

**Province of British Columbia**

# **Guidelines to the Core Administrative and Descriptive Metadata Standard**

**Version 1.0.2**

**November 3, 2023**

## Table of Contents

Guidelines to the Core Administrative and Descriptive Metadata Standard .....	i
1. Purpose .....	3
2. Application .....	3
3. Advice on these guidelines.....	3
4. About the Standard.....	3
Why do we need a standard?.....	4
Guidance for each element.....	5
5. Implementation .....	12
Metadata Application Profiles .....	12
Recommended implementation steps.....	13
6. DEFINITIONS.....	17
7. Resources .....	19
Policy and Information.....	19
Learning and Best Practices .....	19
REVISION HISTORY .....	19

## 1. Purpose

These Guidelines are intended to be read in conjunction with the Core Administrative and Descriptive [Metadata](#) Standard (hereafter “the Standard”), provide background on the Standard, elaborate on the meaning and usage of the core [metadata elements](#), and provide additional information and resources for implementing the standard. For any discrepancies between the Standard and these Guidelines, the Standard is the authoritative document.

## 2. Application

All entities (hereafter, “ministries”) identified in [Core Policy and Procedures Manual Chapter 1, section 1.2.4](#).

## 3. Advice on these guidelines

For questions or comments regarding these Guidelines, please contact:

BC Data Service Division  
Ministry of Citizens’ Services  
[Data Systems and Services Client Hub](#)

## 4. About the Standard

The Standard is based upon the Dublin Core Metadata Element Set defined in ISO 15836. It specifies nine core metadata elements that should be adapted and incorporated into metadata that is currently in use in systems that manage digital government information.

The core metadata elements can be applied at different levels, including:

- entire systems (e.g., transactional systems where all the information have the same management requirements).
- groupings of information (e.g., tables in a database or folders in a document and records management system, such as the [Electronic Document and Records Management System](#) (EDRMS Content Manager).
- individual [digital records](#) or [datasets](#).

All the above are collectively referred to as [information resources](#).

The core metadata elements are:

- Creator
- Date created
- Date modified
- Description
- File format
- Information schedule
- Security classification
- Title
- Unique identifier

The core elements set may be extended with additional elements to meet specific business needs.

### **Why do we need a standard?**

The standard sets a consistent approach to metadata to realize the following outcomes:

1. Trusted and reliable information
  - Legislation and policy require that government information be reliable and trustworthy, to support the day-to-day business and provide evidence of the business of government today and in the future. Metadata helps keep information reliable and trustworthy.
  - Metadata should be appropriately configured and carried forward through system changes to maintain its trusted and reliable characteristics.
2. Findable information
  - The ability to find the correct information depends on metadata. Titles, subjects, tags, and keywords are all metadata for searching and discovery.
  - Standardized metadata helps to facilitate specific searches that can target relevant categories rather than searching across all metadata.
3. Information sharing, reuse, and interoperability
  - Environments for shared data rely on clear and consistent metadata structures that enable management and retrieval across diverse systems.
  - Standardized metadata is essential for interoperability, that is a key enabler of information exchange, seamless system migrations, collaborative business processes and the maintenance of information context and understandability.
4. Security and privacy
  - Metadata can be used to identify information requiring enhanced security or privacy protections.

- In information sharing contexts, metadata provides documentation of the information shared and the ability to identify unauthorized disclosures quickly.
5. Information preservation
- Metadata can be used as a tool to proactively plan for and perform on-going information accessibility and preservation activities such as migration.
  - It can document software and hardware dependencies and helps to manage the vulnerabilities which occur when technology changes.
  - It can also be used to tag information that are in vulnerable or unusual formats that may require specific management to be accessible or useable.
6. Automated classification and disposition
- Metadata can be used to automate the classification and disposition of information, by encoding information management policies into content systems management (e.g., SharePoint).
  - Workflow metadata can support such automated functions and system changes.

## Guidance for each element

### *ELEMENT: CREATOR*

Guidance:	<ul style="list-style-type: none"> <li>• Consider the appropriate organization level (e.g., ministry, branch, team, person) and document its official name (avoid abbreviations and acronyms). Follow other naming conventions and standards to ensure consistency with other metadata for the same Creator.</li> <li>• Establish naming conventions for the consistent capture of Creator information. Avoid use of acronyms or codes, unless these are linked to an authoritative, stable source such as a glossary or explanatory note.</li> <li>• Do not repeat Creator to add additional information. All information about a single Creator should be included in one occurrence or recorded in other metadata properties. If a dataset or publication has more than one Creator, separate them using a defined syntax.</li> </ul>
Examples:	<ul style="list-style-type: none"> <li>• Possible values include names, position, role, Ministry/Office Name, and/or system.</li> <li>• Database system to manage client information. Creator: British Columbia Children and Youth Services; British Columbia Health and Wellness.</li> </ul>

	<ul style="list-style-type: none"> <li>• A government body licenses a third-party resource for BC, e.g., from Statistics Canada or an independent research agency, and makes it available via Data BC. Creator: Statistics Canada.</li> <li>• Dataset of vegetation inventory polygon. Creator: identifier of person who created the data.</li> </ul>
Do not confuse with:	<ul style="list-style-type: none"> <li>• <a href="#">Office of Primary Responsibility (OPR)</a> – identifies those responsible for the management of a government record</li> <li>• Custodian - the person who:           <ul style="list-style-type: none"> <li>o protects and promotes the use of data holdings assigned to them</li> <li>o sets policies, and is accountable for defining the appropriate use of the data</li> <li>o is provider of the authoritative version of the data</li> <li>o is ultimately accountable for issues related to definition, collection, management, and authorised use of the data</li> </ul> </li> <li>• Contributor - contributes to the content of a resource.</li> </ul>

#### *ELEMENT: DATE CREATED*

Guidance:	<ul style="list-style-type: none"> <li>• Systems generally record the dates and times of actions automatically, but some circumstances could require manual entry. Also, systems tend to identify the 'Date Created' of a resource as the date on which it is captured into a repository. The actual creation of a resource and its capture frequently take place on the same date, but this is not always the case (e.g. disseminating a resource sometime after its 'Date Created'; moving content and metadata from one repository to another; and migrating resources to a different hardware and/or software environment).</li> <li>• Capture an accurate Date Created, or a proxy of that date, when bringing existing resources, and/or their metadata into a repository, according to the level of risk and the value associated with those resources. This date could be system-generated or entered manually, depending on the volume and type of resources, the business requirements, and the capabilities of the destination repository.</li> </ul>
-----------	--

Examples:	<ul style="list-style-type: none"> <li>• A dataset compiled in April 2015 published on July 2015 (DATE CREATED is 2015-04)</li> <li>• A report completed in September 2015 but publicly released in January 2016 (DATE CREATED is 2015-09)</li> <li>• A resource created in 2011 is imported into a content management system in 2015. The system automatically generates the Date Created for the resource as 2015-10-25T 10:27:33. This would be the date modified. Another field captures the actual Date Created in 2011</li> <li>• A resource description is created in a content management system which automatically captures the date and time created</li> </ul>
Do not confuse with:	<ul style="list-style-type: none"> <li>• Temporal Coverage - refers to the period of time spanned by the information held in the resource</li> <li>• The date generated by a system upon capture of a resource into a repository</li> </ul>

#### *ELEMENT: DATE MODIFIED*

Guidance:	<ul style="list-style-type: none"> <li>• Systems generally record the dates and times of actions automatically, but some circumstances could require manual entry</li> <li>• Where possible, use a standard syntax both for recording and displaying dates and times, from the largest unit to the smallest unit such as "YYYY-MM-DD"</li> <li>• Date Modified is closely related to the business practices for version control</li> <li>• Ministries should determine which kinds of changes they need to track, and which ones they consider to be Minor and Major revisions</li> <li>• Minor revisions that don't significantly alter the content or that a Ministry does not need to track usually lead to a Date Modified. The revised item completely replaces the previous item and has both the original Date Created and a Date Modified</li> <li>• Major revisions that substantially change the presentation, structure, or content of an item, or require tracking for a period usually result in a new version of an item, with its own set of metadata including a new Date Created</li> </ul>
Examples:	<ul style="list-style-type: none"> <li>• A resource description is changed and is saved as the same version, i.e., replacing the previous version. The date generated automatically by a system may be considered the date modified</li> </ul>

	<ul style="list-style-type: none"> <li>The resource is updated with a 'minor' revision after import, and the revised version replaces the previous resource</li> </ul>
Do not confuse with:	<ul style="list-style-type: none"> <li>Date Created - the date on which an information resource is created or compiled.</li> </ul>

#### *ELEMENT: DESCRIPTION*

Guidance:	<ul style="list-style-type: none"> <li>May include but is not limited to, an abstract, a table of contents, a graphical representation, or a free-text account of the information resource.</li> <li>A description should consist of complete sentences, written in an easily understandable manner. Do not simply repeat the Title in the Description field. It could include:             <ul style="list-style-type: none"> <li>Purpose and function of an electronic information resource</li> <li>What the electronic information resource is or what it measures</li> <li>Potential uses for the data</li> <li>Policy areas or services described by the resource</li> </ul> </li> <li>Descriptions may not be necessary if the title, information schedule, or other information provide enough context to the content of the information resource.</li> </ul>
Do not confuse with:	<ul style="list-style-type: none"> <li><a href="#">Descriptive metadata</a> expressed by other specific elements, including Abstract, Risk Considerations, or Usage Considerations.</li> <li>Abstract - although not a core content element, is a brief statement about the content of an electronic information resource typically displayed with the Title to support search results for example.</li> <li>Risk Considerations - although not core content element, describe factors limiting the distribution of an electronic information resource.</li> <li>Usage Considerations - refer to conditions affecting the interpretation and use of an electronic information resource.</li> </ul>

#### *ELEMENT: FORMAT*

Guidance:	<ul style="list-style-type: none"> <li>A resource with identical or near-identical intellectual content may have multiple formats. For example, a dataset of farmers markets may be made available for download in various formats such as a single file (e.g., CSV), or may be made available to developers</li> </ul>
-----------	---



	<p>through a Web API, such that a computer program could use a Postal Code to retrieve a list of farmers markets in the Postal Code area.</p> <ul style="list-style-type: none"> <li>• Use a controlled vocabulary such as those expressed in PRONOM technical registry maintained by The National Archives (TNA) of the United Kingdom.</li> </ul>
Do not confuse with:	<ul style="list-style-type: none"> <li>• Availability: used when the described resource is available in another digital format through another government or non-government source.</li> <li>• Type: describes the business structure of the content of a resource, e.g., Agenda, Contract, News release, Dataset, Service description.</li> </ul>

#### *ELEMENT: INFORMATION SCHEDULE*

Guidance:	<ul style="list-style-type: none"> <li>• See ministry specific guidance on which schedules apply to your business area. For more information on information schedules, see the <a href="#">ARCS and ORCS User Guide</a> or contact <a href="#">Government Records Service</a></li> <li>• Assign an information schedule number as early as possible in the information lifecycle</li> <li>• If there does not appear to be an existing relevant schedule confirm this with your Records Officer to ensure this gap is identified, and add a “pending” note to this field</li> <li>• Best practice is to apply this element at the file or folder level to facilitate the disposition of groups of records of the same classification (e.g., tables or fields in a database, folders in a LAN drive, SharePoint site, or EDRMS).</li> <li>• Your ORCS system section will be particularly useful in determining the information schedule applicable to information in operational systems.</li> </ul>
Examples:	<ul style="list-style-type: none"> <li>• ‘ARCS 105-02’ used for <a href="#">Organization charts and organization histories</a></li> <li>• ‘ARCS 6820-20’ used for <a href="#">Information system maintenance records</a></li> <li>• ‘ARES 77000-02’ used for <a href="#">Real Estate Services – Appraisal cycle files</a></li> <li>• ‘201306 24000-04’ used for <a href="#">Global education program issue files</a></li> </ul>

**ELEMENT: SECURITY CLASSIFICATION**

Guidance:	<ul style="list-style-type: none"> <li>• Follow the <a href="#">Information Security Classification Standard</a>.</li> <li>• Business areas should develop a consistent internal process to assess and implement security classification.</li> </ul>
-----------	--

**ELEMENT: TITLE**

Guidance:	<ul style="list-style-type: none"> <li>• Create a brief and meaningful title to convey its topic or purpose           <ul style="list-style-type: none"> <li>○ When possible, use the title as it appears in the content of the described information resource. Use the most full and complete name of the resource.</li> <li>○ Review automatically generated titles to ensure they are concise and meaningful.</li> </ul> </li> <li>• Place important words at or near the beginning of the title</li> <li>• Include variables in the Title, such as geography, population subset, and/or reference period (as appropriate).</li> <li>• If a dataset is issued periodically, include a version indicator such a release, update or issue number, code, or phrase.</li> <li>• Minimize the use of abbreviations and acronyms.</li> <li>• Do not duplicate information found in other metadata elements (name of creator, date of creation).</li> <li>• Add values to a title such as a version number, status, or version date if a resource is one of many with the same or similar titles. Titles should be entered in sentence case. Only the first word and proper nouns should be capitalized.</li> <li>• Separate titles and subtitles by a hyphen preceded and followed by a space.</li> </ul>
Examples:	<ul style="list-style-type: none"> <li>• “Core Administrative and Descriptive Metadata Standard”.</li> <li>• A table or Column name.</li> <li>• A web page title.</li> </ul>
Do not confuse with:	<ul style="list-style-type: none"> <li>• Unique Identifier - a unique number, code, or reference value assigned to an information resource within a given context.</li> <li>• A digital file name for an electronic resource such as a web page or document, for example, ‘https://gww.gov.bc.ca/’ or ‘specifications.xlsx’ or ‘metadata_2008.docx’.</li> <li>• The subject line in an email.</li> </ul>

*ELEMENT: UNIQUE IDENTIFIER*

<p>Guidance:</p>	<ul style="list-style-type: none"> <li>• Identify the information resource by means of a string conforming to a formal identification system or a unique and stable natural identifier or a combination of attributes that create a natural identifier that has business meaning           <ul style="list-style-type: none"> <li>○ Examples of formal identification systems: <a href="#">Universal Unique Identifier</a> (UUID), and <a href="#">Standard Book Number</a> (ISBN)</li> <li>○ Examples of natural identifiers: Biogeoclimatic Zone; Client (identified by first name, last name and phone number)</li> </ul> </li> <li>• Every electronic resource should have a system-generated number or code that identifies it from the point of creation or capture and is fixed throughout the life of that resource           <ul style="list-style-type: none"> <li>○ Systems use different terms for Identifiers, both system-generated and process/business area/manual assigned identifiers, and different methods to generate them</li> <li>○ Some identifiers might not be unique across multiple applications, e.g., 'BC-100' could identify a map, a report, and a dataset even though each one is unambiguous within its own context</li> </ul> </li> <li>• Identifiers for electronic information resources may be assigned sequentially or based on the topic/content of the information resources</li> <li>• Title should not be used as an Identifier for an electronic information resource because it is not necessarily unique or linguistically neutral</li> </ul>
<p>Examples:</p>	<ul style="list-style-type: none"> <li>• Universal Unique Identifier (UUID)</li> <li>• Bibliographic call numbers and other shelf locator codes</li> <li>• Numbers or other codes for maps, plans, forms and brochures</li> <li>• Class, folder, and records schedule numbers in a records management system</li> <li>• Geographic locations</li> <li>• Ministry identification codes</li> <li>• Bar coding or other item tagging schemes</li> </ul>

Do not confuse with:	<ul style="list-style-type: none"><li>• Title - the official name by which a dataset or publication is known</li></ul>
----------------------	--

## 5. Implementation

Ministries may wish to prioritize implementing the standard on [critical information](#). Timing for implementation will depend on business needs but ideally will occur during key phases in the information systems lifecycle:

- design
- procurement
- selection
- configuration
- implementation
- service agreement updates
- upgrade
- migration
- decommissioning

### Metadata Application Profiles

Ministries are encouraged to create a Metadata Application Profile (MAP). The MAP defines the metadata for a business area, and provides the business rules, guidance, and best practices for use. For example, see the [Government of Canada Open Government Metadata Application Profile](#). A comprehensive MAP should document the element obligations, constraints, definitions, [encoding schemes](#), vocabularies, data model and [metadata schemas](#), as well as provide examples to assist in the understanding of the elements.

Key criteria for a MAP:

- Expresses all the mandatory elements
- Evaluation of elements that are “Mandatory if Applicable”. Where applicable, these elements also become mandatory
- Include source references. Business areas may rename elements (assign an alias name) but should reference the source for continuity.

A good source for mandatory elements is [Dublin Core](#). Ministries may review the suggested qualifiers, add any that are relevant and develop additional guidance for the specific context.

The MAP can be based on:

1. Direct Application of the standard, including all core elements. Each element must be evaluated to determine its applicability (e.g. if a metadata element is Mandatory if Applicable [MA] but is not applicable, it is no longer required to be used). Business areas may develop additional learning/training documents related to the specific information need.
2. Revised or new metadata profile based on a specific business function, in alignment with the standard.

Where metadata schemas involve concepts that are the same or like those in the standard, it may be useful to map properties across profiles for consistency and interoperability.

## Recommended implementation steps



### Identify information systems

- Survey the systems that are used to create and store government information within your business area, including enterprise systems (databases, LAN drives, SharePoint, EDMRS, intranet, internet, etc.) and line of business IM/IT systems (databases, case management systems, cloud-based systems, etc.).
- List relevant systems. Identify who is responsible for managing the systems (i.e., system administrator / architect / developer) and who is responsible for managing the information in them (i.e., head of the work unit / program area / information owner / custodian).
- Discuss with the system administrator opportunities to add metadata elements, configurations, and rules during the next system upgrade.
- Identify the information

- Use data inventories and systems documentation to identify document and describe the data in the systems.
- Where possible, use your [ARCS and ORCS](#) and other ministry records management documentation to identify the information that are captured and/or stored in the systems. Your ORCS systems section will be particularly useful for understanding the information records series that exist in operational systems.
- Other resources include Personal Information Registries, [PIAs](#), [STRAs](#), and internal information management and business continuity documentation.

#### Identify existing metadata

- What metadata is currently captured?
- Where metadata exists:
  - Where is it captured (e.g., in a database system, embedded in the digital object, elsewhere like a data registry or repository)?
  - Is there a metadata application profile (MAP)? If so, what does it include?
  - What levels of aggregation does it capture (e.g., data point, record, file, folder, system)?
  - Is the metadata schema easy to understand and apply?
  - What metadata is automatically captured?
  - What metadata needs to be manually added?

#### Evaluate existing metadata

- Which elements of the standard are captured?
- Which elements are not captured?
- Consider creating a [metadata crosswalk](#) or mapping to show equivalent elements across schemas. Crosswalks enable consistency and interoperability between metadata schemas and support metadata collection and information exchange.

#### Review/determine where the metadata will be captured and stored

- Decide on the system. Where a schema already exists, is the existing system the most appropriate location to capture and store the metadata? What other options exist?
- Confirm the appropriate level of information resource to apply the metadata. For example, metadata about records can be applied to:

- Individual records. This might include dates, titles, creator, and unique identifiers for each individual record in your system (e.g., documents in a case management system).
- Groups of records. An [Information Schedule](#) may be applied to files or folders to facilitate the disposition of records (e.g., in a LAN drive, SharePoint site, or EDRMS instance). Metadata may also be used to apply a security classification to a database table or column.
- Systems. Metadata may be used to apply access or retention rules to an entire system containing strict data types (e.g., a personnel or finance system).
- Determine how the metadata will be captured. It may be embedded within the information resource itself, and many common file formats enable metadata to be automatically captured.
  - For files stored on shared networks, it may be useful to manually capture metadata in the file properties, such that the metadata moves with the file, can be easily collected, and retains the link to the source data. This may involve effort to determine required fields and a process to manage metadata collection and maintenance.
- Determine where the metadata will be stored.
  - Metadata can be maintained separately and linked to the information resource (e.g., using a metadata crosswalk).
  - Metadata registries combine metadata for multiple information resources into a single spreadsheet or database, providing flexibility in selecting, searching, and changing the metadata schema.
  - Data stores, repositories and content management systems combine a specialised system for metadata capture and storage with file storage systems. Many systems are pre-configured with one or more metadata schemas, are searchable and customizable, and accept multiple formats. Multiple options are available, from free or open source to large commercial systems. The government standard is the EDRMS Content Manager.

#### Develop a plan for metadata capture

- Consult your system administrator to develop and implement a plan to collect necessary metadata elements during the next system upgrade. Note that some systems may require input from a developer, data architect or system administrator.

- Determine an approach to the metadata application profile (MAP). This may include applying the standard directly as a standalone MAP, revising an existing MAP or developing a new MAP in alignment with the standard. Consider the mandatory elements and their application obligation.
  - Where possible, use or adapt existing metadata schemas (e.g., Dublin Core). If a schema and its usage guidelines have already been developed, this could save time and effort.
  - For specialized metadata schemas, consider mapping elements with identical or similar concepts to the standard.
  - Consider options for automatically generating metadata to reduce effort and increase consistency and accuracy.

#### Manage Metadata as a government record

- Metadata should be managed consistent with all government information, according to the [Managing Government Information Policy](#). This includes protecting metadata from loss, unauthorised change, or deletion, and managing access.
- Develop a plan to review and update metadata schemas to reflect the current business needs. Access rules and [controlled vocabularies](#) should be updated when:
  - workgroups are renamed
  - business processes change
  - business locations change
  - business rules change
  - employees change roles etc.
- Manage the metadata application profile and encoding schemes as records. Versions of MAPs and encoding schemes that have been superseded should be retained and managed as records, generally classified under [ARCS 6450-80](#).
- Metadata should be retained or destroyed in accordance with Information Schedules.

#### Ensure that metadata is persistently linked to the information throughout its lifecycle

- For the lifespan of the information resource, metadata should be retained and
- linked with the information resource, including when the resource is transferred out of its original creating environment and through subsequent migrations.



## 6. DEFINITIONS

**Controlled vocabulary:** A controlled vocabulary or language defines what can be entered against a data value, specifies how that information is arranged, and defines which symbols (dashes, commas, colons) are used to separate the individual pieces of information in each value. Different disciplines have developed standard vocabularies that may be automated in systems and software applications as encoding schemes or “pick lists”. Keywording, subject tagging, and classification elements often use controlled vocabularies. When well-devised and rigorously applied, such tools can facilitate sharing of information.

**Critical information:** The information essential to the operations of a government business area. This includes information that supports business continuity by documenting and supporting core programs, functions, responsibilities and commitments (e.g., security and risk mitigation information, information needed to meet financial and legal requirements). Critical information also includes information of public interest and permanent value. See the [Managing Government Information Policy](#).

**Dataset:** Separate data elements that are defined and treated as a collection of information for data manipulation and analysis.

**Descriptive Metadata:** Describes resources for the purposes of identification, discovery and retrieval.

**Digital Record:** A record created and/or maintained by means of digital computer technology. Includes records ‘born digital’ or those that have undergone conversion or digitisation from a non-digital format.

**Digital:** Representing information through a sequence of discrete units, especially binary code. ‘Digital’ is distinguished from ‘analog’, the latter representing information as a continuous signal. ‘Digital’ Often used as a synonym of automated, computerized, electronic or the prefix ‘e-’, although ‘electronic’ may include analog as well as digital formats.

**Electronic Document and Records Management Systems (EDRMS):** A type of content management system that refers to the combined technologies of document management and records management systems as an integrated system. The BC Government Standard for electronic documents is [EDRMS Content Manager](#).

**Encoding Scheme:** A set of specific definitions that describe how to represent data.

**Information Resource:** A set or aggregate of digital government information that is maintained in digital format, and may be accessed, searched, and retrieved via electronic

means. Includes recordkeeping systems, databases, datasets, files, web pages, email messages, pdf documents, etc.

**Interoperability:** The ability of different types of computers, networks, operating systems, and applications to work together effectively, without prior communication, to exchange information in a useful and meaningful manner.

**Metadata Crosswalk:** Also known as metadata mapping. This is the process of defining and associating data elements, semantics, or syntax from one system/schema to another system/schema and documenting their equivalence.

**Metadata Element:** A metadata element (or property) is a specific aspect, attribute, characteristic, or relation that describes a resource, for example: Title, Date Modified, Identifier. Many metadata elements describe the information resources themselves while others provide information about the business context and IT environment, to enable good management of the information.

**Metadata schema:** Is a model for describing data elements or attributes to ensure that the metadata is consistent and communicates the same names for things and concepts. A metadata schema defines how many metadata values can be assigned, whether they are mandatory or optional, how they fit together, and what each individual metadata value (e.g., date of creation, or name) means concretely.

**Metadata:** Metadata is a set of structured data that describes and gives additional detail about an information resource. Metadata helps identify, manage, and share information resources.

## 7. Resources

### Policy and Information

- [Core Policy Chapter 12](#)
- [Date and Time Standard](#)
- [Information Security Classification Standard](#)
- [Information Schedules](#)
- [Managing Government Information Policy](#)

### Learning and Best Practices

- [Dublin Core Metadata Basics](#)
- [Government Records Service Guides and Learning](#)
  - Appropriate Recordkeeping Guide
  - ARCS and ORCS user guide
  - Collaboration Tools Guide
  - Digitizing Government Information Guide
  - EDRMS Content Manager User Tips
  - Managing Website Content Guide
  - Course: IM 112: Managing Government Records (ITEM-41)
  - Course: LAN Organization (ITEM-158)
  - Course: Email and Records Management Best Practices (ITEM-570)
- [CMS Lite User Guide](#)

### REVISION HISTORY

Version	Date	Notes
1.0	Oct. 13, 2022	Approved by Hayden Lansdell, ADM, BC Data Service.
1.0.1	Feb. 13, 2023	Fixed broken link.
1.0.2	Nov. 3, 2023	Fixed broken link to Information Security Classification Standard; updated Application and Advice contact.