RECORDED INFORMATION MANAGEMENT MANUAL

Government Records Service	RIM Number: RIM 503
Province of British Columbia	Approval Date: 2015/04/22
Policy: RECORDS TRANSFER WITHIN GOVERNMENT **Specifications:** RIM 503A *Specifications for Documenting Legal Custodians*	
AUTHORITY From ***Core Policy and Procedures Manual*, 12.3.3 Part III: Managing Information, Objectives:** • Assign responsibility and accountability for the management of information within the custody, or under the control of, government.	
Security Classification: PUBLIC	

1. SCOPE

This policy establishes the responsibilities, requirements and conditions for appropriate, secure transfer of government records within government.

1.1 Authority

- *Document Disposal Act (DDA)* (RSBC 1996, c. 99)
- *Core Policy and Procedures Manual (CPPM)*, c.12

1.2 Applicability

Ministries, agencies, boards, commissions, and Crown corporations covered by the *Document Disposal Act* (hereafter "DDA agencies").

2. POLICY

This policy establishes the requirements for appropriate transfer of government records when their ownership is transferred within or into government, as a result of reorganization, the ending of functions or programs, or when government inherits records from an agency not covered by the *Document Disposal Act*.

Transfer of **government records** must be authorized, managed, and documented appropriately (i.e., in accordance with this policy, related specifications and guides, and internal ministry/agency procedures), and with due regard for any existing access, confidentiality, and security provisions that apply to the records.

2.1 Conditions for Transferring Records Within or Into Government

Legal custody of records may be transferred within government under one of the following conditions:

2.1.1. Reorganization: When functions/programs and the records that document them are transferred to another office, program area, ministry or an agency covered by the *Document Disposal Act*.

2.1.2. Defunct or completed programs: When a function or program ends, and the relevant authorities identify a ministry or DDA agency to take custody of its records.

2.1.3. Transfer of programs and/or records from an agency not covered by the *DDA*: When the originating agency was not covered by the *Act*, and its functions and programs are transferred to a ministry or DDA agency; or when the agency becomes defunct and government assigns responsibility for its records to a ministry or DDA agency.

For transfers that do not meet these conditions, see the relevant policy:

- *Records Transfer to the Government Archives* (RIM 502), or
- *Records Transfer Outside of Government* (RIM 504).

2.2 Principles for Transferring Records Within or Into Government

When transfers happen, the integrity of the records needs to be maintained to protect their value for supporting services to citizens.

The following principles apply to all transfers of government records within or into government ministries and agencies covered by the *DDA*:

Principle I **Records follow function.** When legal custody of a program is transferred, associated operational and administrative records also must be transferred[1]. This includes:

a) Both **digital** and physical records.

b) Records that are managed in the office (onsite) and those that are stored in offsite records storage facilities.

c) Scheduled and unscheduled records (i.e., records with and without approved **records schedules**).

d) Records in the office **recordkeeping system** (maintained in EDRMS TRIM, on the LAN/fileshare, or in another shared location) as well as all other

[1] Normally all records are transferred, but exceptions are sometimes made, e.g., for offsite records or when documents are so integrated into the files and recordkeeping system of the original ministry/agency that information would be lost if they were moved.

records created and received as part of the function or program being transferred (e.g., documents in email folders, SharePoint sites, digital systems, websites, and mobile storage devices).

e) Records at all stages in the **life cycle** (**active**, **semi-active**, and **inactive**).

Principle II **Records integrity must be protected**. To achieve this requires the following:

a) The transfer process must maintain the security, **authenticity**, and **reliability** of the records.

b) The records must remain **accessible** to those who need to use them. This includes not only the inheriting office, program area, ministry, or agency but, in many cases, relevant staff of the transferring office/program area/ ministry/agency[2], due to residual accountabilities and responsibilities. In addition, appropriate public access in accordance with the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*) (RSBC 1996, c. 165) must continue to be available.

c) The chain of custody must be recorded. For the purpose of preserving the security and integrity of records throughout their existence, and for management, accountability, and historical purposes, government needs documentation of records creators and custodians over time (i.e., a historical map). See 2.3 for details.

Principle III **Records must be managed in accordance with schedules.**

a) **Inactive records** should be processed appropriately, in consultation with the receiving agency. This means that those eligible for onsite **destruction** may, as a practical measure, be destroyed instead of being transferred to the receiving agency. Inactive physical records scheduled for **selective** or **full retention** by the government archives should be transferred to storage managed by Government Records Service (GRS) (i.e., approved offsite records storage facilities), if this has not already been done. The scheduled disposition will be administered by GRS.

b) The inheriting ministry or agency may continue to use the relevant approved *Operational Records Classification Schedule* (***ORCS*** or other **ongoing records schedule**), even if this means that more than one ministry or agency will be using the schedule at the same time[3].

Principle IV **Records must have an identified legal custodian.** There must always be a legal custodian (or "business owner") identified for records; i.e., the ministry or agency body responsible for the ongoing maintenance, security and

[2] Please note that records in offsite storage must have only one current legal custodian, but multiple agencies may share access to a given accession (i.e., a specific set of records).

[3] The transferring and/or inheriting agencies may ask their Records Officers to arrange for any amendments to relevant *ORCS* or other operational records schedules that may be needed.

accessibility of the records, and the associated costs. This information needs to remain current and be updated as required during records transfers. See 2.3.2 below.

When ministries and agencies transfer or receive government records, they need to establish protocol agreements that are consistent with these four principles.

2.3 Documenting Transfers

Maintaining current information about the data, documents, files, and boxes in the legal custody of a ministry or agency is integral to managing the records. The following documentation is required to protect the integrity of the records.

2.3.1 Records Managed via Ministry/Agency Systems

Transferring agencies need to document for receiving agencies the following information about records managed by in-house ministry or agency systems[4] (i.e., LAN/fileshare or other recordkeeping system, email folders, websites, SharePoint sites, and any other in-house systems):

a) **Recordkeeping system information**: Records and information need to be identified with titles, dates, and other relevant **metadata**.

b) **Records management information**: Provide all relevant documentation concerning:

- records schedules (both approved and draft),
- work process documentation (e.g., in-house policies and procedures), and
- administration of the records (i.e., records classified under *Administrative Records Classification System* (***ARCS***) primary 432 Records Management, especially the *ARCS* 432-20 accession files that document offsite records).

c) **Other relevant information**: Examples include:

- Access restrictions – such as security classifications and restrictions related to *FOIPPA*,
- Litigation underway or anticipated,
- **Electronic systems** used to store relevant data and records – including in-house systems, systems managed by service providers, and systems shared with other government ministries/agencies, and
- Intellectual property rights contained in the records (such as patents or copyright).

[4] For the purposes of this policy, records systems managed in-house include those managed by service providers other than GRS, whether the providers are within government (e.g., CAS) or contractors.

The transferring agency should also retain documentation of all records that were transferred, the receiving agency, and the date of transfer (filed under *ARCS* secondary 432-25 Custody management case files).

2.3.2 Records Managed via GRS-Administered Systems

(i.e., EDRMS TRIM, CRMS, approved offsite storage facilities)

Ministries and agencies must provide GRS with timely, accurate information about organizational changes and resulting records transfers so that GRS is able to provide any required support services or make updates to records control information. This is essential for those records maintained using GRS systems. The information provided enables GRS to:

- correctly assign **current legal custodian** responsibilities to records,
- track previous offices/agencies responsible for the records over time (i.e., the **creating agency**, the **transferring agency**, and the previous legal custodian), and
- ensure that costs are assigned to the appropriate ministry/agency/office.

Ministries and agencies need to provide GRS with information about new and previous office titles, reporting structures, dates for the changes, and related details.

For further guidance, see RIM 503A *Specifications for Documenting Legal Custodians.*

3. ROLES AND RESPONSIBILITIES

3.1. Government Records Service (GRS)

GRS is responsible for

- establishing policy governing records transfers,
- maintaining and updating records custody metadata in GRS-administered systems (i.e., **EDRMS** TRIM and ARIS, the GRS database used to track records in offsite storage facilities), based on information received from ministries and agencies, and
- maintaining documentation of government records creators and their place in the organizational hierarchy over time.

3.2. Ministries and Agencies

The ministries/agencies involved in transferring a function or program are responsible for maintaining the integrity of the relevant records by:

- establishing protocol agreements,
- identifying records for transfer,
- transferring the records and documentation of them,

- providing GRS with the information necessary to update its systems, and
- generally ensuring that records are transferred in accordance with the principles stated in this policy.

RELATED POLICIES AND SPECIFICATIONS

The following specifications are founded upon this policy:

RIM 503A *Specifications for Documenting Legal Custodians*

Policies and specifications that closely relate to this policy include:

RIM 422 *Preparation of Records for Offsite Storage*

RIM 501 *Records Destruction*

RIM 502 *Records Transfer to the Government Archives*

RIM 504 *Records Transfer Outside of Government*

RELATED GUIDES– see RM Guides and Online Training Modules

n/a

Revision History: First approved: 2015/04/22 Revised: n/a

This policy area was not formerly addressed within RIM.

In the IM/IT Supplement 2007 (policy supplement to CPPM formerly posted by IM/IT Governance Branch of the Office of the Government CIO), this was covered under 12.3.3 III (a) I. *Identification and Management of Government Records, Physical and Legal Custody of Government Records.*

Index and Glossary Terms – see ***RIM Glossary*** for definitions of terms that appear in bold blue text (for the first usage of each term in the policy, as well as below)

Active records	**Electronic system**	***ORCS***
ARCS	**Full retention**	**Recordkeeping system**
Authenticity	**Government records**	**Records schedule**
Creating agency	**Inactive records**	**Reliability**
Current legal custodian	**Intellectual property rights**	Reorganization
Defunct programs	**Legal custody**	**Selective retention**
Destruction of records	**Life cycle**	**Semi-active records**
Digital records	**Metadata**	**Transferring agency**
EDRMS	**Ongoing records schedule**	