IM Advisory — Executive Records

Overview

This Office of the Chief Information Officer (OCIO) Information Management (IM) Advisory provides common best practices to consider when managing executive records. The audience for this advisory includes all public bodies as defined under the Management of Information Act. Public bodies may develop additional requirements to meet individual needs. Public bodies are advised to consult with their internal IM division to access internal requirements, tools and services. This advisory supplements resources available on the OCIO website.

What are Executive Records?

Executive records include the administrative and operational records of the offices of ministers, deputy ministers, assistant deputy ministers, and equivalent positions. Executive records often document the development, implementation, operation, and evaluation of government legislation, programs, and services. Examples of records or functions may include but are not limited to:

— Briefing Notes	— Accountability	— Committee Records
— Cabinet Records	— Legislation	— Jurisdictional Relations
— Communications	— Executive Meetings	— Organizational Reports
— Strategic Planning	— Audit Management	— Corporate Finance Records

Why Manage Executive Records?

Executive records reflect the overall governance and management of a public body. Some executive functions are led by the executive and therefore have a larger volume of documentation stored within the executive suite (e.g. Organizational Reports). The executive is often engaged in matters that originate with the program-specific lines of business in the public body (e.g., communications related to a new initiative). As a result, the executive provides input to the relevant program or service area. In such instances, government records are retained by the line of business. It is important that executive records are managed effectively because they:

— Provide a complete high-level overview of the public body's fulfillment of its mandate.

— Demonstrate compliance with operational, legal and regulatory requirements.

— Capture senior-level decision making processes.

— May be accessed and scrutinized at a later date by other government employees and members of the public.

— Must be easily accessible to decision makers to:

    o Maintain operations and the provision of programs and services

    o Manage and report on resource usage

    o Respond to issues or inquiries

— Have a high rate of records which may have long-term historical or cultural significance that must be transferred to The Rooms Provincial Archives when the public body has fulfilled legal retention requirements.

Record Characteristics

When creating an executive record, it is important that consideration for inclusion of the following characteristics, if available, are present to ensure that it is complete, authentic and reliable. This information may be recorded within the record or as a part of its metadata:

— Date	— Record Type	— Media
— Time	— Draft or Final	— Technology Used
— Location	— Creator	— Recipient
— Participants	— Audience	— Reviewed by
— Signatures	— Reference/Identifier	— Alternative Media

Things to Consider When Managing Executive Records

Employees should have clear direction on how to manage the information used to administer or carry out programs and activities on behalf of the public body. This information may be documented in a training or support manual. Programs or services may have requirements that are unique to the type of information or service as determined by the public body. General considerations when creating information management policies and procedures may include, but are not limited to:

Creation: The OCIO maintains the Corporate Records and Information Management Standard (CRIMS) to provide guidance on the records that may be produced to support executive functions. These examples may be augmented by requirements specific to the public body's mandate (e.g., a Government Department that works closely with the Federal government may participate in Federal, Provincial and Territorial (FPT) working groups).

Cabinet Records: Under the Management of Information Act, Cabinet Records are managed in a manner determined by Cabinet Secretariat. Employees engaged in the cabinet submission process are advised to complete training and remain aware of requirements released by Cabinet Secretariat.

Briefing Materials: There are many types of briefing materials (e.g. executive, departmental, ministerial, etc.). These are described in CRIMS. Cabinet Secretariat has developed new templates to maintain separation between factual information and analysis in briefing materials.

Required Content: For each type of record it is important to ensure that records are complete, accurate and reliable to meet the public body's legal or operational requirements (e.g. report for transparency and accountability meets the needs as specified for the category). Sample content for executive records may include, but is not limited to:

— Memo from Executive	— Correspondence	— Reports
— Completed Template	— Meeting Minutes	— Analysis
— Supporting Documents	— Decision Notes	— Committee Records
— Appendices	— Notes to File	— Legal Opinions

Roles and Responsibilities: Multiple employees may need to access/action executive records. The management team may consider providing employees with a reference including how information is controlled, and how individuals are notified that an action is required (resulting from this activity).

Technology: All employees must comply with the OCIO's Directive on Acceptable Use of the Government Network and Information Technology Assets. Identify the technology solutions used to support the records' functions:

— Use of Network File Share/Personal file share: Define what records will be stored when, how and by whom for all executive functions.

— USB Flash Drives: Use only encrypted removable media when necessary as per the OCIO's guidance.

— Use of an Electronic Document and Records Management System (ERDMS). Public bodies are responsible for their own internal administration of their ERDMS installation. ERDMS has been implemented as the standard tool to support executive correspondence. Public bodies may determine other record types to use in ERDMS to support executive functions.

— Email Management: Compliance with the OCIO's Email Management Policy.

— Instant Messaging: Compliance with the OCIO's Directive on Instant Messaging.

— Mobile Devices: Compliance with the OICO's Directive on Mobile Devices for Government Employees.

Forms/Templates: Use of forms and templates encourages creation of consistent, complete and accurate records.

Transport/Sharing: Identify procedures for how files are to be transferred to another location or shared with authorized persons (e.g. encrypted email vs. use of interoffice mail vs. Canada Post vs. courier). Some files may require specific considerations:

— Cabinet Records

— Budget Documents

Storage: Executive records may have highly-sensitive content. Access restrictions and controls must be enforced to protect personal and confidential information. Records should be stored in physical format in either the executive suite or in a secure location accessible only to authorized employees. Electronic storage, including the network file shares and electronic document and records management libraries, must apply appropriate access levels.

Naming Conventions/Labelling: Identify how individual records, file folders, etc. are to be named/labelled.

Secure Destruction of Transitory Records: Guidance should outline what information needs to be retained in the final file as a government record vs. what information is considered transitory as defined in the Management of Information Act (e.g., retain final versions, eliminate copies, print emails and file deletions from Outlook, etc.). Ensure that copies of transitory records required by lines of business, including executive input, are securely destroyed.

Disposal: Disposal of executive records is permitted when the public body has fulfilled its legal retention requirements:

— Disposal must comply with the Management of Information Act (MOIA).

— Disposal means either secure destruction, transfer to The Rooms Provincial Archives or in rare cases permanent retention by department.

— A disposal authority approved by the Government Records Committee (GRC) is required to dispose of a government record.

— The OCIO supports the Corporate Records and Information Management Standard (CRIMS) for disposal of corporate records.

— Public bodies should reference internal Records Retention and Disposal Schedules (RRDS) for authorization of any additional or specific processes.

— Guidance should outline what information needs to be retained in the final file as a government record versus information considered as transitory as defined in the MOIA (e.g. retain final versions, eliminate copies, file emails and delete from Outlook, etc.).

For additional information on managing records, contact the public body's Information Management Division. General inquiries may be forwarded to IM@gov.nl.ca.

Supporting Materials

Management of Information Act
https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Policy - Email
https://www.ocio.gov.nl.ca/ocio/email/index.html

Directive - Instant Messaging
https://www.ocio.gov.nl.ca/ocio/instant_messaging.html

Directive - Acceptable Use of the Government Network and Information Technology Assets
https://www.ocio.gov.nl.ca/ocio/im/employees/asset_use.html

Directive - Mobile Devices for Government Employees
https://www.ocio.gov.nl.ca/ocio/publications/policies/Directive_Mobile_Devices_for_Government_Employees.pdf

Corporate Records and Information Management Standard
https://www.ocio.gov.nl.ca/ocio/im/c_rims.html

Records Retention and Disposal Schedule Standard
https://www.ocio.gov.nl.ca/ocio/im/disposal.html

Government Records Committee
https://www.ocio.gov.nl.ca/ocio/im/committee.html

FYI - IM Advisory - Note to File
https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Note_to_File.pdf

FYI - IM Advisory - Case Files
https://www.ocio.gov.nl.ca/ocio/im/practitioners/IM_Advisory_Case_Files.pdf

FYI – Information Protection – USB Drives – What You Should Know
https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/FYI_Information_Protection-USB_Drives.PDF

Version History

(OCIO Ref. DOC01134/2019)

1.0	2016 02 04
2.0	2019 03 29

Newfoundland
Labrador