Information Management Directive:	Issued: April 22, 2021
Subject: Information Management Practices	Effective: April 22, 2021 Last Review: May 17, 2023

1 DIRECTIVE OVERVIEW

1.01 When providing any services and programs or performing activities that involve creating or managing information, government bodies and their employees must follow the information management practices set out in this directive for:

- Creation, Capture and Management of Information
- Retention, Destruction and Preservation of Information
- Systems and Devices Used to Maintain Information
- Transfer of Information
- Data Management

2 PURPOSE

2.01 The purpose of this directive is to support the GNB Policy on Information Management by establishing requirements:

- for creating, capturing, managing, retaining, destroying, maintaining and transferring information based on applicable laws and best practice;
- for managing data based on applicable laws and best practice; and
- to monitor and report on compliance with the policy.

3 SCOPE

3.01 This directive applies to government bodies and employees in Parts I-1V listed in the First Schedule of the *Public Service Labour Relations Act*, except universities.

4 DIRECTIVES

4.01 Government bodies and employees must comply with the following information management practices unless the *Archives Act*, regulations under the Act or other applicable legislation state otherwise:

4.02 **Creation, Capture and Management of Information**:

(a) Identify information required to support the organization's business and activities.

(b) Organize, classify and manage information that is a record in order to preserve its context and ease of retrieval.

(c) Documenting activities and decisions related to government business.

(d) Manage records in accordance with approved records retention and disposition schedules.

(e) Take measures to ensure the authenticity, reliability, integrity, and usability of information that is a record throughout its full lifecycle.

(f) Take appropriate measures to protect information that is a record based on:

i) the length of time the information must be maintained

ii) the nature of the information (personal, sensitive, confidential, etc.), and

iii) the format or medium on which the information is stored

iv) for personal information, the level of risk of unauthorized access, use,

disclosure or disposal of the information and the degree of harm that might arise from any unauthorized access, use, disclosure or disposal of the information.

See AD-7107 Government Information Technology Systems - Security Policy.

4.03 **Retention, Destruction and Preservation**

(a) Schedule retention of information that is a record in accordance with operational, legal, administrative and historical requirements.

(b) Only destroy information that is a record in accordance with approved records retention and disposition schedules, guidelines or standards issued or approved by the Provincial Archives.

(c) Destroy or dispose information that is a record at the end of its retention period using secure and/or permanent methods (see Secure Destruction of Records Directive) unless:

i) a legal hold is in place or pending, or

ii) a freeze or hold for business purposes is approved by the Finance and Treasury Board – Provincial Archives' Corporate Information Management Unit.

(d) Destroy non-records that no longer serve a useful purpose in accordance with the Provincial Archives' Identifying and Handling Records and Non-Records. Information identified as a non-record includes an employee's personal communications, duplicates, drafts and reference material created or acquired by government employees pursuant to their individual responsibilities.

4.04 **Systems and Devices Used to Create and Maintain Information**

(a) Ensure that government-approved systems or infrastructure such as shared drives, business applications, cell phones, ipads, etc., are capable of meeting information management and legislative requirements, and that the information created within these systems be managed following the requirements of this directive.

(b) Ensure a business information system or a major change to an existing system is assessed by an information/ records manager for compliance with information standards and requirements before the system or change is implemented or before information/data is migrated to or from the system.

(c) Take reasonable security measures to safeguard confidential, personal, or sensitive information on electronic storage devices or systems, and paper-based when transporting or using the information outside the workplace.

(d) Don't download or store a government body's confidential or sensitive information on a non-government device. A non-government device includes a personal smartphone and computer, a memory stick and an external hard drive.

See AD-7107 Government Information Technology Systems - Security Policy.

4.05 **Transfer of Information**

(a) Transfer records deemed to be of permanent value in accordance with approved records retention and disposition schedules to the Provincial Archives for preservation and eventual access.

(b) Where a government body or a function performed by a government body ceases to exist, transfer all the records to the Provincial Archives.

(c) Where an administrative or organizational change occurs and a function or activity is transferred to another government body, transfer all the records to the inheriting government body.

(d) Where an administrative or organizational change occurs and a function or activity is transferred to an organization outside the government, establish a memorandum of understanding or an agreement specifying details regarding the ownership, transfer, retention, access, use, protection of personal information and security of the records for approval by the Provincial Archives' Corporate Information Management Unit. Note: For the transfer of electronic records to the Provincial Archives, please contact: Records.Centre@gnb.ca

4.06 **Data Management**

Government bodies and, where applicable, employees must

(a) Identify, classify, inventory, document, and maintain data and its corresponding systems throughout their lifecycle.

(b) Establish and maintain a data governance framework to manage the design, integrity, availability, lifecycle, and efficient use of data and information systems.

(c) Identify a data steward for data and corresponding information systems.

5 RESPONSIBILITY

5.01 Heads of government bodies or their delegates must:

(a) Ensure implementation of the information management practices in this directive.

(b) Ensure the organization's officers and employees know they are required to follow these practices.

5.02 Information Managers for government bodies must:

(a) Advise on implementation and maintenance of information systems to ensure compliance with the information management practices in this directive.

(b) Manage records storage costs and carry out information management practices such as the recommendation and application of records retention and disposition schedules, the creation and use of file classification plans, etc.

(c) Develop organizational policies, practices, procedures and employee training on information management in collaboration with others.

(d) Identify and protect records critical to the organization's business operations.

5.03 The Corporate Information Management (CIM) Unit, Department of Finance and Treasury Board, is responsible to:

(a) Help government bodies understand and apply the practices in this directive.
(b) Monitor and report compliance with this directive as determined by the CIM Unit in consultation with government bodies.

5.03 Employees must:

(a) Follow the information management practices set out in this directive or established by their organization pursuant to this directive.
(b) Provide and bring information requirements and issues to their manager's attention and, when appropriate, to the organization's information manager.
(c) Participate in any information management onboarding/orientation session for new employees and other required information management training.

6 DEFINITIONS

6.01 **Data** means a fact or collections of facts collected together for reference or analysis. Data can be unstructured or structured.

6.02 **Data management** means the development, implementation, and administration of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. Data management addresses the end-to-end lifecycle of data.

6.03 **Data steward** means a data quality expert who is responsible for organizational data on a day-to-day basis. The responsibilities of a data steward are to draft data quality rules, measures, and to ensure the proper management of data within their organization.

6.04 **Employee** means a person retained under any form of employment or personal services agreement for a government body, including members of agencies, boards, commissions or tribunals, students and interns, contractors and service providers.

6.05 **Government body** means a public body in Parts I to IV listed in the First Schedule of the *Public Service Labour Relations Act*.

6.06 **Information** means information that can be defined as data that is given meaning and relevance based on its context. Information is considered data that has been processed or converted into a useful and intelligible form for decision-making purposes.

6.07 **Information management** means a discipline of people, processes and technology needed to effectively structure, classify, describe, and govern information across an organization and information technology systems to improve efficiency, promote

transparency and enable business insight and decision support.

6.08 **Information manager** means a person who leads and oversees information management activities such as the planning, organizing, structuring, processing, controlling, evaluation of all records and information assets of the organization.

6.09 **Other applicable legislation** means other legislation with information management provisions that apply instead of or in addition to the *Archives Act*.

6.10 **Record** means recorded information, regardless of medium or format, created or received during government business, and maintained as evidence of such activity, as defined by *The Public Records Act* and the *Archives Act*.

6.11 **Records management** means the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions.

6.12 **Records retention and disposition schedules** are legal documents that specify the length of time records must be kept in an office, and how long they must be stored off-site at the Provincial Archives Records Centre, if required. It also states what happens to the records once they reach the end of their lifecycle. Records retention and disposition schedules are issued by the Provincial Archivist, but are agreed to jointly by the records-creating government body, and the Archivist.

6.13 **Secure destruction** is the process of destroying information on tapes, disks, paper documents, graphs and other forms of electronic and physical storage to the point that it is completely unreadable and cannot be reconstituted, accessed, or used for unauthorized purposes.

7 RELATED LEGISLATION, POLICIES AND DIRECTIVES

Protection of Personal Health Information Act
Right to Information and Protection of Personal Information Act R-10.6
Information Systems Policy and Guidelines AD-7101
Government Information Technology Systems - Security Policy AD-7107
Email and Electronic Communications Directive