New Nouveau Brunswick
CANADA

# Electronic Information Management (EIM)

## Directives

Corporate Information Management Unit
Provincial Archives of New Brunswick

# Revision History

| Version | Revision Date | Author | Summary of Changes |
|---|---|---|---|
| 1 | *Last Review: February 2020* | CIM unit | Review of procedures |
| 2 | *Last Updated: November 2021* | CIM unit | Updated policy AD-1508 to AD-7114 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

**PREFACE .......... 5**

**ELECTRONIC RECORDS .......... 6**

**RESPONSIBILITY FOR ELECTRONIC RECORDS .......... 6**

**ELECTRONIC INFORMATION MANAGEMENT ENVIRONMENT .......... 6**

**WHY ARE EIM DIRECTIVES IMPORTANT? .......... 7**

**PURPOSE .......... 7**

**SCOPE AND INTENDED AUDIENCE .......... 7**

**ORGANIZATION OF THE DOCUMENT .......... 8**

**RECORDS AND INFORMATION MANAGEMENT LIFE CYCLE .......... 8**

**1.0 RECORDS .......... 9**
1.1 Public Records .......... 9
1.1.1 Ministers' Records .......... 9
1.2 Non-Records .......... 10
1.2.1 Duplicates .......... 10
1.2.2 Drafts, Versions, and Working Papers .......... 11
1.2.3 Reference Materials .......... 11
1.2.4 Published Material .......... 12
1.2.5 Advertising Material .......... 12
1.2.6 Personal Content .......... 12

**2.0 CREATION/RECEIPT, COLLECTION, AND CAPTURE .......... 13**
2.1 Records Creation .......... 13
2.2 Mandatory Capture (Force Save) .......... 13
2.3 Profiling Electronic Records .......... 13
2.3.1 Mandatory Metadata .......... 14
2.3.2 Profiling Physical Records .......... 14
2.3.3 Profiling Databases and Business Applications .......... 15
2.3.4 Profiling Workflows .......... 15
2.3.5 Profiling Web Pages .......... 15
2.3.6 Profiling Outputs from Collaborative Spaces .......... 16
2.3.7 Profiling Series of Records .......... 16
2.3.8 Profiling Folders .......... 16
2.3.9 Profiling E-mail Messages and Attachments .......... 17
2.4 Naming Conventions for Records .......... 17
2.4.1 Naming Conventions for Folders .......... 18
2.5 Use of Controlled Vocabularies/Thesaurus .......... 18
2.6 Date Convention .......... 18
2.7 Collaborative Authoring of Records .......... 18
2.8 Version Management .......... 19

2.9 Imaging – Treatment of the Paper Record ..... 19
2.9.1 Imaging- Quality Assurance and Quality Control ..... 20
2.9.2 Imaging – Optical Character Recognition (OCR) ..... 20

**3.0 ORGANIZATION, RETRIEVAL, USE, AND DISSEMINATION ..... 20**
3.1 File Classification Plans ..... 20
3.2 Folder Creation ..... 21
3.3 Search and Retrieval ..... 22
3.4 Sending E-mail and Attachments ..... 22
3.5 Remote Access to EIMS ..... 23
3.6 Templates ..... 23
3.7 Publishing and Posting ..... 23
3.8 Hyperlinks and Dynamic Linking ..... 23

**4.0 STORAGE, MAINTENANCE, AND PROTECTION ..... 24**
4.1 User Profiles ..... 24
4.2 Electronic Records Storage ..... 25
4.2.1 Metadata Storage ..... 25
4.2.2 Storage of Physical Records ..... 25
4.3 Vital Records ..... 26
4.4 Personal Information ..... 26
4.5 Access Rights ..... 27
4.6 Permissions ..... 27
4.7 Transferring Access Rights ..... 28
4.8 Login to EIMS ..... 29
4.9 Security Classification of Records ..... 29
4.10 Encryption ..... 30
4.11 Use of Redaction ..... 30
4.12 Record Authenticity and Integrity ..... 31
4.13 Record Declaration ..... 31
4.14 Maintaining Audit Data ..... 31
4.14.1 Mandatory Audit Events ..... 31
4.15 System Backups and Storage Monitoring ..... 32
4.16 Migration of Records to Upgraded Software ..... 32

**5.0 RETENTION AND DISPOSITION ..... 33**
5.1 Records Retention ..... 33
5.1.1 Extending or Suspending Records Retention ..... 33
5.1.2 Retention Requirements for Triggered Events ..... 34
5.2 Closing Folders ..... 34
5.3 Disposition of Records ..... 34
5.3.1 Disposition of Metadata ..... 35
5.3.2 Disposition of Folder Metadata ..... 36
5.3.3 Disposition Approval ..... 36
5.3.4 Retention and Disposition of Audit Trail Data ..... 36

**6.0 REVIEWS ..... 36**
6.1 Review of Directives ..... 37

**7.0 QUALITY CONTROL ..... 37**

**GLOSSARY ..... 38**

## Preface

The records of government are a valuable resource and an important asset that document its business activities. Their effective management enables government to support future action and decision making, reduce costs, meet business, legal and accountability requirements, and preserve New Brunswick's documentary heritage.

The Provincial Archives' Corporate Information Management Unit is responsible for the government-wide records management program under the *Archives Act*. Provincial government organizations manage their records according to corporate standards, guidelines and policies to support the delivery of their programs and services.

The Provincial Archives of New Brunswick Corporate Information Management Unit provides central records management services and support to departments, crown corporations and agencies within the government of New Brunswick by:

- developing and authorizing retention and disposition schedules that control the period of time government records are retained as well as their final disposition through the transfer to the Provincial Archives or destruction;
- developing and establishing policy, standards and guidelines;
- providing training, technical and consultative services in the development, implementation and maintenance of programs to manage recorded information in all formats;
- maintaining and administering the centralized offsite records storage program for semi active government records;
- identifying archival and records management issues at the beginning of the information life cycle.

Departments manage recorded information by:

- applying the *Classification Plan and Retention Schedules for Common Records* for retention scheduling;
- establishing a file classification plan for operational records;
- developing and maintaining written policies and procedures;
- cooperating with the Provincial Archives to develop and apply retention and disposition schedules for all government records in all formats*;*
- taking advantage of the centralized records storage and retrieval services of the Provincial Archives Records Centre.

It is important to note that records must not be destroyed or removed from the control of the Government of New Brunswick, unless such action is authorized under the *Archives Act*.

## Introduction

### Electronic Records

Electronic records are records created, communicated and maintained by means of computer technology. They may be ‘born electronic’ (created using computer technology), or they may have been converted into electronic form from their original format (e.g. scans of paper documents). Organizations create and store electronic records in a variety of ways. Common types of electronic records include Word documents, spreadsheets, PowerPoint presentations, e-mails, websites and online transactions. However, recorded electronic information can be found in many systems throughout an organization – including databases and business information systems such as CAD software and GIS, shared folders, and hard drives.

### Responsibility for electronic records

Every employee has the responsibility to properly create, capture, and manage the electronic records they create and to maintain them for as long as they are required.  To be of value as evidence, electronic records must possess and maintain context and structure through proper management within a record-keeping system.

### Electronic Information Management environment

In the electronic information management (EIM) environment, specialized software applications are used to manage electronic and paper records. The software provides a framework for the capture, maintenance and accessibility of records over time. Electronic information management software may be comprised of a suite of applications including, but not limited to, the following components:

- Document management – Captures, profiles, controls, and organizes documents within a secure virtual repository.

- Records management – Enables an organization to assign specific retention periods to records from point of creation or receipt; automates the final disposition process.

- Web content management – Manages the publishing and maintenance of content delivered to websites

- Collaboration - Allows multiple users regardless of physical location to work on the same content in a common electronic environment

Although all components may not be deployed at once, it is expected that, at a minimum, the document management and records management applications will be deployed. These two applications form the core of the EIM system by managing a central repository for the storage of all e-records and by providing a mechanism for collecting metadata, applying security permissions, records retention periods, and capturing audit trails.

## Why are EIM Directives Important?

Recorded electronic information must be protected and remain easily accessible for as long as required to meet business needs and to comply with legislation relating to right to information, legal admissibility as evidence, privacy, and archives.

Electronic records are at risk of losing their authenticity because they can be easily modified or altered and may be rendered inaccessible by technological obsolescence. It is therefore necessary to ensure proper management and security measures are in place such as access restrictions, disaster recovery plans, and long-term preservation solutions. EIM directives dictate the actions applied to ensure security

EIM applications are highly configurable (for example settings can be turned on or off to prevent or require certain actions). Successful use of EIM applications depends on decisions made by system administrators and even more on the behavior of end users (for example categorizing content into record and non-record types). EIM Directives provide the parameters for working with the EIM technology

EIM directives are critical in ensuring that business and compliance requirements are met.

## Purpose

The purpose of this document is to provide corporate standards for the creation, capture, management, disposition, and preservation of electronic recorded information using an EIM system. It consists of a set of high-level directives to assist departments and agencies, boards, commissions, and corporations in the implementation of systems that manage electronic information using practices that are common across the Government of New Brunswick (GNB).

It is expected that these corporate EIM directives will be supplemented by departmental/agency or workgroup rules that will meet the specific needs of those organizations.

## Scope and Intended Audience

The *EIM directives* apply to public records created or received by the Government of New Brunswick as evidence of business activity.  Although they are geared towards the management of electronic records, they apply to public records in any format. Electronic records include all records that are created in an electronic format (born electronic), or which have been converted, according to digitization standards, into an electronic format.

The *EIM directives* are intended for GNB IM specialists and practitioners, project managers, implementation teams preparing for and conducting EIM implementations, but all employees should be familiar with them to fulfill their responsibilities for the electronic records they create and receive.

Table of Contents

### Organization of the document

These directives are organized into four categories which follow the life cycle of content and records:

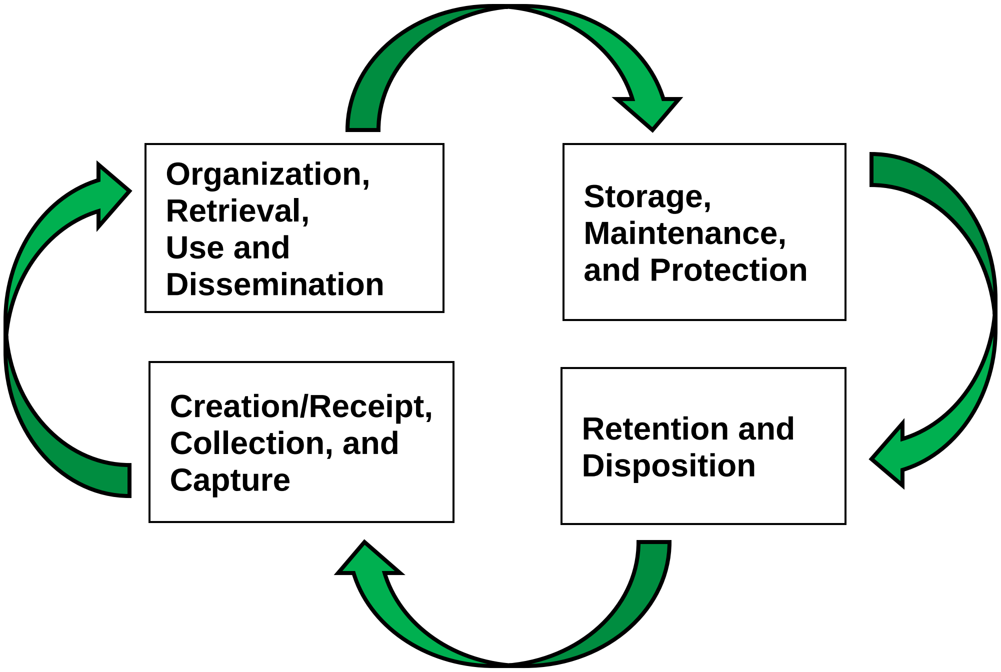
- Creation/Receipt, Collection, and Capture
- Organization, Retrieval, Use, and Dissemination
- Storage, Maintenance, and Protection
- Retention and Disposition

More specifically, the directives provide information on the following:

- common types of electronic records;
- managing electronic records;
- creating and capturing electronic records into recordkeeping systems;
- storing and securing electronic records;
- preserving electronic records;
- providing access to electronic records;
- disposing of electronic records; and
- managing source records

The strategies described in these directives are implemented as part of government of New Brunswick’s corporate information management procedures.

## Records and Information Management Life Cycle


Organization, Retrieval, Use and Dissemination
Storage, Maintenance, and Protection
Creation/Receipt, Collection, and Capture
Retention and Disposition

## 1.0 Records

A **record** is recorded information in any format which provides evidence of a business function, activity, decision, or transaction.

According to the *Archives Act* a **record** means correspondence, memoranda, forms and other papers and books; maps, plans and charts; photographs, prints and drawings; motion picture films, microfilms and video tapes; sound recordings, magnetic tapes, computer cards and other machine-readable records such as e-mails, texts, word documents, PowerPoint presentations, etc.; and all other documentary materials regardless of physical form or characteristics.

## 1.1 Public Records

Public records are the books, papers, and records vested in Her Majesty under the *Public Records Act*, and includes records-prepared or received by any department pursuant to an Act of the Legislature or in connection with the transaction of public business; preserved or appropriate for preservation by a department, containing information on the organization, functions, procedures, policies or activities of a department; or other information of past, present or potential value to the Province.

Public records do not include personal or constituency records of a Minister of the Crown, working papers, or published works. *(For exceptions see* section 1.2*)*

**Directives**:

- **All public records, regardless of format, must be managed by the EIMS.**
- **Public records may be destroyed only in accordance with an approved retention and disposition schedule.**
- **It is the responsibility of the author, recipient, program manager, records manager, or delegate to determine if a document is a public record.**

### 1.1.1 Ministers' Records

Ministers' records fall into two categories:

Ministers' Office Records- generated by ministers in their capacity as ministers of the Crown. These records are public records and are subject to the *Public Records Act*, the *Right to Information and Protection of Privacy Act*, and the *Archives Act*.

and

Ministers' Personal, Political and Constituency Records**-** generated by ministers in their capacity as members of the Legislature and private citizens. These are the ministers' personal property and may be disposed of as the minister sees fit.

**Directives:**

- **Ministers' office records are public records and must be managed by the EIMS.**

- **Ministers' personal, political, and constituency records are not public records and must not be stored in the EIMS but may be kept on GNB hardware, if required.**

**Note: Ministers' personal, political, and constituency records that are stored on GNB hardware may be subject to disclosure and e-discovery under the *Right to Information and Protection of Privacy Act.***

## 1.2 Non-Records

Not all information created or received in the course of government business meets the criteria of a record. Records of temporary usefulness having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record are **non-records**. They are of such short-term value that they are not required to meet legal or fiscal obligations, initiate, sustain, evaluate or provide evidence of decision-making, administrative or operational activities.

Non-Records include: library material made or acquired and preserved solely for reference or exhibition purposes, extra copies of records created only for convenience of reference, some working papers, or stocks of publications or printed documents.

**Directives:**

- **Non-records may be managed by the EIMS but should not be retained any longer than required. Non-records may be destroyed in accordance with the document *Identifying and Handling Records and Non-Records - Directives*.**

***Exceptions: See*** Directives 1.2.6 – Personal Content ***&*** 1.1.1.- Ministers' Records

- **It is the responsibility of the author, recipient, program manager, records manager, or delegate to determine if a document is a non-record *Identifying and Handling Records and Non-Records - Directives* will assist in this determination.**

### 1.2.1 Duplicates

A duplicate is an exact copy of a record, regardless of format, and is used as an information copy. An information copy is normally kept for the purposes of convenience and is required only for a limited period of time. The author or recipient, their delegate, or the administrator can destroy duplicates.

**Directives:**

- **Duplicates can be managed by the EIMS but should not be retained any longer than required. Duplicates should be destroyed in accordance with the document *Identifying and Handling Records and Non-Records - Directives***

### 1.2.2 Drafts, Versions, and Working Papers

A draft is a preliminary version or work in process that is not considered to be the final product. This includes items that have been used in the development or creation of a declared record. Generally, once a final version of the record is placed into a records or information management system, drafts and working materials lose their value and may be destroyed.

In certain instances, it may be necessary to keep drafts and working materials. If they are needed to track the development or modification of a significant document, they should be filed along with the other records relating to that program or service. Examples include: drafts/versions of legislation; legal documents; contracts; agreements; policies, standards, guidelines, and procedures; and audit reports. This may also apply to technical specifications, requests for proposals, action requests, briefing notes and reports, depending on the circumstances.

**Directives**:

- **A draft/version/working paper that is never communicated beyond the author/s or never modified is considered a non-record and can be managed by the EIMS but should not be retained any longer than required. Drafts/Versions/Working papers may be destroyed in accordance with the document** *Identifying and Handling Records and Non-Records - Directives*

- **When drafts/versions/working papers serve as evidence of the evolution of a significant activity, all drafts (including all versions) should be declared public records.**

- **The most current draft/version/working paper stored within the EIMS that is not declared a public record may be modified by the original author or his/her delegate. Other EIMS users attempting to modify a draft for which they are not the author must save it as a new record.**

- **When a draft/version/working paper is authored collaboratively (i.e. by two or more individuals) the users granted co-authoring rights will be permitted to modify it.**

### 1.2.3 Reference Materials

Reference materials from internal or external sources related to the activities and functions of an individual or workgroup are often collected.

**Directives**:

- **Reference material is considered temporary content and can be managed by the EIMS but should not be retained any longer than required. Reference material may be destroyed in accordance with the *Guidelines for Handling Non-Records.***

- **When reference material serves as evidence of the evolution of a significant activity, it should be declared a public record.**

### 1.2.4 Published Material

In most cases, published material includes published items originating from outside the Government of New Brunswick or copies of materials that are produced by the Government of New Brunswick. These materials would normally be maintained in a reference library only as long as administratively useful. Examples of published material are books, magazines, periodicals, brochures, journals, newspapers, and software documentation.

In cases where a department or public body creates a publication, the original or master, as well as the documentation related to its development, is considered a public record.

**Directives**:

- **Published material originating from outside the GNB is considered temporary content and can be managed by the EIMS but should not be retained any longer than required. Published material may be disposed of in accordance with the *Identifying and Handling Records and Non-Records - Directives*.**

- **When published material is created by the GNB and serves as evidence of a significant activity/transaction, it should be declared a public record along with its supporting documentation.**

### 1.2.5 Advertising Material

Advertising material is considered solicited or unsolicited information received from organizations or individuals advertising their products and services. This includes brochures, company profiles, sales letters, menus, catalogues, and price lists.

**Directives**:

- **Advertising material originating from outside the GNB is considered temporary content and can be managed by the EIMS but should not be retained any longer than required. Advertising material may be disposed of in accordance with the *Identifying and Handling Records and Non-Records - Directives*.**

- **When advertising material is created by the GNB and serves as evidence of a significant activity/transaction or is of value and forms part of a public record, it should be declared a public record along with its supporting documentation.**

### 1.2.6 Personal Content

Personal content refers to a GNB employee's private and personal information/*matter* which is unrelated to GNB business. This includes such things as correspondence with family and friends, family photographs, résumés, and jokes.

**Directives**:

- **Personal content is not the result of a business activity of the Government of New Brunswick and must not be managed within the EIMS.**

**Note: Personal records which are stored on GNB hardware may be subject to disclosure and e-discovery under the *Right to Information and Protection of Privacy Act.***

## 2.0 Creation/Receipt, Collection, and Capture

The following directives provide guidelines for records creation, capture, and naming.

Each GNB employee is responsible for the records they create during the regular course of government business. Records must be managed in accordance with the *Records Management Policy* and *Archives Act.*

### 2.1 Records Creation

Authentic, reliable, and accurate records allow the orderly and efficient conduct of business, and provide evidence of business activities and transactions, help meet legislative and regulatory requirements, and facilitate the decision-making process.

**Directives**:

- **All GNB employees as well as external consultants working on behalf of the province must create and maintain full and accurate records of their activities.**

### 2.2 Mandatory Capture (Force Save)

The EIMS can be configured to automatically capture public records or give the user the choice of whether or not to save a record within the EIMS.

Automatic or mandatory capture of records ensures that GNB employees are managing all public records they create in the course of regular business in a single repository.

**Directives:**

- **The EIMS used in departments and other public bodies must implement a mandatory capture (force save) rule and be configured accordingly.**

### 2.3 Profiling Electronic Records

Profiling is the assigning of required and optional metadata to a record at the time of its creation, capture or receipt by the person who saved the record in the EIM system.

In information management, metadata is structured information that describes the context, content and structure of records for their management through time. Metadata describes how, when, and by whom a particular record was collected, and how the record is formatted.  Examples of metadata for electronic records include author, document type, and date created.

Capturing metadata allows for reliable, meaningful, and accessible records that meet business and evidential requirements and are preserved, where warranted, in the Provincial Archives.

**Directives:**

- **All electronic records managed within the EIMS must be profiled (assigned metadata).**

- **It is the responsibility of the record creator, receiver (for records originating from outside GNB), or the first person on a list of recipients to profile the record at the time of its creation, receipt, or capture.**

### 2.3.1 Mandatory Metadata

Consistent and standardized application of metadata facilitates the search and retrieval of records from the EIMS repository. Metadata requirements will delineate mandatory elements and how information should be entered.

**Directives:**

- **Mandatory metadata elements are to be used and applied when profiling records in the EIMS in accordance with the *GNB Metadata Standard (under development).***

### 2.3.2 Profiling Physical Records

A physical record is a record held in a medium other than an electronic format, for example: papers, maps, photographs, microfilm, books, audio tapes, and electronic records *held in removable media* outside of the EIMS.

The EIMS can profile physical records not stored in the EIMS by assigning metadata to them which includes information such as their locations and custodian. The benefit of profiling physical records is that it allows users to “locate” all records pertaining to their search regardless of the medium in which they are held.

**Directives:**

- **Physical records which provide evidence of GNB business activities, decisions, and actions must be profiled by the EIMS.  At a minimum, physical records must be profiled at the series level.**

- **Mandatory metadata elements must be applied when profiling physical records in accordance with the GNB Metadata Standard (under development).**

***For additional metadata associated with physical records stored in the Records Centre during their semi-active period, See*** Directive 4.2.2. – Storage of Physical Records***.***

### 2.3.3 Profiling Databases and Business Applications

The EIMS is generally designed to manage only unstructured information such as documents and, as a result, cannot manage structured information or “data” contained in databases and business applications.

However, like physical records, databases and business applications can be profiled in the EIMS. Metadata may include information about its contents, location and custodian. Profiling databases and business applications allows users to “locate” all information resources pertaining to their search.

**Directives:**

- **Databases and business applications (and other collections of structured data) which provide evidence of business activities or which support routine operations must be profiled by the EIMS.**

- **Mandatory metadata elements must be applied when profiling databases and business applications in accordance with the *GNB Metadata Standard* (under development).**

### 2.3.4 Profiling Workflows

Workflow is a component of the EIM environment that allows organizations to automate a manual business process. The EIMS possesses the ability to profile workflow events which include~~s~~ the tasks completed, content reviewed and approved, and requirements for information input and output fulfilled.

**Directives:**

- **Automated workflow events originating from or integrated with the EIMS must be profiled.**

- **Mandatory metadata elements must be applied when profiling workflows in accordance with the *GNB Metadata Standard (under development)*.**

### 2.3.5 Profiling Web Pages

Websites frequently contain discoverable items. The accuracy and integrity of the content displayed on GNB websites must be verifiable and are subject to admissibility in court. GNB/departments/public bodies may be required to produce entire web pages from a particular point in time to demonstrate what information was presented to its citizens.

**Directives:**

- **Web sites and web pages must be profiled in the EIMS.**

- **Mandatory metadata elements must be applied when profiling web sites and web pages in accordance with the *GNB Metadata Standard (under development)*.**

### 2.3.6 Profiling Outputs from Collaborative Spaces

Collaboration tools in the EIMS allow multiple users to work on the same record in a common environment.

**Directives:**

- **Outputs from work performed in collaborative spaces that capture evidence of government decisions and actions must be profiled in the EIMS.**

- **Mandatory metadata elements must be applied when profiling outputs from collaborative spaces in accordance with the GNB Metadata Standard (under development).**

- **One person must be delegated the responsibility for profiling and managing the content created from collaborative spaces within the EIMS and determining which versions are captured and stored in the EIMS for ongoing retention.**

### 2.3.7 Profiling Series of Records

A records series is a grouping of records according to the business functions or activities that they support. Records series are generally organized within a file classification structure.

**Directives:**

- **Mandatory metadata elements must be applied when profiling records series in accordance with the *GNB Metadata Standard* (under development).**

### 2.3.8 Profiling Folders

Most EIMS allow for the creation of folders and associated metadata such as folder name, creator, and security access data.

**Directives:**

- **Mandatory metadata elements must be applied when profiling folders in accordance with the *GNB Metadata Standard (under development)*.**

### 2.3.9 Profiling E-mail Messages and Attachments

Electronic mail and attachments properly managed by the EIMS facilitates the control of duplication, reduces storage space requirements, reduces size and volume on government's e –mail network servers, ensures that critical information is shared with other authorized users and is not hidden inside individual exchange folders, ensures that e-mail and attachments are recognized as public records and scheduled in accordance with approved records schedules and records management policy.

**Directives:**

- **E-mail messages and attachments that are created or received in the course of government business are public records and must be managed in the EIMS. See** Directive 1.1 – Public Records

- **Mandatory metadata elements must be applied when profiling folders in accordance with the GNB Metadata Standard (under development). The relationships among all components of the message must be maintained. Copies of attachments may also be captured/declared separately.**

- **Personal e-mail messages and attachments must not be managed in the EIMS. See** Directive 1.2.6 – Personal Content**.**

- **When profiling an e-mail that pertains to more than one topic, the record creator must determine if it is appropriate to associate the e-mail to more than one records series in the file classification plan. See** Directive 3.1 File Classification Plans**.**

- **It is the responsibility of the e-mail creator, receiver (in cases where the message originates from outside GNB), or the first person on a list of recipients to profile the e-mail at the time of its creation, receipt, or capture.**

## 2.4 Naming Conventions for Records

Titles within the EIMS for records, e-mails, and physical records maintained outside the EIMS, should contain enough information to describe them and facilitate search and retrieval.

**Directives:**

- **Record titles must be meaningful, accurate, simple, and possess the following basic format: [Title.extension].**

- **Specific naming conventions for records can be defined at the department/public body or section level.**

- **Duplicate record titles are not permitted.**

- **Use of acronyms should be limited to those that are commonly used by GNB at large, or highly recognizable.**

### 2.4.1 Naming Conventions for Folders

Folder names should contain enough information to properly describe the contents of the folder and facilitate search and retrieval activities.

**Directives:**

- **Folder names must be meaningful, accurate, and simple.**

- **Naming conventions for folders may be defined at the Department/public body or section level.**

- **Duplicate folder names are not permitted.**

- **Use of acronyms should be limited to those that are commonly used by GNB at large, or highly recognizable.**

## 2.5 Use of Controlled Vocabularies/Thesaurus

Controls such as controlled vocabularies or a thesaurus reduce the ambiguity found in normal language where the same concept could be given multiple names. The primary purpose of semantic control is to achieve consistency in the description of records and to facilitate accurate retrieval of information.

**Directives:**

- **Departments/public bodies or sections should establish a controlled vocabulary standard such as a specialized thesaurus to identify or describe records series, records, and folders within metadata profiles.**

## 2.6 Date Convention

The standard for date convention must apply to all records and folders.

**Directives:**

- **When profiling records or folders within the EIMS, the following standard must be applied in accordance with *ISO 8601: Data Elements and Interchange Formats — Information Interchange — Representation of Dates and Times*: YYYY/MM/DD *(Year/Month/Day).***

## 2.7 Collaborative Authoring of Records

Some records have more than one author as they are created and modified through a collaborative effort.

**Directives:**

- **In a collaborative situation, one person must be delegated the responsibility for profiling and managing the record within the EIMS, declaring it when appropriate, and determining which versions are captured and stored in the EIMS for ongoing retention.**

## 2.8 Version Management

The EIMS provides many functions that enable users to efficiently manage drafts of records such as the ability to apply the same metadata profile to all document versions; capture comments about what has changed from one version to the next; prevent the deletion or edits of past versions; make the final version read-only (declaring); and differentiate between a major or minor version.

**Directives:**

- **Version management controls in the EIMS environment must be used and implemented to manage and maintain drafts that were created in the course of government business. *See*** Directive 1.2.2. – Drafts, Versions and Working Papers

- **Major Versions – Authors must create a new version when modifications are significant e.g. when there are fundamental changes to the direction, content, meaning, or spirit of the information, and the insertion or deletion of significant information. (Version 2 would be created in succession to version 1)**

- **Minor versions – Authors may create a minor or sub-version when modifications are minor e.g. formatting changes, spelling, punctuation, and grammar check. (Version 1.1 would be created in succession to version 1)**

## 2.9 Imaging – Treatment of the Paper Record

Imaging technology can be used in EIMS to scan and digitize paper records, converting them into electronic images. Such functionality can improve the quality of the image through cropping, de-skewing, and mark-up.

**Directives:**

- **Paper records which have been scanned and profiled may be disposed of only in accordance with an approved records retention and disposition schedule.**

- **When the imaged copies are considered public records, they may be destroyed only in accordance with an approved retention and disposition schedule.**

***See also the** New Brunswick Evidence Act **and the** New Brunswick Electronic Transactions Act*

### 2.9.1 Imaging- Quality Assurance and Quality Control

When the electronic image of a paper record is required for evidentiary purposes, documented verification of the imaging procedure is necessary through quality control and quality assurance processes.

Imaged records may be admissible in legal proceedings provided the imaging process complies with approved imaging procedures. ***See the** New Brunswick Evidence Act**.***

**Directives:**

- **In cases where the electronic image of a record is to serve as the public record, approved and well-documented imaging procedures must be followed. Procedures should take into consideration the:**

*New Brunswick Electronic Transactions Act*
*New Brunswick Evidence Act*

### 2.9.2 Imaging – Optical Character Recognition (OCR)

Optical Character Recognition is the imaging application that translates scanned images of typed or hand printed text into a form that the computer can read and manipulate. OCR enables the EIMS to perform full-text search within the record's content. Generally, the OCR document is not intended to replace the original record.

**Directives:**

- **After the application of OCR, the document must be made read-only to ensure that it is unalterable. The original image of the record must be linked in the EIMS with the OCR image.**

## 3.0 Organization, Retrieval, Use, and Dissemination

The following directives relate to how records are organized, classified, shared, and retrieved.

Records which are efficiently organized ensure timely and enduring accessibility to GNB employees.

### 3.1 File Classification Plans

File classification plans are the framework for the management of all records and provide a method of logically organizing information by function or by subject.  The EIMS accommodates different types of classification structures which support business activities in GNB.

File classification plans are accompanied by retention and disposition schedules and are used to specify the time records are retained, and to identify their final disposition (destruction or archives).

File classification plans must be maintained at the departmental level to link records to programs, projects, functions, etc., of that department.  Departmental classification structures are developed in accordance with standard RIM policies and procedures.

*For the classification plan relating to common records, please refer to the Classification Plan and Retention Schedules for Common Records - CPRS 2010*

**Directives:**

- **All records must be managed by the EIMS in accordance with a file classification plan. Each department/public body is responsible for the establishment and implementation of a file classification plan based on an analysis of functions and activities.**

- **Records must be associated with an appropriate folder within the file classification plan maintained in the EIMS to enable their proper management throughout their lifecycle.**

- **New file classifications may be determined at the departmental, branch, or work group level only when their creation does not affect the approved retention and disposition schedules or breach any access and security protocols.**

***Guidance on creating and maintaining the file classification plan should be provided by an authorized authority such as a Records Manager.***

## 3.2 Folder Creation

The EIMS can be configured to allow users to create folders within file classification plans or restrict this capability to system administrators and/or delegated individuals.

Limiting the capability to create folders to EIMS administrators and/or delegated individuals has its advantages and disadvantages. Unless there are established standards in place, allowing all users to create folders may result in records which are unmanageable. Allowing only system administrators or delegated individuals to create folders can help control records management; however, it may result in inefficiencies, delays and frustration when a new folder is required.

**Directives:**

- **The EIMS will be configured according to the department/division’s decision whether EIMS administrators, specified individuals, or all EIMS users will be permitted to create folders within the file classification plan.**

## 3.3 Search and Retrieval

The EIMS facilitates fast and accurate retrieval of information by providing advanced search features such as full text, metadata, and wildcard search. To ensure that only authorized users can access content in the EIMS, access to items can be set at the file classification plan, folder, and document level. In addition, permissions can be set at the user and group levels.

**Directives:**

- **The EIMS must be configured to allow searching across the entire department/public body's records collection.**

- **By default, all EIMS users must be able to view, at a minimum, the metadata information for records managed in the EIMS.**

## 3.4 Sending E-mail and Attachments

The sender has two choices when sending an e-mail message with an attachment that is stored in the EIMS:

Provide a link – a pointer or shortcut to the actual record stored in the EIMS. When the recipient clicks on the link, the record is retrieved from the EIMS repository.
Provide a copy – a duplicate of the record is sent with the e-mail message. The actual document in the EIMS is not retrieved and accessed by the recipient.

By sending links instead of copies of records as attachments, the integrity of documents is maintained, duplication is reduced, and the volume of traffic on the e-mail system decreases.

**Directives:**

- **When sending an attachment which is stored in the EIMS to another EIMS user (i.e. has access to the EIM repository in which the attachment is saved), only a link must be sent.**

- **When sending an attachment which is stored in the EIMS to a non-EIMS user (e.g. external to GNB) a copy of the record must be sent.**

- **When sending an attachment which is stored in the EIMS to a distribution list with both EIMS and non-EIMS users, or if it is not known whether all recipients are EIMS users, both a link and a copy must be sent.**

- **EIMS users receiving an e-mail with both link and copy attachments, must use the link to retrieve the document.**

- **Records classified as medium or high sensitivity must not be e-mailed to those who do not have the right to view the record, according to security classifications.**

## 3.5 Remote Access to EIMS

The EIMS can be configured to allow users to access repositories remotely via web browsing.

**Directives:**

- **Remote access to the EIMS via home computers or other mobile devices must be performed through a secure link.**

- **Check-in and check-out controls must be used when accessing records from the EIMS to remote or mobile devices. Departments/public bodies must have practices in place which govern the period of time records may remain checked-out of the EIMS.**

- **Any time a record is accessed via a remote or mobile device, an audit trail must be maintained.**

## 3.6 Templates

Templates can be created and managed by the EIMS.

**Directives:**

- **Standard record templates should be created only if they are commonly used types of records (forms) in a department/public body, division, branch, or section.**

- **Standard templates must be managed in the EIMS at the level at which they reside (department, division, branch, section).**

## 3.7 Publishing and Posting

Content and records which are managed in the EIMS can be published through uploading the final record to a website in a read-only format so that it is accessible to others.

**Directives:**

- **All postings and publications to an intranet, extranet, and/or internet site must be performed in accordance with related GNB policies, standards, and procedures. *See AD 7108 – Internet Access, Use, and Posting.***

## 3.8 Hyperlinks and Dynamic Linking

When including the contents of one record into another, for example including the contents of a table in another document, users can either embed the object or insert the information, or use dynamic linking by inserting a hyperlink to the record's location (i.e. a link in the document providing the location of the table).

It should be noted, however, that although dynamic linking will allow the user to access the most current information, it is difficult to capture and manage changing versions of the record over time as links can be broken, thereby affecting its integrity and reliability.

**Directives:**

- **The use of hyperlinks in records is not permitted in the EIMS. Users should embed the content in the "host" record. Exception: Web pages and their contents may utilize dynamic linking.**

- **When linked web content is pertinent to understanding the context of the record, users should embed the web content objects in the "host" record.**

## 4.0 Storage, Maintenance, and Protection

The following directives help ensure that records remain usable, reliable, and secure through time.

The EIMS will be the corporate storage and management environment for all unstructured government information, and will include many items that will, to varying degrees, be sensitive in nature. Protecting these records from unwanted access or manipulation is therefore a primary objective to be met by the EIMS and the technical environment in which it operates.

The EIMS must be capable of managing and controlling records in a way that ensures the legal admissibility and security of records in court. Standard practices for storage, maintenance, and protection will be applied to ensure the integrity and authenticity of the record and associated metadata stored within the EIMS. This includes readability, protection against loss and unauthorized access, use, alteration, destruction, or alienation. Special measures will be taken for the security of classified records and vital records.

### 4.1 User Profiles

User profiles for individuals and groups help capture important information about the users and groups to help link EIMS actions to the individuals and groups performing those actions.

User profiles within EIMS will be linked with the active Government Directory. As result, most required user profile fields will be completed automatically, depending on departmental/public body needs.

**Directives:**

- **A profile will be established and maintained on each authorized EIMS user/group. Maintaining user profiles will be the responsibility of the EIMS Administrator and/or delegate with guidance provided by Corporate Information Management Services (CIMS).**

**User metadata includes:**

| | |
|---|---|
| **User ID** | **User name** |
| **Organization ID** | **Organization name** |
| **User security clearance level** | **System access rights** |
| **User language preference** | |

**Directives:**

- **Steps must be taken to ensure that the link between the audit trail and an employee is not lost even after the employee has left the organization.**

## 4.2 Electronic Records Storage

Records may continue to be managed in EIMS although they may be assigned different storage formats over time. The criteria for storing and migrating records regardless of format or structure within the EIMS repository are usually dependent on departmental storage policies and business requirements. Records may be stored:

**Online** such as in the EIMS.
**Near-line** such as optical disks kept on-site.
**Off-line** such as an off-site storage facility.

**Directives:**

- **Records must be stored, managed, and protected within the EIMS repository, regardless of their format or structure. Records, associated metadata, and other associated records such as indexes and audit logs will be stored on-line. They will be maintained until records have reached the end of their active and semi-active retention periods. It is the responsibility of the department/public body to determine and establish the criteria for storing and migrating records with guidance from CIMS.**

### 4.2.1 Metadata Storage

Records managed by the EIMS must have associated metadata. However, records and their associated metadata are separate entities, and the disposal of one does not necessarily lead to the disposal of the other.

**Directives:**

- **Metadata associated with records stored in the EIMS must be maintained until at least the records' final disposition.**

***See also*** Directive 5.3.1– Disposition of Metadata

### 4.2.2 Storage of Physical Records

Physical records can be managed in the EIMS through the assignment of metadata. It is not expected that all physical records must be converted to an electronic format.

**Directives:**

- **Physical records must be stored in locations consistent with government standards and policies *AD 1508 – Records Management Policy*.**

- **Physical records stored in office or in the GNB Records Centre according to approved retention and disposition schedules may be managed by the EIMS.**

***See*** Business Rule 2.3.2 – Profiling Physical Records

## 4.3 Vital Records

Vital records are those that are essential to the continued operation or resumption of the government following an interruption of services or a disaster. The protection of vital records should be included in departmental/public body disaster recovery plans.

**Directives:**

- **It is the responsibility of each department/public body to identify their vital records and ensure that the records continue to be accessible in accordance with continuity planning and disaster recovery.**

- **Vital records will inherit the attributes of the folders in EIMS in which they are classified (these attributes will include measures to ensure their protection).**

## 4.4 Personal Information

According to the *Right to Information and Protection of Privacy Act (RTIPPA),* “personal information” means information about an identifiable individual, including:

(*a*)the individual’s name,
(*b*)the individual’s home address or electronic mail address or home telephone or facsimile number,
(*c*)information about the individual’s age, gender, sexual orientation, marital status or family status,
(*d*)information about the individual’s ancestry, race, colour, nationality or national or ethnic origin,
(*e*)information about the individual’s religion or creed or religious belief, association or activity,
(*f*)personal health information about the individual,
(*g*)the individual’s blood type, fingerprints or other hereditary characteristics,
(*h*)information about the individual’s political belief, association or activity,
(*i*)information about the individual’s education, employment or occupation or educational, employment or occupational history,
(*j*)information about the individual’s source of income or financial circumstances, activities or history,
(*k*)information about the individual’s criminal history, including regulatory offences,
(*l*)the individual’s own personal views or opinions, except if they are about another person,

(*m*)the views or opinions expressed about the individual by another person, and
(*n*)an identifying number, symbol or other particular assigned to the individual.

**Directives:**

- **All public records are open to disclosure unless subject to the exemptions set out in RTIPPA and other operating procedures*.***

## 4.5 Access Rights

One of the objectives of the EIMS is to ensure that records within the government can be shared and accessed. It is the responsibility of the EIMS Administrator to monitor the degree and nature of access rights/restrictions being placed on the records. Access to records in the EIMS can be as open or as restricted as required to suit the organization/public body's information access and security needs.

**Directives:**

- **Electronic records managed by the EIMS should be organized within a file classification structure and must inherit security attributes where applied to a file class (folder level). The inherited security attributes must restrict the actions that a user or group can perform on records within the EIMS.**

- **Security attributes within the file classification plan must be based on overall sensitivity of the file class or folder contents. For example, access to folders that contain medium to high sensitivity records should be restricted. See the *Government Information Technology Systems Security Policy (GISSP)***

- **Access restrictions must be established on records managed by the EIMS as required. Restrictions to access may be set to:**
  - **allow users the ability to view the record metadata within a search result list, but not be able to access the record; or**
  - **prevent users from viewing records or metadata within the search result list (i.e. providing no indication that a particular record exists); or**
  - **prevent users from viewing record or folder metadata with the search result list (i.e. providing no indication that a particular record folder exists).**

- **Security attributes within the file classification structure may allow authors to override the default access permissions associated with the file class, where appropriate.**

## 4.6 Permissions

The EIMS Administrator is responsible for maintaining the EIMS and consequently requires full access to the application and its functionality.

**Directives:**

- **EIMS users will have the following rights to (in accordance with applicable policies and procedures):**
  - **Store records within EIMS;**
  - **Create new versions of records;**
  - **Modify records that have not been declared as final, along with their associated metadata;**
  - **Declare records as a final for retention application; and**
  - **Delete non-records.**

- **It is the responsibility of the department/public body to delegate an EIMS Administrator.**

- **The EIMS Administrator must have full rights to manage the EIMS. In addition to the rights of a user, the EIMS Administrator will have the ability to:**
  - **Add, remove, and modify user accounts;**
  - **Add remove, and modify access permissions;**
  - **Assign rights to an author's delegate;**
  - **Add, remove, and modify specific metadata fields;**
  - **Add to or modify the file classification structure;**
  - **Add, remove, or modify folders to the file classification structure;**
  - **Apply retention periods in accordance with approved records retention and disposition schedules;**
  - **Delete records in accordance with approved records retention and disposition schedules and in accordance with approved records disposition procedures; and**
  - **Change software configurations as required.**

- **Departmental records managers must have similar rights to the EIMS Administrator such as:**
  - **Add, remove, and modify specific metadata fields;**
  - **Add to or modify the file classification structure;**
  - **Add, remove, or modify folders to the file classification structure;**
  - **Apply retention periods in accordance with approved records retention and disposition schedules; and**
  - **Delete records in accordance with approved records retention and disposition schedules and in accordance with approved records disposition procedures.**

## 4.7 Transferring Access Rights

Access rights to records and folders may be transferred to a new user (e.g. when a staff member has left) or a new workgroup (e.g. when a department/branch is transferred to another).

**Directives:**

- **It is the responsibility of the manager responsible for a user leaving a department/public body/workgroup to determine whether it is necessary to**

**transfer all of the user's rights to another user in order to ensure continued access to the records.**

- **When the responsibility for a business activity or function is transferred from one workgroup to another (i.e. when organizational re-structuring occurs), the new workgroup must assume responsibility for the records and their associated metadata. This includes the right to review retention and disposition schedules.**

- **It is the EIMS Administrator's responsibility to execute access rights transfers at the manager's request.**

## 4.8 Login to EIMS

The *Government Information Technology Systems Security Policy (GISSP)* helps define operational principles, requirements, and best practices for the protection of GNB's networks and computer systems.

**Directives:**

- **All authorized access to the EIMS by department/public body employees, casual/temporary employees must be subject to an approved verification process. At a minimum, that process must be the entry of an approved, unique login identification and password combination.**

## 4.9 Security Classification of Records

The Government of New Brunswick follows the standards for security classification of data set out in the *Government Information Technology Systems Security Policy (GISSP) Standards and Directives*.

The security classification categories are:

| | |
|---|---|
| High | Could reasonably be expected to cause extremely serious personal or enterprise injury, including any combination of<br>extremely significant financial loss,<br>loss of life or public safety,<br>loss of confidence in the government,<br>social hardship, or<br>major political or economic impact |
| Medium | Could reasonably be expected to cause serious personal or enterprise injury, including any combination of<br>loss of competitive advantage,<br>loss of confidence in the government program,<br>significant financial loss,<br>legal action, or<br>damage to partnerships, relationships and reputations. |
| Low | Could reasonably be expected to cause significant injury to individuals or enterprises including any combination of<br>limited financial losses, |

| | |
|---|---|
| | limited impact in service level, or performance, embarrassment and inconvenience |
| Unclassified | Will not result in injury to individuals, governments or to private sector institutions and financial loss would be insignificant. This would fall under public information. |

**Directives:**

- **All records must be managed by the EIMS regardless of security classification. Security controls and access rights/restrictions must be configured to ensure appropriate access to the records.**

## 4.10 Encryption

Encryption is the conversion of electronic information to a coding which is illegible to unauthorized users to ensure security and privacy. The authorized users must use another code to decipher the text.

**Directives:**

- **When transmitting information classified as High or Medium via e-mail to external organizations, the attachment or complete e-mail message must be encrypted in compliance with the e-mail security standard set out in the *Government Information Technology Systems Security Policy (GISSP) Standards and Directives*.**

## 4.11 Use of Redaction

Redaction is the process of removing or masking information within a record when the full record cannot be released or disclosed.

**Directives:**

- **Redaction should be used on records when:**
  - **Publishing or releasing records – or parts of records - pursuant to a right to information request under the RTIPP Act.**
  - **Releasing information in accordance with other legal obligations for confidentiality.**

- **Use of redaction is not permitted on original records. A copy of the record must be made and then redacted. The redacted copy must be saved as a new record, and not another version of the original.**

- **The redacted record must be "linked' with the original using EIMS features. To restrict access to the original, use EIMS access controls.**

## 4.12 Record Authenticity and Integrity

The EIMS offers various features to help users preserve content integrity including version control, audit trails, and check-out and check-in controls.

**<u>Directives:</u>**

- **EIMS controls such as check-out (which locks out other users from editing records) and check-in must be used to manage records and preserve their integrity. Metadata and version management controls should capture changes in authorship when they occur.**

## 4.13 Record Declaration

Declaration is the point at which an author or recipient, their delegate, the Records Manager, or the EIMS Administrator decides that at this time, the record is considered a *public* record and retention is applied. To declare a record final means it can no longer be altered, deleted, or edited.

**<u>Directives:</u>**

- **When a document reaches its final state and/or it is approved or released, it is the responsibility of the record's author or other designated individual, to declare it as a final record which locks its contents and metadata profile so as to protect them from alteration.**

## 4.14 Maintaining Audit Data

Audit data is data relating to actions taken on records that are generated by or within EIMS such as who conducted the action, what action took place, and the date the action took place. Audit data can hamper EIMS performance if allowed to accumulate. Regular archiving of audit data is recommended.

**<u>Directives:</u>**

- **Audit data generated by or within EIMS shall be maintained as a record in accordance with approved records retention and disposition schedules**.

- **In order to maintain system performance, steps must be taken to ensure that audit data is archived regularly (e.g. data older than 12 months) to an offline storage location and is retrievable until the end of its retention period.**

### 4.14.1 Mandatory Audit Events

The EIMS can be configured to capture any or all audit data within the system. To ensure the system performance is not compromised by the unnecessary accumulation of audit information, the capture of only necessary sets of activities is recommended.

**Directives:**

- **The EIMS must be configured to capture, at minimum, the following set of mandatory audit trail events:**

**Access, check-in, check-out, set or change access rights, set or change security classification, create, create new version, copy, copy from, copy to, edit, edit metadata, file, e-mail copy, e-mail link, publish, print, view/look, delete or transfer out of system.**

## 4.15 System Backups and Storage Monitoring

GNB departments and public bodies perform scheduled backups (or copying) of system applications and data for security of information and emergency system recovery purposes. Backups are not performed for the purpose of long-term storage of information. Although backups may contain files that fall under retention schedules, backups are intended to restore files, not to maintain them for long-term use.

Requirements for back-ups should follow the *Government Information Technology Systems Security Policy (GISSP) Standards and Directives*. More specific departmental or program area requirements should be incorporated in IT Service Level Agreements

Failure to ensure that information on backup media is rendered inaccessible when no longer required creates a liability to GNB under the *Right to Information and Protection of Privacy Act.*

**Directives:**

- **EIMS backups must be scheduled and performed on a regular basis. Backups are to be maintained and disposed of in accordance with the *Classification Plan and Retention Schedules for Common Records (CPRS).* A storage monitoring function must be enabled and controlled.**

## 4.16 Migration of Records to Upgraded Software

Generally, applications, software, and hardware will change, move, cease, or require upgrades over time. However, the records created and stored using such technologies must continue to be managed and secured.

**Directives:**

- **Records and their associated metadata must remain authentic, reliable, and usable regardless of changes to format, migration between hardware and operating systems, or software application during the period of their retention.**

- **Departments/public bodies are responsible for monitoring readability and for migrating records as required.**

## 5.0 Retention and Disposition

The following directives relate to records retention and disposition schedules, actions, and responsibilities. Retention and disposition ~~is a~~ are significant components in the life cycle management of records.

Records retention and disposition schedules are developed by departments and other public agencies in conjunction with the Provincial Archives and govern the retention and disposition of all public records.

### 5.1 Records Retention

A records retention and disposition schedule determines the amount of time records must be kept, what will be done with them at the end of their active and semi-active life and determines their final disposition. The retention periods must ensure that records are maintained and protected for as long as required to meet administrative, operational, fiscal, legal, and/or historical value.

**Directives:**

- **Departments and other public bodies must identify retention periods for all public records in accordance with retention and disposition schedules, as approved by the Provincial Archivist.**

- **Retention and disposition schedules must be applied to records through the EIMS and linked to the file classification plan. The records will inherit the retention and disposition attributes of the folder in which it resides.**

- **Retention and disposition schedules should not be applied lower than the folder level in the file classification plan.**

### 5.1.1 Extending or Suspending Records Retention

Extending or suspending records retention (legal hold) may occur owing to current or pending litigation, audits, outstanding requests made under the *Right to Information and Protection of Privacy Act*, investigations, or other conditions that would alter the normal operational, legal, or fiscal value of records.

**Directives:**

- **Designated authorized individuals (e.g. executive management) have the authority to extend or suspend records retention (initiate a legal hold), identify the records affected, apply the hold, and determine when to release the hold. It is the responsibility of each department/public body to designate such individuals.**

- **The EIMS will permit the extension or suspension of the retention and disposition of an individual record or collection of records. There will be a designated person (administrator) authorized to extend or suspend a retention period.**

- **It is the responsibility of program managers to ensure that affected records in their custody are not destroyed, regardless of assigned records retention and disposition schedules, until the suspension is lifted.**

- **All staff and the EIMS Administrator who have received a notification of the records suspension (legal hold) are responsible for complying with the order.**

- **Departments must comply with directives issued by the Provincial Archivist to suspend destruction or transfers to the Provincial Archives.**

### 5.1.2 Retention Requirements for Triggered Events

Some records require triggered events in order to allow retention periods to begin. These are generally denoted by "active period (AP)" or "Superseded/Obsolete (SO)".

**Directives:**

- **The implementation of retention requirements initiated by a business event or trigger must occur only as prescribed by approved records retention and disposition schedules.**

- **Departments must designate individuals responsible for declaring when a business event or trigger has occurred.**

## 5.2 Closing Folders

Folders form the file classification plan within the EIMS environment. When a folder is open and accessible, records can be captured, stored, and managed by the EIMS. However, when a folder is closed, it is no longer possible to capture records within it.

**Directives:**

- **Closure of folders within the EIMS must occur only as prescribed by approved retention and disposition schedules or at the authorization of a designated authorized individual.**

## 5.3 Disposition of Records

Disposition is the final action taken on records and consists of destruction or transfer to the Archives for selection or permanent retention and preservation.

**Directives:**

- **The disposition of all public records managed by the EIMS must be conducted through the application of records retention and disposition schedules. Disposition specifications will be assigned to records through their association to folders within the file classification plan.**

- **Records disposition will include the complete transfer or destruction of electronic and physical records, attachments, and metadata from the file classification system and all storage media (e.g. on-line, near-line discs, tapes).**

- **Where records have been copied from one area of the file classification plan to another, final disposition must ensure that a version of the copy remains fully accessible and retained in accordance with any longer retention periods associated with the folder to which the record was copied.**

- **In the EIMS, the disposition action must ensure that records (including attachments) and associated data cannot be re-constructed without extraordinary means.**

- **Transfer to the Provincial Archives of New Brunswick must include all folder and record-level metadata. Departments should keep copies of portions of the metadata in order to help form a record of disposal along with audit logs or metadata recording disposal events.**

- **Transfers to the Provincial Archives of New Brunswick must follow the procedures set forth in the *Guidelines for Transferring Electronic Records to the Provincial Archives of New Brunswick (draft).***

- **Non-records managed in the EIMS should be routinely disposed of by the author or receiver in accordance with the *Guidelines for Handling Non-Records*.**

***Rules for the transfer of electronic records to Provincial Archives will be developed when the corporate digital preservation strategy is completed. For assistance at any time, please contact the government records archives unit at*** *provincial.archives@gnb.ca*

### 5.3.1 Disposition of Metadata

Records managed in the EIMS environment must have associated metadata. Records and their metadata are separate entities: disposal of one does not automatically mean the disposal of the other. A separate approved metadata retention and disposition schedule may be required.

**Directives:**

- **Metadata for records within the EIMS must be retained at least until the associated records' final disposition.**

### 5.3.2 Disposition of Folder Metadata

Each folder in the EIMS must have associated metadata. The folder and its metadata are separate entities; disposal of one does not automatically mean the disposal of the other. A separate approved metadata retention and disposition schedule may be required.

**Directives:**

- **Folder level metadata (or a subset of that data) will be kept by the department/public body permanently, as will the certificate of final disposition. Folders which are transferred to the Provincial Archives will have their associated metadata transferred with them, but a copy will be maintained in the EIMS so that users are aware that the material has been transferred.**

### 5.3.3 Disposition Approval

Public records can be disposed of only in accordance with records retention and disposition schedules approved by the Provincial Archivist.

**Directives:**

- **Approval by the designated person responsible for the disposition of records managed by the EIMS must be obtained at the folder level from the EIMS Administrator or designate prior to undertaking the actual physical disposition.**

### 5.3.4 Retention and Disposition of Audit Trail Data

The audit trail is the main instrument for documenting actions taken on records. It is an unalterable record of final disposition, individuals approving and undertaking the action, dates as evidence of the final actions taken, and schedule under which records were transferred or destroyed.

**Directives:**

- **The EIMS must be configured to capture and preserve audit trail data on disposition actions for an identified period of time for all records.**

- **The EIMS Administrator or designate must maintain this audit information as a record. Audit data is a public record and must be disposed of in accordance with approved retention and disposition schedules.**

## 6.0 Reviews

The following directives relate to the assessment of the overall performance and compliance of the directives, the review of their effectiveness, their ability to reflect organizational changes, as well as the ability to meet business needs.

## 6.1 Review of Directives

The EIMS Directives should evolve over time to ensure that they continue to meet the needs of the organization, as well as legal requirements.

**Directives:**

- **The Provincial Archives of New Brunswick must review and evaluate the EIMS directives on a regular basis (i.e., every two years or when a significant change has occurred – e.g. technology, policy).**

- **Departments/public bodies are also responsible for reviewing and evaluating the EIMS directives, as they apply to them, on a regular basis (i.e., every two years or when a significant change has occurred– e.g. technology, policy). Evaluations and reviews must be conducted at the level at which the rules were developed and implemented.**

## 7.0 Quality Control

Quality control is the monitoring of the EIMS to ensure the records are properly managed. This will include monitoring the use of the EIMS to identify issues such as non-compliance.

**Directives: Quality control will be performed on records managed by the EIMS. This will include ensuring that:**

- **the appropriate folder codes and metadata are assigned to records and references to collections of records;**
- **records remain accessible and can be shared where appropriate;**
- **appropriate actions are taken to protect vital records;**
- **retention and disposition schedules are assigned to electronic and non-electronic records;**
- **suspensions or "freezes" of retention periods are invoked according to defined criteria, and are lifted when appropriate;**
- **records are disposed of or transferred in accordance with the Records Retention and Disposition Schedule and with the approval of the Administrator or his/her designate;**
- **all duplicates of records are disposed of or transferred; and**
- **approved destruction of records is completed or**
- **transfer of archival records to the Provincial Archives is completed**.

# Glossary

*Capture* – the point at which content is created, saved, and/or stored in the EIMS.

*Content* - consists of any item that has not been declared a record. **Note:** Not all content will become a record.

*Declare* – the point at which an author or recipient, his/her delegate, or the Administrator decides that content is a record. The record is then considered “final” and retention schedules are applied.

*Department* - for the purposes of this document, the word “department” includes government agencies, boards, commissions, and corporations.

*Electronic Information Management System (EIMS)* - A suite of products that includes information management tools (e.g. document management, records management, web publishing) and information access tools (e.g. search, navigation, portal).

*Encryption* – to convert electronic records or data into a code that is indecipherable to unauthorized users.

*File Classification Plan* – a logical, systematic arrangement of recorded information into subject groups or functional categories.

*Final Disposition* – The action determined for the disposal of inactive records, usually according to a retention and disposition schedule. Final Disposition can occur in one of three ways: 1) records no longer having any value are destroyed; 2) records of ongoing value are transferred to the Provincial Archives for selection where an archivist determines if some or all of the records will be preserved; or 3) records of ongoing value are transferred to the Provincial Archives in their entirety for permanent preservation.

*Metadata* –describes the context, content and structure of records and their management through time.

*OCR (Optical Character Recognition* - an imaging application that translates scanned images of typed or hand printed text into a form that the computer can read and manipulate (i.e. for editing). OCR enables the EIMS to perform full-text search within the record’s content.

*Profiling Records* –assigning metadata to a document, a record or a collection of records at the time of its creation, collection and capture to describe its content, context and structure.

*Record* - regardless of format, provides evidence of a business activity, decision, or transaction related to the functions and activities of the Government of New Brunswick. Once a record is **declared** it is unalterable and can be disposed of only via an approved retention and disposition schedule.

*Redaction* – the process of removing or masking information within a record when the full record cannot be released or disclosed.

*Retention and Disposition Schedule* – a timetable that describes the lifespan of a record from the time of its creation through to its final disposition.

*Structured Records*– consists of any record that has an enforced composition. Structured records are managed by technology that allows for querying and reporting against predetermined data types and understood relationships such as a database.

*Unstructured Records*– consists of any record stored in a format that is unstructured such as word processing, e-mails, and spreadsheets.

*Vital Records* – those records that are essential to the continued operation or resumption of the government following an interruption of services or a disaster.