migrated and Converted Information

This category covers data and other records that have been copied or moved (migrated) from one hardware or software configuration to another or converted from one file format to another.

As a government employee, you migrate information every time you save information into your office's appropriate recordkeeping system from the place it was created or received (e.g., H drive, OneDrive, SharePoint, MS Teams) and delete the original. Follow your ministry's procedures for saving information to your office recordkeeping system. For your purposes, the Collaboration Tools Guide is likely to be helpful.

Ministries may migrate or convert information:

- during a system upgrade,
- as part of a business process where data is routinely transferred from one system to another system that is used to process and/or store the data (e.g. in nightly batches), or
- for access, storage, or preservation purposes (e.g. moving long-term data to a format that meets preservation requirements).

See the **Migration Guide** <under development> for guidance on the processes of migrating and converting information.

This category excludes information that has been altered as this data constitutes a different record (because data or metadata has been removed or meaningfully changed). The intention in these cases is not to migrate or convert data, but to adapt it for a new purpose (e.g. merge it with other data for statistical or research uses).

Examples of originals	Destroy originals when you've confirmed that:
Data/records that have been: ○ copied to the latest format ○ moved to an upgraded system ○ routinely moved for processing or storage purposes	1. A complete, accurate copy of the data has been made and verified. 2. The authoritative copies of the data have been saved in an appropriate system. 3. The original data does not need to be kept to comply with an information schedule, legislation, or policy. 4. A defensible process is in place and has been followed (see Section D).

4 Digitized Information

Digitization is the process of making digital copies of physical records (e.g. paper, magnetic media, microfilm). Commonly, but not universally, the goal of this process is to replace the originals. The process of replacing original source records with digitized copies is governed by the Digitizing Government Information Standard and the Redundant Source Information Schedule.

To comply with policy requirements, you need to follow a defensible process.

If you are making copies of a few documents for a one-time/ad hoc purpose using your office Multi Function Device (MFD), use the How to Use the MFD to Digitize RM Guide and also follow any additional requirements established by your ministry. No formal sign-off process is required unless your ministry has put one in place.

If you are digitizing as a regular practice or for a specific project, you need to follow a process authorized by your Government Records Service Records Officer using the RSIS Defensible Destruction process form (available upon request). This includes:

- **Digitizing as part of a business process**: digitizing as part of a regular/ongoing ministry work process, such as managing incoming correspondence in both digital and physical formats, and
- **Legacy conversion project:** digitizing a set of older physical files so you can use them more easily as part of a digital workflows for an ongoing function (e.g. registering corporations or births), at the same time freeing up physical space in the office or in offsite storage.

To find out more about how to establish a defensible process, see the Digitizing Government Information Guide.

Examples of originals	Destroy them when you've confirmed that:
○ paper documents that have been scanned to create digital versions ○ microfilm that has been copied to a digital format ○ audiovisual recordings that have been digitized	1. Authoritative copies have been made and verified against the originals. 2. The authoritative copies have been saved in an appropriate system. 3. A defensible process is in place and has been followed (see next section).

D. What is a Defensible Process?

A defensible process for replacing redundant source information with authoritative copies needs to have the following features to comply with the *Redundant Source Information Schedule*:

- the copying process complies with relevant requirements and standards (see previous section to find out about requirements relevant to your copying project)
- authoritative copies have been created and filed in an appropriate system
- requirements in applicable information schedules have been addressed
- where authorization is required:

- for migration/conversion: the process established by the ministry IMB or equivalent has been followed and documented, or
- for digitization: the destruction has been authorized using the RSIS Defensible Destruction form (available upon request from your Government Records Officer; note that for previously unscheduled information and any records designated for full or selective retention, you will need to provide additional information, and a GRS archivist's review may be required to ensure no valuable original records are destroyed).

E. RSI Checklist

Checklist for Meeting RSIS Requirements	Done
1. Created authoritative copies (see Sections A and B)	
2. Filed authoritative copies in appropriate system (see Section A)	
3. Confirmed the applicable defensible process requirements and determined if authorization is needed in consultation with your Records Officer (see Section C)	
4. If authorization is needed, submitted the RSIS Defensible Destruction form to your Records Officer for authorization.	
5. Filed completed form under ARCS 432-30 or 432-35 as appropriate	
6. Destroyed source records (i.e. originals) in accordance with government policy and ministry protocols	

Additional Information

Contact your Records Officer and check out the other RM Guides.