Office of the Information and
Privacy Commissioner of Alberta

Investigation Report F2019-IR-01

Investigation into the management and storage of email by the Government of Alberta

March 12, 2019

Service Alberta, Alberta Transportation,
Alberta Education and Executive Council

Investigations 006900, 006898, 006899 and 006663

Commissioner's Message

On September 28, 2017, the Official Opposition wrote to me outlining several concerns about how the Government of Alberta (GoA) manages and uses email. These concerns were based on responses the Official Opposition had received to several access to information requests made to various GoA departments, and included allegations that GoA departments may have improperly deleted over 850,000 emails between the fall of 2015 and the spring of 2016, and that one ministry (Alberta Transportation) offered a draw for a gift card for employees who deleted the most emails. At the time, the Official Opposition issued a news release describing these and other allegations.[1]

Based on the letter and information provided to me, as well as the considerable media and public interest, I opened this investigation on my own motion under section 53(1)(a) of the *Freedom of Information and Protection of Privacy Act* (FOIP Act), which reads:

> **General powers of Commissioner**
>
> 53(1) In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records…

I retained MT>3, a division of McCarthy Tetrault LLP, to investigate this matter. MT>3's report is attached.

The investigation did not confirm the allegations made by the Official Opposition in its letter to me, but instead concluded:

- There is no compliance program established to ensure that staff members have received appropriate training and are following the records management plan for their department.
- That most staff members are retaining more email records than required (e.g. the majority of email mailboxes reported in the responses to the access requests contained at least 50,000 records, with many over 100,000 records).
- There is a lack of consistency in how official records are being stored. Most official email records appear to be saved in individual staff members' mailboxes, which makes it more difficult to find responsive information for business, legal, regulatory or FOIP Act responsibilities.

[1] United Conservative Party, "United Conservatives mark Right to Know Week, call for investigation into deleted government records", September 28, 2017, available at www.ucpcaucus.ca/united-conservatives-mark-right-to-know-week-call-for-investigation-into-deleted-government-records/

The investigation report recommends:

- Service Alberta's plan to develop an information management reporting and compliance program should include:
    - Specific requirements for GoA departments to measure and report on the compliance of the records management plan
    - Service Alberta should compile annual statistics from each department
    - Service Alberta should work with the departments to develop a method to ensure that all staff members understand and follow the regulations
- Service Alberta should develop a method to measure:
    - Whether each department is retaining the records they should be retaining
    - How efficiently each department can find records in response to a business, legal, regulatory or FOIP Act requirement
    - Verify that records required by a business, legal, regulatory or FOIP Act requirement are properly identified by each department
- Service Alberta should begin planning to implement a government-wide official records electronic storage repository, so that records responsive to business, legal, regulatory or FOIP Act requirements can efficiently and accurately be identified

Overall, this investigation reinforces the fundamental importance of a comprehensive, effective records management program to ensure that public bodies are able to fulfil their access and privacy obligations under the FOIP Act, and for meeting other business and legal responsibilities.

Jill Clayton
Information and Privacy Commissioner

MT>3

A DIVISION OF McCARTHY TÉTRAULT

Investigation of the Management and Storage of Email by the Government of Alberta

Prepared by
Chuck Rothman
December 13, 2018

Table of Contents

1. Introduction 1

2. Background 2

3. Issues 4

4. Analysis and Findings 5

   A. Information Gathering 5

   B. GoA's *Records Management Regulation* 6

   C. Service Alberta's Records Management Policies, Standards and Procedures 6

   D. Alberta Education's Email Management Program 9

   E. Alberta Transportation's Email Management Program 10

   F. Interviews with Senior Staff Members 11

   G. GoA Email System 12

   H. eVault System 13

   I. Service Alberta's Process to Compile Email Mailbox Sizes for Access Requests 13

5. Conclusions 14

6. Recommendations 17

1. INTRODUCTION

On September 28, 2017, Mr. Nathan Cooper, Interim Leader of the Official Opposition, formally requested that the Information and Privacy Commissioner of Alberta (“Commissioner”) open an investigation under the *Freedom of Information and Protection of Privacy Act* (“FOIP Act”) into the management and storage of emails by the Government of Alberta (“GoA”). Specifically, the Commissioner was asked to review practices surrounding how GoA emails were retained and disposed of (letter attached as Appendix A).

The request was predicated upon a series of access to information requests (“access requests”) made by the Official Opposition in 2015 and 2016 to obtain information on how political staff and senior figures in the GoA use email.

On October 27, 2017, the Commissioner opened investigations against Alberta Transportation, Alberta Education, Service Alberta and Executive Council.

On December 8, 2017, the Commissioner retained the services of MT>3, a division of McCarthy Tétrault LLP, to assist in the investigation of GoA email management, retention and disposition. This report outlines the findings and recommendations from the investigation.

2. BACKGROUND

In December 2015, the Official Opposition made an access request to several GoA departments for the number of emails stored within the inbox folder of the email mailboxes of senior government and political staff. They received documents (one per GoA department) listing the number of emails in each person's inbox folder, as of the week of December 22, 2015.

In the spring of 2016, the Official Opposition made two more access requests, one for the number of emails stored in each person's entire mailbox during the month of February 2016, and one for the number of emails stored in the inbox, sent, deleted and drafts folders, plus all subfolders for each of these main folders, of each person's mailbox, between March 10, 2016 and March 29, 2016.

The data was analysed. The Official Opposition prepared a report (provided subsequent to their letter to the Commissioner dated September 28, 2017). In the report, the Official Opposition raised concerns about the way email was used and retained by GoA staff. Specifically, the Official Opposition concluded that:

1. Between the first and second access requests, the number of emails stored in mailboxes increased on average, but for certain uses, decreased significantly. The Official Opposition concluded that at least 859,681 emails were deleted between the fall of 2015 and the spring of 2016.

2. As mentioned in the Official Opposition's report, when questioned about the deleted emails identified by Official Opposition, Service Alberta's Executive Director of Information Access and Protection explained that the decrease in emails was due to an increased awareness of email volumes after the first request, and steps that had been taken to reduce volumes.

   The Official Opposition specifically mentioned Alberta Education and Alberta Transportation in their report, both of which launched email management programs following the first access request to improve the way their staff managed email.

   The Official Opposition concluded that the emphasis of these programs was to reduce volume without regard to retaining official records.

3. The Official Opposition stated in its report that government guidelines require the person sending an email to be responsible for preserving it. They identified several senior officials whose mailboxes had very few emails. Based on this, the Official Opposition concluded that these people were either not generating email or were not preserving the emails they sent.

4. The Official Opposition asserted that, when a GoA staff member leaves the government or moves to another department and their email mailbox is retired, their emails are deleted, and cited examples from their analysis to substantiate this.

5. The Official Opposition raised a concern about accountability with respect to how records management is carried out. They cited a Public Accounts Committee meeting held on October 11, 2017 where an Assistant Deputy Minister of Service Alberta said:

> “I do believe in the employees of the government of Alberta, that they are adhering to the policies and processes that we've put in place, and in fact through the communication channels we have, that we are clearly expressing to our employees the appropriate practice for use of these tools. In fact, I can't guarantee that every individual is adhering to them, but I'm fairly confident, and I would hope that the large majority of them are.”

6. The Official Opposition suggested that errors may have occurred during collection of the email data provided to them, and if so, they claim that since the data was derived from a standard department billing report, GoA departments were being undercharged for email use.

7. The Official Opposition identified several people’s mailboxes as having thousands of emails in the sent items folder, but only a few in the inbox. The Official Opposition offered an explanation that these people may be storing their received email outside their mailbox but did not provide any detail to substantiate this assumption.

8. In their letter of September 28, 2017, the Official Opposition mentioned that they received conflicting information about the nature of the GoA’s email eVault system. It appeared that this system had been, or was in the process of being, decommissioned and there was concern about how the emails stored in the system were preserved, particularly for retired mailboxes.

3. ISSUES

The following issues were identified for this investigation:

1. What are the regulations, guidelines and procedures applicable to determining whether an email record should be retained or can be disposed of?

2. Are the regulations, guidelines and procedures being followed by GoA staff?

3. Are the regulations, guidelines and procedures applicable to email management sufficient to ensure that official records are retained in such a way that they can be found for business and regulatory requirements?

4. How do Alberta Education and Alberta Transportation educate their staff to manage email?

5. How did Service Alberta compile the information provided in response to the access requests?

6. How are emails stored within retired mailboxes preserved?

7. How were emails stored in the GoA's eVault system preserved after that system was decommissioned?

4. ANALYSIS AND FINDINGS

A. Information Gathering

The following steps were taken to gather information for this investigation:

1. Service Alberta was contacted in writing and asked for details concerning:

   a. How Service Alberta generated the email mailbox volume information contained in the reports provided to the Official Opposition for both Round 1 (inbox only) and Rounds 2/3 (entire mailbox size and specific folder sizes). We asked to review the scripts they used, and any exception reports that may have been generated during the data collection process,

   b. a description of the Symantec eVault system, including the time period it was active, whether staff had any control over which emails were archived, and the disposition of the eVault contents after it was decommissioned,

   c. a description of the current GoA email system,

   d. Service Alberta's role in setting, communicating and monitoring email usage and retention policies and procedures.

   The results of the query were reviewed and a request for further information to clarify details was made.

2. Alberta Education and Alberta Transportation were contacted in writing and asked for details concerning:

   a. What measures each department had in place to educate their staff on email management and retention before the first access request was made in the fall of 2015,

   b. what email management and retention education initiatives they instituted between the first and second access requests, and

   c. what current policies and standards are related to email management and retention.

   The results of the queries were reviewed and requests for further information to clarify details were made.

3. We compiled a list of senior GoA and political staff members, identified by the Official Opposition through their analysis of the information provided by the access requests, as having either very few emails in their entire mailbox or inbox folder or having a significant reduction in emails between the first and second access requests. Eight people were randomly chosen from this list for face-to-face interviews to ascertain their email management and retention activities. The positions/titles of the eight individuals are:

- Assistant Deputy Minister, Heath Standards, Quality and Performance Division, Health
- Assistant Deputy Minister, Heritage Division, Culture & Tourism
- Assistant Deputy Minister, Tax & Revenue Administration, Treasury Board & Finance
- Deputy Chief of Staff, Premier's Office, Executive Council
- Deputy Minister, Community & Social Services
- Executive Director, Labour & Employment Practices, Public Service Commission
- Executive Director, Capital Projects Delivery Division, Infrastructure
- Chief Sheriff/Executive Director, Sheriffs Branch, Justice and Solicitor General

B. GoA's *Records Management Regulation*

Records management in the GoA is governed by Alberta Regulation 224/2001, *Records Management Regulation* (attached as Appendix B). This regulation requires that Service Alberta be responsible for:

- Establishing a records management program, including all necessary policies, standards and procedures to manage records in the GoA,
- organizing and managing the Alberta Records Management Committee, whose responsibility is to review and approve all records retention schedules, provide advice to the Minister of Service Alberta on the policies, standards and procedures established to manage GoA records, and evaluate the implementation of the records management program in each GoA department.

The *Records Management Regulation* requires that the deputy head of each GoA department be responsible for preparing records retention and disposition schedules and ensuring that the records within that department's custody and control are managed in accordance with the policies, standards and procedures established by Service Alberta.

C. Service Alberta's Records Management Policies, Standards and Procedures

Service Alberta's records management standard is standard number A000024, Records Management Program Standard (attached as Appendix C). This document was created in 2011, and last updated in 2017. It references ISO 15489-1-2016, an international standard describing the concepts and principles used to develop policies related to creation, capture and management of records. ISO 15489-1-2016 covers:

a. Records, metadata for records and records systems;

b. policies, assigned responsibilities, monitoring and training supporting the effective management of records;

c. recurrent analysis of business context and the identification of records requirements;

d. records controls;

e. processes for creating, capturing and managing records.

Service Alberta has published guidance on the identification and management of official records in a document entitled “Official and Transitory Records: A Guide for Government of Alberta Employees” (attached as Appendix D). This document is designed to assist GoA staff to identify official records, which are records that are applicable to the department’s retention and disposition schedules, and transitory records, which are records that are not governed by retention and disposition schedules and can be disposed of at the discretion of the staff member.[1]

The guide was published in October 2015. It defines a record and includes examples of record types. It further defines official and transitory records (with examples).

The guide describes in detail how to dispose of transitory records. For official records, the guide notes, “Official records document and provide evidence of business transactions. They are records that must be retained and filed in official records systems, and managed in accordance with government policies, standards, and practices. These are records that document or provide evidence of a ministry’s business activities… Official records should be stored securely so that they will be readily available to those who need them and are authorized to access them. They must be retained and disposed of in accordance with an approved Records Retention and Disposition Schedule.”[2]

While Service Alberta’s document “Official and Transitory Records: A Guide for GoA Employees” is the current authoritative source for GoA staff to use when identifying official records, they also publish “Managing Electronic Mail in the Government of Alberta”, dated February 2005 (attached as Appendix E). This document includes directions for departments to establish email management procedures, and in particular, has guidelines related to where emails designated as official records should be stored.[3]

Service Alberta has posted several resources online, at www.alberta.ca/managing-government-information.aspx, including an Email Decision Diagram (attached as Appendix F) to assist GoA

[1] Service Alberta noted that transitory records are governed by the Transitory Records Schedule (1995/007-A001). It emphasized that, “Transitory records cannot be routinely destroyed when there is a FOIP request or litigation.”

[2] Service Alberta noted that, “Departments may have established additional processes, procedures, and guidance on where official records are to be stored (i.e., Exchange to a PST file, file share, SharePoint), due to differing technologies, processes/procedures, or regulatory requirements.”

[3] Service Alberta noted that, “Managing Electronic Mail in the Government of Alberta is no longer an authoritative source for enterprise guidance, and was removed from Enterprise Information Management’s website June 2017 as other guidance materials (i.e., Email Tip Sheets, Official and Transitory: A guide [sic] for Government of Alberta Employees) have superseded the publication from 2005.”

staff to determine whether an email is an official or transitory record. This resource is very detailed and makes it clear that there is no specific requirement that only the sender of an email is responsible for classifying and retaining an official email record. The document requires that all staff members review and classify every email record they send or receive.

Service Alberta have also prepared online education training modules. Service Alberta noted that, “The online training modules require GoA employees to log in using network credentials (gov.ab.ca) through a learning management system, which tracks course completions. Completion statistics for GoA employees are regularly provided to departments and sector IMT professionals. Due to network access restrictions individuals from Agencies, Boards and Commissions (ABCs) access modules hosted on a web server. As there is no requirement to log in, we are not currently able to track completion rates for ABCs.”[4]

Service Alberta’s guidelines indicate that official records are to be stored in an appropriate recordkeeping system, which they define in their online education module as, “Recordkeeping is the creation and maintenance of complete, accurate and reliable evidence of business transactions. Recordkeeping systems are information systems capable of capturing, maintaining and providing access to records in all media over time.”

In Service Alberta’s “Managing Electronic Mail in the Government of Alberta” document, on page 16, they list the following options for how to store official email records:[5]

a. In folders within each staff member’s email mailbox,

b. within a broader electronic records and document management system, or

c. printing off the record and including it in the manual records retention system.

Service Alberta does not provide any guidance on which method is preferred, nor whether the email storage method should be standardized within a department.

Service Alberta was specifically asked for their role in the GoA’s records management program. The response was that Service Alberta provides enterprise guidance on the management of government records, as per the *Records Management Regulation*. They also stated that each individual department is responsible for ensuring that the guidance and standards provided by Service Alberta are being followed.

The regulations appear to absolve Service Alberta of the responsibility for ensuring that GoA staff comply with the regulations, standards and procedures, assigning that responsibility to each department’s deputy minister. However, Service Alberta still retains the ability to evaluate each department’s records management program.

[4] Service Alberta added that, “Information Management eCourses launched in June 2017, promote awareness of the importance and benefits of managing information effectively. They provide advice and resources to manage the information you receive, collect or create at work. Participants are not able to proceed/complete the modules unless correct responses are provided throughout the eCourse.”

[5] Service Alberta noted that, “Managing Electronic Mail in the Government of Alberta is no longer an authoritative source for enterprise guidance…”

When we asked if Service Alberta actually evaluates any department's records management program to ensure that they are complying with the *Records Management Regulation*, Service Alberta did not specifically respond. Service Alberta instead reiterated that it is the responsibility of each department to ensure that they are complying with the regulations. Service Alberta did mention in their response that they are in the process of developing a compliance program that will include reviewing whether departments understand and follow information management guidance/standards. No further details on this compliance program were provided.

D. Alberta Education's Email Management Program

Alberta Education's records management policy dates from April 4, 2011. It refers to the *Records Management Regulation* and several Service Alberta guidelines. The policy includes a requirement that all department staff must attend records and information management training/awareness sessions.

A cross-government review of records management was undertaken in 2012. Following this review, Alberta Education initiated its own review of records management practices. This resulted in some changes to the way Alberta Education managed records.

Since 2014, Alberta Education has produced several training and awareness resources to complement Service Alberta's online resources. Some of these are designed to better explain, in simple terms, records management and assist the staff member in determining which records are official records, while others are specific to email management.

Alberta Education encourages their staff members to take training seminars and use online tools, but they do not monitor who has taken the training, and there is no evaluation to grade how well the staff members understand their records management responsibilities.

Alberta Education requires that emails designated as official records should be saved as a file and stored on Alberta Education's network servers, either in an appropriate group file share or within one of Alberta Education's SharePoint sites. There does not appear to be any monitoring of this to verify that it is being complied with.

Following the first access request, Alberta Education launched an informal program in the spring of 2016, and a more formal program in the summer of 2016, with an emphasis on training staff to better manage the contents in their email mailbox. Although the goal of the program was to reduce overall mailbox size, the material emphasized that staff members must classify emails as either official and transitory records before determining if an email could be deleted. The programs also reinforced how official records should be treated.

Alberta Education has an Employee Departure Guideline that requires staff members who will be retiring, leaving indefinitely, changing departments, etc. to plan with their manager ahead of time to ensure that any official records in their possession are transferred to the appropriate person, and transitory records are deleted. A training video and checklist is included with the guideline.

Alberta Education does not have any policy or procedure in place to carry out random spot-checks of staff members to evaluate the effectiveness of their training programs. They are not aware of any compliance evaluation of the records management policies and procedures by Service Alberta.

E. Alberta Transportation's Email Management Program

Alberta Transportation provided a copy of their Records & Information Management Policy, dated April 29, 2017. This is the first records management policy for this department. Prior to 2017, Alberta Transportation did not have any formal records management policy or training program for staff members.

In the summer of 2017, Alberta Transportation launched a program called the "Electronic Records Improvement Project", with the stated goal of reducing the number of transitory files and emails. An email, dated June 29, 2017, was sent to all staff (attached as Appendix G). The email indicates that the goal was to reduce the number of files within each staff member's My Documents folder, and the number of emails within each staff member's mailbox, both by 25%. An incentive, in the form of a draw for a $50 Apple gift card, was offered to those who achieved the greatest reduction in volume. Several resources (guidelines and online training) were offered, and each staff member was invited to attend a one-hour training session.

According to Service Alberta, the training sessions were attended by 141 staff members. Alberta Transportation monitored email mailbox sizes throughout 2017 to measure the effectiveness of their program. Alberta Transportation provided us with two graphs showing the volume of email stored month to month in 2017 and the rate of growth measured month over month in 2017. While the volume of emails stored in the system increased every month, the rate of growth declined gradually after June 2017. Alberta Transportation interpreted this to mean that their staff were managing their emails better, deleting transitory and obsolete emails. They did not provide any specific evidence to verify that the decrease in the growth of mailbox size was due to just the deletion of transitory and obsolete emails (i.e. the type of information being stored in the mailboxes was not determined, just the size).

We asked Alberta Transportation who won the Apple gift card. Their response was that they did not hold the draw, nor did they award the Apple gift card to any staff member. No reason for cancelling the draw was provided.

Prior to the 2017 records management program, Alberta Transportation did not provide guidance or training to staff members as to where official records should be stored, and most staff either retained all email without classifying them as official or transitory, or retained official email records in their email mailbox. The 2017 initiative included guidelines to store official email records in a centrally accessible repository (either network group file share or SharePoint site). However, as of mid-2018, Alberta Transportation advises that most staff members are still storing official email records in their own mailboxes.

Alberta Transportation's policy with respect to retired email mailboxes is that Service Alberta, who manages the email server infrastructure, copies all emails within the mailbox to a PST file (a portable mailbox file). The PST file is provided to the Service Request Coordinator within Alberta Transportation, who has 90 days to copy emails to other locations. At the end of 90 days, the PST file, and all remaining emails within, is deleted. The Service Request Coordinator is supposed to work with the local manager to assess the contents of the mailbox and extract records that should be retained.

Alberta Transportation expects that the departing staff member will move or forward official record emails to another staff member before they leave. They do not yet have a policy or guidelines in place to specifically define the steps that should be taken by the staff member but expected one to be approved before the end of 2018.

Alberta Transportation does not have any policy or procedure in place to carry out random spot-checks of staff members to evaluate the effectiveness of their training program. They are not aware of any compliance evaluation of the records management policies and procedures by Service Alberta.

F. Interviews with Senior Staff Members

The information exchanges with Alberta Education and Alberta Transportation revealed some details of how departments typically guide their staff to manage emails. Given that neither department carries out any review of actual staff practices, and Service Alberta does not carry out any compliance evaluations of staff practices, the information obtained from these sources was insufficient to evaluate actual compliance with the guidelines.

The Official Opposition had specifically highlighted senior staff members who had very few emails in either their inbox folder or in their entire email mailbox and questioned whether these individuals were complying with the records management requirements.

To address the Official Opposition's concerns, and develop more of an appreciation of how well individual staff are complying with records management procedures and guidelines, eight senior staff members from a set of 75 people identified as those with few emails were randomly selected for face-to-face interviews. A standard list of questions was developed.

Based on the interviews:

a. Most people move official email records and transitory email records into either subfolders of the inbox folder or to folders and subfolders at the root level of the mailbox. Very few people actively deleted emails. This would account for the situation where an individual had very few records in their inbox folder compared to the number of records in their sent items folder;

b. Two of the people interviewed said that they actively deleted most emails they received and sent. When asked why, they indicated that they sent and received very few emails that would be considered official records. We asked the nature of the emails they sent and received that would not be considered official records and were told that they were generally requests for information or replies to requests for information. Both confirmed that they had taken the online records management training modules;

c. Seven of the eight people interviewed had taken some online records management training courses; one individual had not taken any online training, claiming it was unnecessary because they already understood what an official record was. This individual moved email out of their inbox folder into other folders, but deleted very little email;

d. All interviewees said that they were not aware of any evaluation or other steps to measure how their staff members were complying with the guidelines;

e. Only one interviewee mentioned that they use a central repository in their department to store official record emails. This person actively encouraged the staff members in their department to store emails in the central repository.

G. GoA Email System

Service Alberta manages the email infrastructure for the GoA. The email system is based on Microsoft Exchange, with staff members accessing their mailbox through Microsoft Outlook, through their GoA-issued mobile device, or through Outlook Web Access via an Internet web browser. As of January 1, 2018, Service Alberta maintained almost 42,000 email mailboxes.

Email messages are limited to 100 MB in size, including message body, headers and attachments.

All staff can copy or move emails from their mailbox to either an offline PST file, save an email as a file on a local or network drive, or save an email to a GoA SharePoint site.

Some email mailboxes have been configured with a specific retention period for certain folders. Once an email reaches the retention age, it is automatically deleted. The intent is for staff members to move emails that they want to retain to another location (another folder in their mailbox, an offline PST file, a file share, or SharePoint) before the retention period is reached, and have the system automatically remove transitory emails. This retention/automatic deletion system can be set up and configured by individual staff members.[6]

Emails moved to the deleted items folder are automatically deleted after 30 days but remain recoverable for an additional 30 days. Emails within the junk folder are automatically deleted after 45 days.

Service Alberta does not apply any system-wide retention limits to emails, except as indicated above for deleted items and junk folders.

Up until December 2015, emails within a staff member's mailbox older than 30 days were automatically transferred to an eVault archiving system. The emails were still accessible to the staff member but were no longer stored in the mailbox.

Since January 2016, all emails remain in a staff member's mailbox unless the email is specifically moved to another location or deleted either explicitly by the staff member or through a retention rule.

[6] Service Alberta noted that, "A 28-day policy is available for individual users to manually apply to any folder within the mailbox with the exception of Inbox, Drafts, Sent Items, Deleted Items. This type of auto delete functionality cannot be applied at the mailbox level."

H. eVault System

Up until December 2015, Service Alberta used an eVault system to store older emails. The system would automatically move emails older than 30 days from the staff member's mailbox and replace the email with a "stub". The stub provided a link to the moved email, so that the staff member could retrieve it if necessary.

Service Alberta began decommissioning the Symantec eVault system in December 2015 and completed the work in November 2017. All emails that had been archived into the vault were returned to the original custodian's mailbox. If the original mailbox no longer existed, the emails were exported to a PST file and delivered to the appropriate department to be managed in the same way that retired email mailboxes are managed.

Service Alberta maintained audit trails of all emails restored from the eVault to ensure there would be no data loss as a result of the eVault decommissioning.

I. Service Alberta's Process to Compile Email Mailbox Sizes for Access Requests

When the Official Opposition issued the first access request in the fall of 2015, Service Alberta did not have a standard method of collecting the requested data. To meet the request, Service Alberta technicians created a custom script. Due to the different information required in the second access request, a second script was created to compile the necessary information. Existing billing reports were not used to compile the information.

Logs and operating notes associated with the operation of the first script were not available. Logging was incorporated into the second script. The only errors reported were associated with gathering record counts in staff members' drafts folder. A total of 37,263 email mailboxes were scanned by the second script; 7,308 were identified as non-person mailboxes. Record counts for the remaining 29,955 mailboxes were reported. The script ran for approximately 10.5 days.

5. CONCLUSIONS

The GoA's overriding records management regulation is Alberta Regulation 224/2001, *Records Management Regulation*. This regulation requires that Service Alberta set out the procedures and standards that each GoA department should follow but assigns responsibility for implementation of the records management plan to each department. Service Alberta is responsible for evaluating each department's records management plan to ensure that it meets the requirements.

According to the "Official and Transitory Records: A Guide for Government of Alberta Employees" produced by Service Alberta (Appendix D), except in the case of legal or access request holds, only official records need to be preserved. Transitory records can be disposed of once they are no longer needed.

The Service Alberta guidelines, standards and procedures appear to be very detailed, and emphasize the need to identify and segregate official records from transitory records. However, we have identified two areas that appear to be missing:

a. Consistent storage location for official records. Although Service Alberta lists a number of different locations where official records can be stored, there is no requirement that all staff members in a department use the same storage location. Each staff member is left to decide where official records will be stored. The consequence of this is that official records tend more often than not to be stored in individual email mailboxes. This could lead to official records being inadvertently deleted when mailboxes are cleaned up and makes it much more difficult to find official records when they are needed for GoA business, legal or FOIP Act responsibilities.

b. Compliance assessment to ensure that staff members have received the appropriate training and are following the records management plan for their department. The *Records Management Regulation* gives Service Alberta the right to evaluate the creation and implementation of each department's records management plan. However, it appears that evaluations are not being conducted. The guidelines, standards and procedures produced by Service Alberta do not include any recommendations for departments to check that their staff understand and are complying with the requirements. There is currently no way to measure the extent to which GoA staff members are actually meeting the *Records Management Regulation*.

The lack of consistency in how official records are being stored and no oversight to ensure that the requirements are being followed are significant findings. These are two key aspects of a sound records management plan.

Some individual staff members appear to have insufficient training to understand the definition of an official record and could be deleting records that may otherwise have to be retained. For example, two of the interviewees claimed that they sent and received very few emails that would be considered official records, as they mostly sent and received requests for information. The training material indicates that records needed to support business decisions are official records. Requests and replies for information would likely fall into the category of supporting business decisions. More specifically, the Transitory Records Schedule (1995/007-A001) attached to Service Alberta's "Official and Transitory Records: A Guide for Government of Alberta Employees" states that, although drafts and working materials may be considered transitory, "In some cases, offices responsible for drafting legislation (acts, regulations, orders-in-council), legal documents (contracts, agreements, etc.), policy, audit reports, budgets, standards, guidelines, procedures, communications materials (publications, posters, films, etc.) or for conducting scientific research (laboratory notes, calculations, etc.) might need to track the evolution of the final product. These offices may need to keep various drafts, research and working materials in order to have a record of changes that were made and why."

Based on the raw mailbox records counts obtained from the access requests and our interviews, any lack of retention appears to be limited to a very small number of individuals. Implementation of a compliance measuring system should identify these people. Given that adequate education resources are available, once identified, these individuals should be able to be properly trained.

It does appear that most people are retaining more records than required, based on the following:

a. The majority of email mailboxes reported in the responses to the access requests contained at least 50,000 records, with many over 100,000 records.

b. Five of the eight people interviewed said that they keep more than just official records "to be on the safe side".

c. Although Alberta Transportation's findings from monitoring email mailbox sizes during 2017 showed that the rate of growth of mailboxes decreased after they launched their training program, the size of mailboxes still increased, suggesting that new transitory email may have been deleted, but older transitory email was remaining in the mailboxes.

Most official email records appear to be saved in individual staff members' mailboxes (seven of the eight interviewees said that they never move emails out of their mailbox, instead storing official record emails within their mailbox folders). This makes it more difficult to find responsive information, whether for business reasons or to meet litigation and regulatory requirements as individual mailboxes can only be searched one at a time, searching mailboxes is time consuming, not all records can be searched (such as scanned documents), and the individuals with responsive information needs to be known ahead of time. If the responsive information is not found as a result of how it is stored, the end result is the same as if the information had been deleted.

We did not find any indication of intentional deletion of official email records. Where official records may have been deleted, it appeared to be due to lack of understanding of what constitutes an official record (as discussed above with respect to two staff members who were interviewed). We also did not find any indication that the contents of retired mailboxes, or emails restored from the discontinued eVault system, were automatically deleted, as claimed by the Official Opposition. None of the people interviewed said that they save emails outside their mailbox (such as in offline PST files as suggested by the Official Opposition).

Although extensive education and training resources are available, and departments are trying to educate their staff, the training is not compulsory.[7] An evaluation or test following the training modules would ensure that staff understand how to identify an official record.

The number of emails in a GoA staff member's mailbox has no bearing on whether the person is properly identifying and retaining official records. Transitory records do not need to be retained, and official records only need to be retained for the applicable period specified in the department's records retention schedule. Official record emails can be saved outside of the email mailbox.

Based on our analysis, it is likely that the reduction in the number of records in some staff members' mailboxes, while others increased at the same time, was due to a combination of applying better email management following the first access request, end of year mailbox cleanup and archiving, and moving official records from the mailboxes to other repositories. We did not identify any evidence that 859,681 emails had simply been deleted.

Email management awareness prior to the Official Opposition's first access request was inconsistent between departments and was sorely lacking in Alberta Transportation. One noticeable effect of the access requests was increased awareness of how email information was being managed by the GoA staff. This can only have benefits, as identification of official records and simultaneous reduction in transitory emails reduces email volumes, increasing overall efficiency.

[7] Service Alberta noted that, "Some departments have chosen to make Information Management training mandatory (e.g. Environment and Parks). All departments are encouraged to promote this training as an annual exercise." However, no departments subject to this investigation chose to make information management training compulsory.

6. RECOMMENDATIONS

a. When asked whether Service Alberta actually verifies that GoA departments are following the records management guidelines and recommendations, they replied that, “From a compliance perspective, Service Alberta is in the process of developing an enterprise information management reporting and compliance program that will include reviewing whether or not departments understand and follow information management guidance/standards.” Although they did not provide details of the program or when they expect to launch it, we do consider this a positive development. We would recommend that this program include:

   1. Specific requirements for GoA departments to measure and report on the compliance of the records management plan,

   2. Service Alberta should compile annual statistics from each department, and

   3. Service Alberta should work with the departments to develop a method to ensure that all staff members understand and follow the regulations.

b. As part of Service Alberta’s program to review each GoA department’s records management processes (item “a” above), they should develop a method to measure:

   1. Whether each department is retaining the records they should be retaining,

   2. how efficiently each department can find records in response to a business, legal, regulatory or FOIP Act requirement, and

   3. verify that records required by a business, legal, regulatory or FOIP Act requirement are properly identified by each department.

   This process could involve Service Alberta and the departments conducting random tests on a periodic basis. Results could be presented in the form of precision[8] and recall[9], and could be used by Service Alberta to report on each department’s records management state.

c. Service Alberta should begin planning to implement a government-wide official records electronic storage repository, so that records responsive to business, legal, regulatory or FOIP Act requirements can efficiently and accurately be identified.

[8] Precision is the percentage of responsive records retrieved within a set of collected records. For example, if 100 records are collected, and 50 are considered to be responsive, the precision is 50%. Precision measures the efficiency of the collection method.

[9] Recall is the percentage of responsive records actually collected. For example, if 100 responsive records are available to be collected, and 50 records are collected, the recall is 50%. Recall measures the accuracy of the collection method.

Appendix A

Letter from Mr. Nathan Cooper, Official Opposition Caucus

Dated Sept 28, 2017

LEGISLATIVE ASSEMBLY
ALBERTA

Nathan Cooper
UCP Caucus
9820 107 Street
Edmonton, AB T5K 1B2

September 28, 2017

Commissioner Jill Clayton
Office of the Information and Privacy Commissioner
#410, 9925 109 Street NW
Edmonton, AB T5K 2J8

Dear Commissioner Clayton:

I am writing to request that you open an investigation into the management and storage of email by the Government of Alberta. As you may be aware, the Office of the Information and Privacy Commissioner in BC published a report on October 22, 2015 about the "record retention and disposal practices of the Government of British Columbia" and I am concerned that there is a similar problem here. In addition, I am concerned that there may have been direction to delete email and to interfere with our FOIP requests.

Using the FOIP process, our team made requests in an attempt to capture the information we were looking for, which was how political staff and senior figures in the government use email. Our first request was for the amount of email in a user's inbox; our second was for the number of email in the mailbox; and our third request asked for the amount of email in a user's mailbox folders.

Analyzing the data we received, our team was able to see that a small portion of users appear to have deleted approximately 800,000 email messages over the course of about three months. This 800,000 number represents those messages "missing" when comparing numbers from our third FOIP request to those from our first and therefore does not take into account any additional messages those users received throughout the process. Similarly, it does not capture how much email may have been deleted by the remaining users whose comparisons showed growth in messages.

Several Deputy Ministers, Chiefs of Staff and political staff also appear to have sent ten or fewer emails, despite being in their positions for months or years. For example, senior political staff Brian Topp and Anne McGrath each had only one email in their sent emails folder after nearly ten months on the job, and the Premier's Press Secretary Cheryl Oates had only 77 sent emails. This indicates they are either not creating email records with their public accounts, or they are not retaining those records. This calls into question whether the records found and released through access requests under the current government are complete, or whether important decisions were not recorded or were made through private channels.

We also found other concerning numbers in the data, including:

- Several staff appear to have less than two dozen emails in their inboxes, despite their positions and their time in their role
- It appears that when you leave a position your email account is deleted, even if you remain with the Government: who is responsible for preserving those records? Can FOIP be evaded simply by switching to a new position in the GOA?
- Eight individuals appear to have deleted their mailboxes to zero after our first FOIP request
- Some staff seem to have disproportionate amounts of email in different folders, including one person with a 962:1 ratio of sent to kept emails

I am very concerned with how government departments reacted to these access requests. After receiving our first request in December 2015, the executive team at Education met and discussed it in January 2016, and created briefing note AR 93852 by April. After considering an automated "targeted delete of emails" in the accounts of employees by the IT department, which would certainly have run counter to employees' responsibility to manage their own records, the department settled on mandatory training for employees determined by the volume of email they held. No consideration of the proper retention schedule of records is apparent, rather that focus is on volume of records and the cost of storage. The Transportation Department ran a contest, with the 25 employees who attended training and then reduced their records volume the most entered into a draw for gift cards. The training and the encouragement to reduce volume of records occurred after the numbers we analyzed were returned. While it is commendable that departments placed a priority on training for records management, the fact that the central focus of their concern was on the volume of records they held rather than ensuring proper records retention is particularly alarming. This was the response in two departments, and I am concerned given the evidence that it is indicative of a wider issue in the Government of Alberta.

As well, between our requests the eVault email archiving service used by Service Alberta was phased out. This was a backend archiving system that seamlessly archived old content in a user's mailbox, and appears to have even kept email for former employees. With the system gone, what happened to those emails?

As I have also mentioned, I am concerned with interference in the FOIP process, specifically as it relates to these three requests. In conversations with Service Alberta (who largely spear-headed the coordination of the requests) we were told conflicting information, such as the email numbers not including archives, but also that the Government doesn't use archives, and then later informed about the eVault service which archives email behind the scenes for users. We also have evidence of a conversation including a FOIP manager appearing to coerce an employee to provide a rationale for inflating a fee where there was "no system cost that can be directly related to this request."

As access to information is important for the public, I urge you to consider looking at the issues that I have raised here. I would ask that, should you decide to pursue an investigation, you look primarily at the incidence of records retention and disposition, but that you also consider looking at the issue of interference, whether specific to this FOIP project or using that as a starting point to look more broadly at the issue. Should you require additional information, such as portions or the entirety of the records released to us, I would be happy to provide it to you.

Sincerely,

Nathan Cooper
Interim Leader United Conservative Party
MLA Olds-Didsbury-Three Hills

Appendix B

Province of Alberta
Records Management Regulation

Alberta Regulation 224/2001

Province of Alberta

GOVERNMENT ORGANIZATION ACT

RECORDS MANAGEMENT REGULATION

Alberta Regulation 224/2001

With amendments up to and including Alberta Regulation 34/2018

Office Consolidation

Alberta Queen's Printer
Suite 700, Park Plaza
10611 - 98 Avenue
Edmonton, AB T5K 2P7
Phone: 780-427-4952
Fax: 780-452-0668

E-mail: qp@gov.ab.ca
Shop on-line at www.qp.alberta.ca

Copyright and Permission Statement

Note

All persons making use of this consolidation are reminded that it has no legislative sanction, that amendments have been embodied for convenience of reference only. The official Statutes and Regulations should be consulted for all purposes of interpreting and applying the law.

(Consolidated up to 34/2018)

ALBERTA REGULATION 224/2001

Government Organization Act

RECORDS MANAGEMENT REGULATION

Table of Contents

1 Interpretation

2 Alberta Records Management Committee

3 Chair, vice-chair and secretary

4 Records management program

5 Evaluation of program

6 Approval of records retention and disposition schedules

7 Advice to the Minister

8 Archival appraisal

9 Departmental responsibility

10 Records retention and disposition schedule

11 Destruction of records

12 Repeal

13 Expiry

Interpretation

1(1) In this Regulation,

(a) "Committee" means the Alberta Records Management Committee established under section 2(1);

(b) "department" has the meaning given to it in section 14 of Schedule 11 to the *Government Organization Act*;

(c) "deputy head", in respect of a department, means

(i) the chief officer of the department, or

(ii) if there is more than one chief officer of the department, the chief officer of that part of the department for which he or she is responsible;

(d) "Minister" means the Minister of Service Alberta;

(e) "record" has the meaning given to it in the *Freedom of Information and Protection of Privacy Act*;

(f) "Schedule" means Schedule 1 to the *Freedom of Information and Protection of Privacy Regulation* under the *Freedom of Information and Protection of Privacy Act*.

(2) For the purposes of this Regulation, an agency, board, commission, corporation, office or other body listed in the Schedule is considered to be a department.

AR 224/2001 s1;251/2001;35/2007;186/2008

Alberta Records Management Committee

2(1) There is established the Alberta Records Management Committee consisting of the persons appointed as members under subsection (3).

(2) On the request of the Minister, nominations must be made in accordance with the following and submitted to the Minister:

(a) 5 people must be nominated by the Department of Service Alberta;

(b) one person must be nominated by the Provincial Archives of Alberta;

(c) one person must be nominated by the Department of Justice and Solicitor General;

(d) one person must be nominated by the Department of Treasury Board and Finance;

(e) repealed AR 68/2008 s17;

(f) repealed AR 9/2006 s2.

(3) The Minister may appoint as members of the Committee

(a) the persons nominated in accordance with subsection (2), and

(b) any other persons the Minister considers appropriate.

(4) A person nominated under subsection (2)(c) may in writing designate an employee of the Government who is under the administration of the Minister of Justice and Solicitor General to attend and act on behalf of the person at one or more meetings of the Committee.

AR 224/2001 s2;9/2006;35/2007;68/2008;31/2012;170/2012;
62/2013

Chair, vice-chair and secretary

3 The Minister must designate a chair, vice-chair and secretary for the Committee from the persons nominated under section 2(2)(a).

AR 224/2001 s3;9/2006

Records management program

4(1) The Minister is responsible for establishing a records management program.

(2) For the purpose of providing the details for the operation of the records management program, the Minister may establish, maintain and promote policies, standards and procedures for the creation, handling, control, organization, retention, maintenance, security, preservation, disposition, alienation and destruction of records in the custody or under the control of departments and for their transfer to the Provincial Archives of Alberta.

Evaluation of program

5 The Committee may evaluate the implementation of the records management program in each department.

Approval of records retention and disposition schedules

6(1) A records retention and disposition schedule and any subsequent amendment to it must be approved by the Committee before it is implemented in the department.

(1.1) The Committee or the secretary of the Committee on the Committee’s behalf may set an expiry date for and approve amendments to a records retention and disposition schedule and, where it is no longer required, cancel a records retention and disposition schedule.

(1.2) Notwithstanding subsection (1.1), the secretary of the Committee may not approve an amendment of the type described in section 10(2)(b) or (e) to an approved records retention and disposition schedule of a department.

(2) The Committee may approve records retention and disposition schedules submitted by the secretary of the Committee that are to apply to all departments.

AR 224/2001 s6;9/2006

Advice to the Minister

7 The Committee may provide advice to the Minister relating to the policies, standards and procedures referred to in section 4(2).

Archival appraisal

8 The member of the Committee referred to in section 2(2)(b)

(a) must provide an archival appraisal of each records retention and disposition schedule submitted by a department, and

(b) may provide advice on archival concerns.

Departmental responsibility

9 The deputy head of a department must ensure that records in the custody or under the control of the department are managed in accordance with the policies, standards and procedures established under section 4(2).

Records retention and disposition schedule

10(1) The deputy head of a department must ensure that the department prepares records retention and disposition schedules for all records under the control of the department.

(2) The records retention and disposition schedule must

(a) describe the records under the control of the department,

(b) specify how long the department must keep the records,

(c) specify where the records must be kept,

(d) specify the format in which records must be stored, and

(e) describe what the final disposition of the records will be.

(3) Repealed AR 9/2006 s5.

(4) Records may be disposed of only in accordance with the approved records retention and disposition schedule.

AR 224/2001 s10;9/2006

Destruction of records

11 The deputy head of a department must ensure that records are destroyed only in accordance with policies established under section 4(2).

Repeal

12 The *Records Management Regulation* (AR 57/95) is repealed.

Expiry

13 For the purpose of ensuring that this Regulation is reviewed for ongoing relevancy and necessity, with the option that it may be repassed in its present or an amended form following a review, this Regulation expires on March 31, 2023.

AR 224/2001 s13;9/2006;33/2016;35/2017;34/2018

9780779802647

Printed on Recycled Paper

Appendix C

IMT Standard Oversight Committee
Government of Alberta

Standard Number A000024

IMT Standards **IMT Standards Oversight Committee** **Government of Alberta**	**Effective Date: 2011-11-08** **Scheduled Review: 2018-10-04** **Last Reviewed: 2017-10-04**
	Type: Process
Standard number A000024	
Records Management Program Standard	
Category: IM **Keywords: Records Management, Information Management, ISO 15489, Standard RM Processes**	

Description of Standard

This standard provides the foundation for establishing a records management program in the Government of Alberta (GoA).

This standard will help to ensure:

- The integrity of the records management program;
- The authenticity and reliability of records;
- That appropriate attention and protection is given to all records; and
- That evidence and information contained within those records can be retrieved efficiently and effectively.

Standard Specification

This standard is specified by:

- ISO 15489-1:2016 (E): Information and documentation – Records management – Concepts and principles

ISO 15489-1:2016 (E) is published by the International Organization for Standardization and applies to the management of records in all formats or media that are created or received in the conduct of GoA activities.

Outlined below are foundational principles for records management programs. For additional information, please consult ISO 15489-1:2016 (E).

Managing records is based on the following principles:

- The creation, capture and management of records are integral parts of conducting business, in any context.
- Records, regardless of form or structure, are authoritative evidence of business when they possess the characteristics of authenticity, reliability, integrity and useability.
- Records consist of content and metadata, which describes the context, content and structure of the records, as well as their management through time.

- Decisions regarding the creation, capture and management of records are based on the analysis and risk assessment of business activities, in their business, legal, regulatory and societal contexts.
- Systems for managing records, regardless of their degree of automation, enable the application of records controls and the execution of processes for creating, capturing and managing records. They depend on defined policies, responsibilities, monitoring and evaluation, and training in order to meet identified records requirements.

ISO 15489 provides the GoA records management principles and establishes a framework to support the management of records. Further, it provides a monitoring framework, so compliance can be measured.

ISO 15489-1:2016 (E) provides guidance:

- To assist staff with routine, yet critical, records management tasks;
- For managing organizational records and ensuring that records are created, captured, and managed;
- For determining the responsibilities of organizations for records and records policies, procedures, systems, and processes; and
- On the design and implementation of a records system.

This standard does not include the management of archival records collections within the Provincial Archives of Alberta.

Terms

Authenticity: An authentic record is one that can be proven to:

- Be what it purports to be;
- Have been created or sent by the agent purported to have created or sent it; and
- Have been created or sent when purported.

Integrity: A record that has integrity is one that is complete and unaltered.

Record(s): “Records” means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records[1].

Records management: Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records. Includes processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records.

Reliability: A reliable record is one:

a) whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest; and
b) which can be depended upon in the course of subsequent transactions or activities.

Useability: A useable record is one that can be located, retrieved, presented and interpreted within a time period deemed reasonable by stakeholders.

Where to Apply This Standard

This standard applies to all departments defined under schedule 11 section 14(1) of the *Government Organization Act*.

Authority and Exceptions

Unrestricted

Supporting Documentation

- ISO 15489-1:2016 (E): Information and documentation – Records management – General
- ISO 15489 Update Reference Guide

Owner

Service Alberta, Information Management Branch
SA.InformationManagement@gov.ab.ca

Contact

GoA IMT Standards at imt.standards@gov.ab.ca

Additional Information

Audience	Government of Alberta
Source	Service Alberta, Information Management
Sensitivity	Public
Proposed Date	2011-02-01
Proposed By	Service Alberta Maureen Towle, Executive Director Information Management Branch

1) ISO 15489 (2016) provides an alternate definition of record(s). The definition above is GoA's definition of record(s) - *Freedom of Information and Protection of Privacy Act*.

Appendix D

Official and Transitory Records: A Guide for Government of Alberta Employees

Official and Transitory Records: A Guide for Government of Alberta Employees

Alberta Government

Contents

Introduction 2

Scope and Audience 2
Relevant Acts and Regulations 3

Records in the GoA 3

What is a record? 3
What Are Official Records? 4
What Are Transitory Records? 4
Examples of Official Records 5
Examples of Transitory Records 5
Roles and Responsibilities in Managing Official and Transitory Records 6
How to Decide Which Records Are Official 6
How to Decide Which Records Are Transitory 6
Exceptions 7
When There Is a *FOIP* Request or Litigation 7

How to Securely Dispose of Transitory Records 8

Disposing of Non-Confidential Records 8
Disposing of Confidential Records 9

Appendix 1: Official and Transitory Records Decision Diagram 10
Appendix 2: Tips for Controlling the Growth and Disposing of Transitory Records 11
Appendix 3: Acceptable/Unacceptable in Locked Bins and Transitory Boxes 12
Appendix 4: Transitory Records Schedule (1995/007-A001) 12

Introduction

The Government of Alberta (GoA) is the trusted steward of information held on behalf of Albertans. The quality, reliability and integrity of information are critical to good decision making in the government. The GoA's ability to respond to the needs of Albertans depends on how well it can create, use and preserve information to make decisions and take action to achieve its operational and strategic goals. Along with people and finances, information is a key business resource for the GoA and, as such, the management of that information is critical to achieving the government's priorities.

GoA employees have an obligation to properly document what they do by creating accurate records of their activities and by ensuring that the appropriate records relating to business decisions are retained.

Some records need to be kept indefinitely (land, birth, death, and marriage records) while others can be disposed of as soon as the transaction is completed (advertising materials, meeting invites, and duplicates). To maximize the potential benefit from our information resources we need to manage them effectively. Doing so provides assurance that information-related risks are reduced and that staff are complying with their legal responsibility.

Identifying and retaining official records is an important part of that responsibility. Identifying and disposing of transitory records is just as important. The guidelines in this document are intended to help each government employee to:

- Decide which records to retain,
- Decide which records can be disposed of as soon as they are no longer needed,
- Dispose of transitory records securely, and
- Comply with the requirements of the Records Management Regulation (RMR) and the *Freedom of Information and Protection of Privacy (FOIP) Act*.

Scope and Audience

This guide applies to all records created and held in any format (physical or digital). It outlines how to identify records. This is essential to achieving the right balance between retaining valuable information assets and ensuring that information that has become obsolete is disposed of.

This guide is applicable for all GoA employees, as well as Agencies, Boards, Commissions and Ministers' offices. All government employees are obligated to follow established procedures for identifying and disposing of both official and transitory records.

Relevant Acts and Regulations

When handling records—official or transitory—there are two essential legal authorities to consider:

The **Records Management Regulation** (RMR), enacted under the authority of the **Government Organization Act**, outlines the legal requirements for records management in the Government of Alberta. The *RMR*:

- Mandates the government-wide records management program,
- Assigns accountability to Deputy Heads for management of records in their custody or control,
- Requires records retention and disposition schedules for all government records, and
- Controls the destruction of government records.

The ***Freedom of Information and Protection of Privacy Act (FOIP)*** ensures that the government protects the privacy of individuals by controlling the manner in which public bodies collect, use and disclose personal information. The *FOIP Act:*

- Requires the government to be accountable to the public by providing a right of access to records in the custody or control of the government, subject to limited and specific exceptions, and
- Limits the collection, use and disclosure of personal information by the government and sets rules for the protection of personal information.

Records in the GoA

What is a record?

In the GoA, the *FOIP Act* defines "record" as a record of information in any form and it includes:

- Notes
- Images
- Audiovisual recordings
- X-rays
- Books
- Documents
- Maps
- Drawings
- Photographs
- Letters
- Vouchers
- Papers
- Any other information that is written, photographed, recorded or stored in any manner

Records provide evidence of government business and can be in any medium or format. Decisions we document that are related to our jobs, whether we use a computer, pen, camera or phone, can produce a record.

There are two classes of records: Official Records and Transitory Records.

What Are Official Records?

Official records document and provide evidence of business transactions.
They are records that must be retained and filed in official records systems, and managed in accordance with government policies, standards, and practices. These are records that document or provide evidence of a ministry's business activities**.**
Official records:

- contain information that has ongoing business value,
- are required to support business operations,
- document and provide evidence of business transactions,
- are required by legislation,
- protect the rights of citizens and the government,
- provide evidence of compliance with accountability or other business requirements, and
- have future business, financial, legal, research or archival value.

Official records should be stored securely so that they will be readily available to those who need them and are authorized to access them. They must be retained and disposed of in accordance with an approved Records Retention and Disposition Schedule.

A records retention and disposition schedule is a legal document that outlines how long records are to be kept, where they are to be kept, and what their final disposition will be

What Are Transitory Records?

Transitory records are records in any format that are of short-term value, with no further uses beyond an immediate transaction.

In other words, transitory records are only required for a limited period of time, in order to complete a routine action or to prepare a subsequent draft or final version.

Transitory records:

- have no further value beyond an immediate and minor transaction,
- are produced or received in the preparation of other records which supersede them or for convenient reference,
- are not needed as evidence of a business activity and, as such, can normally be routinely disposed of,
- are not filed in official records systems, and
- are not required to meet legislative or regulatory obligations.

Why is it important to effectively manage transitory records? A significant amount of information retained by organizations is temporary in nature and does not merit long-term retention. It has been estimated that in most cases only 20 percent of recorded information is official, while 80 percent is transitory. Hence, if transitory records are not destroyed, valuable space is taken up on servers and hard drives, in file rooms, workstations and storerooms, and makes it more difficult to locate and retrieve the records that we need.

Examples of Official Records	Examples of Transitory Records
• Policies, directives, briefing notes, • Final reports and recommendations, • Business deliverables, • Draft materials in the preparation of legislation, legal documents, audit reports, etc., • Accounting working papers, • Work plans, schedules, assignments and performance results, • Materials of historical or research importance, • Agendas and minutes of meetings, or • Legal agreements of any kind.	• Advertising materials and junk mail, • Blank information media such as obsolete stationery and blank forms, • Notices of social events such as retirements or office parties, • Duplicate copies used for convenience, • "FYI" email notices on meetings, holidays, boardroom reservations etc., • Photocopies of departmental publications, or • Draft documents, working or research materials used in preparation for the final version.

Roles and Responsibilities in Managing Official and Transitory Records

- All employees are responsible for making decisions in the regular course of their work about which records are official or transitory.
- It is the responsibility of all GoA employees to be able to distinguish official records from transitory records.
- Senior Records Officers (SROs) are responsible for ensuring records retention and disposition schedules are created for all information holdings under the custody and control of the ministry.
- SROs should ensure that requirements for the handling and disposition of records are included in agreements between government organizations and contracted service providers.
- All employees are obligated to follow policies established by their organizations for identifying and disposing of specific types of records.
- The *Transitory Records Schedule* (1995/007-A001) delegates authority to destroy or delete transitory records to every GoA employee. It authorizes the routine disposition of transitory records:
  - Individual employees decide which records should be retained and filed and which records are of immediate or short-term usefulness,
  - Enables the immediate destruction of transitory records,
  - Can be applied to decisions about individual documents, but not to sets of records or file folders in a records series.

NOTE: Transitory records containing sensitive or confidential information must be securely destroyed or deleted (See the subheading How to Securely Dispose of Transitory Records). **Transitory records *cannot* be routinely destroyed when there is a *FOIP* request or litigation.** See the subheading When There Is a *FOIP* Request or Litigation.

How to Decide Which Records Are Official

Consider the following questions when deciding if an information resource is an official record:

- Will the information in the record have some future business, legal, or archival value to the government?
- Does it explain, justify, or document an official action or decision?
- Was it created during the course of official duty?

If the answer to any of the questions above is “yes”, then it is an official record. It should be retained and filed. See Appendix 1: Official and Transitory Records Decision Diagram.

How to Decide Which Records Are Transitory

Determining whether a record is transitory depends on individual judgment of the value of the record. If a record has only immediate value to government and will not be required again, it can be disposed of as soon as we are finished with it. See Appendix 1: Official and Transitory Records Decision Diagram.

Exceptions

The above categories of official and transitory records are not absolute—there are always exceptions to the general guidelines. Records could appear to meet the criteria of being transitory, but the roles of the employees and the use of the information could make them official. For example, a post-it note that documents an approval or a recommendation that could help guide future financial or legal decisions may appear to be transitory because of its format, but it is an official document that must be kept.

Not all drafts are automatically transitory. Offices responsible for drafting legislation, legal documents, policies, budgets, or procedures might need to track the evolution of the final product. These offices may need to keep various drafts and working materials in order to have a record of changes that were made and why.

Not sure whether it is an official or a transitory record?

If you are in doubt, keep the record.

Documents are considered duplicates only when they are exact copies where nothing has been added, changed or deleted.

If unsure, you can ask the SRO in your ministry. A good rule is: If in doubt, keep the record.

When There Is a *FOIP* Request or Litigation

If a *FOIP* request is received, the ability to routinely destroy transitory records is suspended until the *FOIP* request has been processed and any appeal or appeal period has been completed. It is an offence to wilfully destroy records during this time. The same is true during litigation and discovery. GoA legal counsel, your *FOIP* Coordinator, SRO and/or IM manager are responsible for notifying staff when a *FOIP* request has been received or a legal action is underway.

The Alberta Rules of Court require the identification and disclosure of relevant records and information. Once the GoA is served with a Statement of Claim, or if litigation is reasonably anticipated, all relevant records must be preserved. If the litigation goes forward, this evidence will need to be produced. For more information on GoA obligations during litigation and discovery, see Roles and Responsibilities during Litigation and Discovery.

How to Securely Dispose of Transitory Records

As government employees we must make sure that records are disposed of in a secure manner. Information management employees manage the disposition of official records, as well as coordinate the destruction of transitory records containing confidential or sensitive information. However, we all regularly dispose of transitory records when we delete electronic documents and discard paper documents in confidential receptacles or Locked Bins. See Appendix 3 for the proper use of Locked Bins.

The method that should be used to dispose of records depends on the medium of the records, and whether or not they contain sensitive information.

Just like official records, some sensitive transitory records may contain:

- Personal information about individuals,
- Third party business information,
- Cabinet confidences, and
- Draft legislation or policies.

Sections 16-29 of the *FOIP Act* provide guidance on information that could be considered sensitive or confidential. For example, obsolete forms that could be misused should be disposed of as confidential transitory records. These include:

- Old unused cheques,
- Blank letterhead,
- Purchase orders, and
- Requisition forms.

Disposing of Non-Confidential Records

Sometimes, we might need to shred paper transitory records on-site or have it done by a mobile shredding company. If this type of process is used, make sure that the destruction procedure is secure and that the shredded paper is securely disposed of.

The process for disposing of non-confidential electronic records is the same. In the current environment, we should routinely delete emails, spreadsheets, etc. after we have determined that they are transitory records. This means regularly emptying Deleted Items folder, Sent Items folder, Public Folders, and electronic Recycle Bins once the records we need to retain are filed in an organized filing system.

In addition, messages or documents might be automatically deleted by a system after a specified period of time, or when an individual's allocated workspace on a network server is full.

If your organization does this, then it is particularly important to regularly determine which records need to be kept and filed, and delete the rest.

When deleting a transitory record, delete duplicates and drafts of the record that could be located elsewhere such as: C:\ drive, individual workspaces on networks, shared drives, active and archived email folders, flash drives, laptops, and other portable computing devices.

Disposing of Confidential Records

It is not acceptable to place confidential records in regular recycle receptacles. As with official records, confidential transitory records should be collected and disposed of through a secure process in your business unit. Confidential transitory records should not be disposed of through regular recycling procedures which are adequate for non-confidential transitory records. The Alberta Records Centre (ARC) manages the disposition of many of the government's confidential transitory records through contracts with private shredding companies. The process is secure and environmentally friendly.

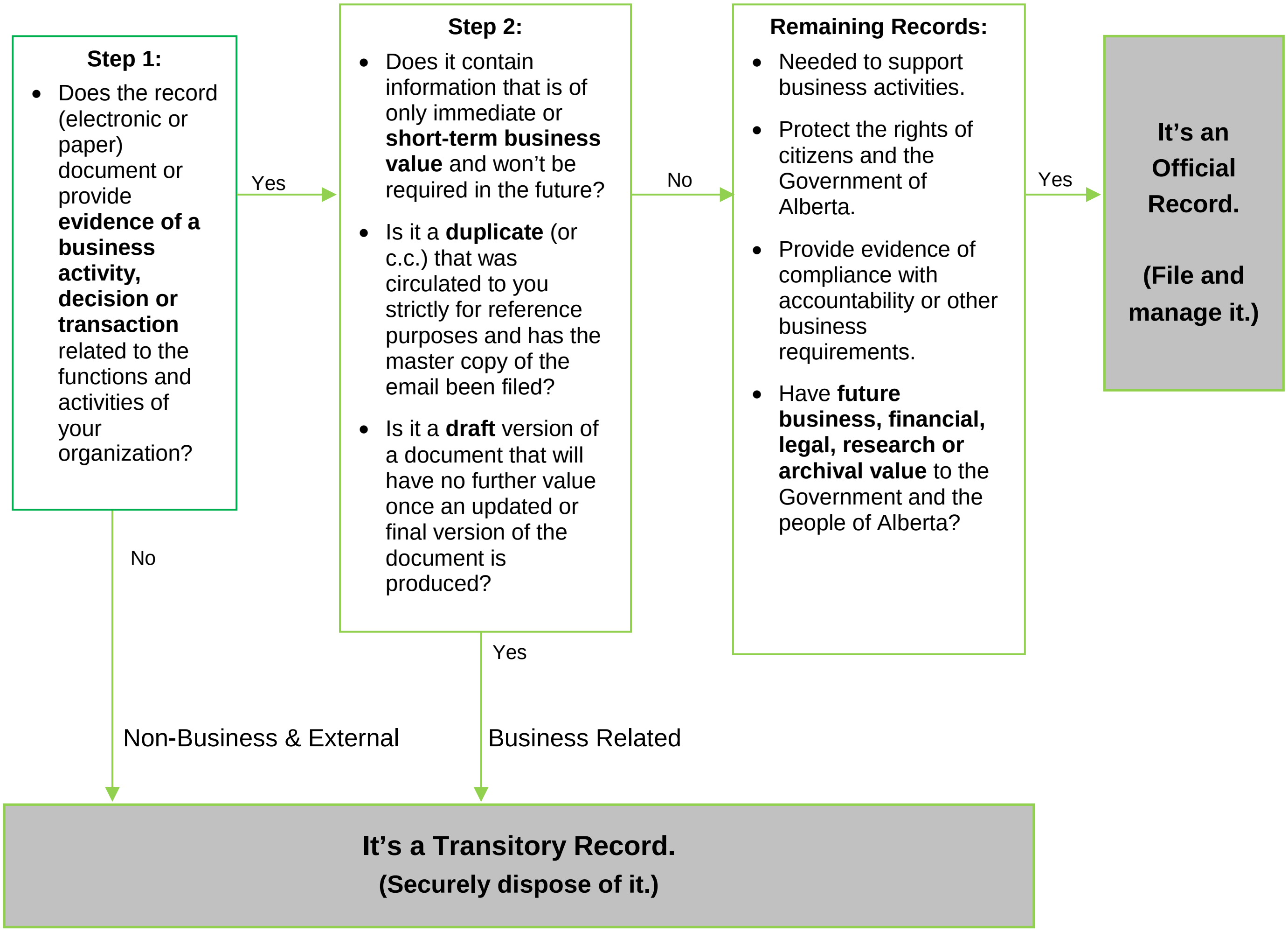
Government computers and electronic devices are often reallocated within and between departments, or sold as surplus outside government. Any official records on reallocated or surplus computers must be copied or moved to another storage device. Transitory records on them must be deleted, and the drives wiped according to government standards before such devices are transferred. The Ministry SRO should work with an information technology (IT) specialist to ensure that records are deleted properly. Failure to do so could result in an inadvertent disclosure of sensitive personal or government information.

Occasionally, to securely dispose of confidential transitory records, we may have to physically destroy other media such as microfilm, audio/video tape, flash drives, CDs, DVDs, or magnetic tapes. As with reallocated and surplus computers, it will be necessary to copy or move any official records to another storage medium before the first medium is destroyed.

If you are unsure whether a transitory record is confidential, err on the side of caution and treat it as confidential. For further assistance, please contact Service Alberta at SA.DispositionServices@gov.ab.ca or call the main line 780-644-3994.

Appendix 1: Official and Transitory Records Decision Diagram

The diagram below can help you identify records that are considered “official” or “transitory” and, thus, should be retained or can be deleted.



Step 1:

- Does the record (electronic or paper) document or provide **evidence of a business activity, decision or transaction** related to the functions and activities of your organization?

Step 2:

- Does it contain information that is of only immediate or **short-term business value** and won’t be required in the future?
- Is it a **duplicate** (or c.c.) that was circulated to you strictly for reference purposes and has the master copy of the email been filed?
- Is it a **draft** version of a document that will have no further value once an updated or final version of the document is produced?

Remaining Records:

- Needed to support business activities.
- Protect the rights of citizens and the Government of Alberta.
- Provide evidence of compliance with accountability or other business requirements.
- Have **future business, financial, legal, research or archival value** to the Government and the people of Alberta?

It’s an Official Record.

(File and manage it.)

It’s a Transitory Record.
(Securely dispose of it.)

Appendix 2: Tips for Controlling the Growth and Disposing of Transitory Records

Here are some common-sense tips for dealing with transitory records:

- Don't create unnecessary transitory records by downloading documents and distributing them as attachments. If possible, link to the original website instead.
- Transitory email should be deleted as soon as no longer required.
- Discard duplicate print and electronic documents when you are sure the master has been filed.
- Dispose of draft versions of documents and working materials that you don’t need to keep when you are sure the final version has been distributed and a copy filed.
- Securely destroy supplies of blank forms and business cards once they are obsolete.
- Discard routine, external publications once they have been circulated and/or you no longer need them.
- Use techniques such as Spam Filters to reduce spam.
- Dispose of information with short-term value once you have acted on it.
- Dispose of advertising material and unsolicited mail as soon as you are finished with it.
- Review emails regularly and delete transitory messages once they are obsolete.
- Erase voicemail messages after listening to them; erase archived messages once you no longer need to save them.
- Keep a recycle box by the photocopier for extra copies and photocopying errors, BUT be sure you don't discard any copies with confidential or sensitive information.
- Make good use of the Locked Bins for confidential transitory records.

Appendix 3: Acceptable/Unacceptable in Locked Bins and Transitory Boxes

Locked bins are for the secure disposal of confidential or sensitive transitory materials that cannot go into the regular building recycle.

Acceptable in the Locked Bins:

- Paper, paper clips, staples, bull clips, some plastics (bindings, coils, covers).
- Small amounts of contaminants (CDs, Discs, DVDs placed in a plastic shopping bag and tied to bin handle will be put into bin on day of pickup).

Unacceptable in the Locked Bins:

- Newspapers, magazines, cardboards, large amounts of plastics, plastic sleeves/pockets, plastic bags, phone books, file folders, Shannon folders (Use building recycle).
- Binders, books, manuals (Send to Surplus Sales outlets).
- Candy wrappers, lunch wrappers, drink cups, decorations, woods, shoes, etc. (Garbage).

Transitory Boxes

- Use recycled ARC box, 8x11 paper box, nothing larger and not exceeding 30 pounds for overflow between locked bin pickups.
- Extra stock can be left in original boxes (envelopes, mail-outs, pamphlets, manuals, letterhead).
- Seal/tape the boxes and write **TRANSITORY** on each box. ***Do not write confidential on any box.***
- Contaminants are non-biodegradable materials in records that cannot be pulped. Some examples are microfilm, tapes/disks, bound book covers, plastic coverings, stamps, mylar, CDs, Discs, DVDs, VHS tapes, file folders, etc.

  Note: For large amounts that are deemed transitory, box separately and indicate on the top of the box “contaminants”.
- All Transitory boxes must be marked with a large **RED X.**

If you are uncertain regarding the acceptable/unacceptable use, please contact Service Alberta at SA.DispositionServices@gov.ab.ca or call our main line 780-644-3994.

Appendix 4: Transitory Records Schedule (1995/007-A001)

Government of Alberta

Service Alberta

Alberta Records Management Committee

Records Retention and Disposition Schedule

Organization Name Service Alberta ** All GoA **	**Org Code** SA **	Schedule Number/Status 1995/007-A001 Approved
Program/Service Name: TRANSITORY RECORDS		

SCHEDULE ADMINISTRATION

Type:
Continuing Schedule

Organization Chart:
External Documents:
Comments: Y

Related Schedule(s):
2008/042 Information Management - Spam E-Mail

Cancels/Replaces Schedule(s):

Amendment History

Number	Amendment to	Date Approved	Item(s)
A001(Minor)	1995/007	Apr 04, 2003	1, 2, 2, 2, 3, 3, 3, 4, 5, 6

Reason for Amendment:

Schedule Transfer History
---------- Originated/Transfer To ----------

Schedule	Organization	Submit Date	Status	Date
1995/007-A001	Government Services	Aug 01, 2007	Completed	Aug 07, 2007

Transfer Comments: SRO: Hollow,Damian (8/1/2007) Comments: Please amend to include all GoA ministries

Schedule	Organization	Submit Date	Status	Date
1995/007-A001	Government Services	Aug 07, 2007	Completed	Aug 07, 2007

Transfer Comments: SRO: Hollow,Damian (8/7/2007) Comments: Please add GoA as secondary org. ARMC: Borys,Linda (8/7/2007) Comments: Schedule transfer requested as a result of the government reorganization in December 2006.

Schedule Cancellation History
---------- None ----------

SCHEDULE APPROVALS

Senior Program Manager: Evans, Gordon	**Date:** Apr 01, 2003

Senior Records Officer: Smith, Diane	**Date:** Apr 03, 2003
ARMC Chair: Thackeray, Tom	**Date:** Apr 04, 2003

APPROVED IN ACCORDANCE WITH RECORDS MANAGEMENT REGULATION (A.R. 224/2001) AND GOVERNMENT ORGANIZATION ACT (R.S.A. 2000, Chapter G-10, Schedule 11)

PROGRAM/SERVICE INFORMATION

Purpose/Function

Transitory records are records in any media that:

- will have no further value to government beyond an immediate and minor transaction; or

- will be only be required for a short time, until they are made obsolete by an updated version of a record or by a subsequent transaction or decision.

Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions and are not filed in official records systems. Records required for business, legal, financial, research or archival purposes must be retained and filed in official records systems and disposed of in accordance with an approved records retention and disposition schedule.

The Transitory Records Schedule delegates authority to destroy or delete transitory records to every Government of Alberta employee. Transitory records containing sensitive or confidential information must be securely destroyed or deleted.

Brief History

The Transitory Records Schedule (# 1995/007) was approved by the Public Records Committee on April 4, 1995. Previously, transitory records were referred to as 'non-record material' and were disposed of under the authority of the Public Records Regulation (repealed in 1995).

Mandate/Legal Authority

Government Organization Act (RSA 2000, Chapter G -10, Schedule 11, Section 14)

Records Management Regulation (Alberta Regulation 224/2001)

APPRAISAL

Archivist: (not on file)	
Manager, Government Records: (not on file)	**Date:**
Director, Provincial Archivist: (not on file)	**Date:**

Organization Purpose:

Business Function

Comments
Special Preservation/Conservation Factors
Special Storage Requirements

OPINIONS

No Opinions Requested.

SCHEDULE ITEMS

1 * Advertising Material

Advertising material includes solicited or unsolicited information received from businesses or individuals advertising their products or services. Examples of advertising material are paper or electronic brochures, company profiles, sales letters, menus, catalogues and price lists. Business units may choose to retain and file advertising material relevant to their operations.

Date Range:

Media: Paper Microfilm Electronic
Other: Audio-visual

Legal Reference:

FOIP Ref :

Closure Criteria: Superseded or obsolete	**Retention On-site:** 0 Year(s)	**Retention Off-site:** 0 Year(s)
Concurrence Conditions:	**Final Disposition:** Destroy	

Items to be cancelled:
None

Reason for Amendment A001: Minor Change to Item Description and Number

2 * Blank Information Media

Blank information media includes anything that was intended to be used for collecting or storing information but was not used, or has been used and erased, and has become obsolete. Obsolete stationery and blank forms are examples. Another example is blank storage media such as video or audio tape, diskettes, compact disks, digital video disks, magnetic tapes or hard drives which must be destroyed to prevent the possible recovery of erased information.

Date Range:

Media: Paper Microfilm Electronic
Other: Audio-visual

Legal Reference:

FOIP Ref :

Closure Criteria: Superseded or obsolete	**Retention On-site:** 0 Year(s)	**Retention Off-site:** 0 Year(s)
Concurrence Conditions:	**Final Disposition:** Destroy	

Items to be cancelled:
None

Reason for Amendment A001: Minor Change to Item Description and Number

3 * Draft Documents and Working Materials

Draft documents and working materials include draft versions of correspondence, reports, and other documents as well as research and working materials collected, and used in the preparation of documents. Once the final version of a document is completed and distributed, and a copy is filed in an official filing system as the master record, most drafts and working materials become transitory records.

NOTE: Not all drafts and working materials are automatically transitory. In some cases, offices responsible for drafting legislation (acts, regulations, orders-in-council), legal documents (contracts, agreements, etc.), policy, audit reports, budgets, standards, guidelines, procedures, communications materials (publications, posters, films, etc.) or for conducting scientific research (laboratory notes, calculations, etc.) might need to track the evolution of the final product. These offices may need to keep various drafts, research and working materials in order to have a record of changes that were made and why.

Date Range: **Media:** Paper Microfilm Electronic
Other: Audio-visual

Legal Reference: **FOIP Ref :**

Closure Criteria: Superseded or obsolete	**Retention On-site:** 0 Year(s)	**Retention Off-site:** 0 Year(s)
Concurrence Conditions:	**Final Disposition:** Destroy	

Items to be cancelled:

1988/081	22	COMPENSATION RESEARCH

Reason for Amendment A001: Minor Change to Item Description

4 * Duplicates

Duplicates are exact copies of documents where:

- nothing has been added, changed, or deleted;
- the copies have been used for reference or information purposes only; and
- the master version of the document has been filed in an official filing system.

A record must meet all three of these conditions to be a duplicate. If something has been added, changed or deleted then it is no longer a duplicate. It could still be transitory, however, depending on the significance and future value of the addition, change or deletion. Some examples of duplicates are

- photocopies of paper documents;
- copies of government brochures and pamphlets;
- duplicates of microfilm, CD-ROMs, DVDs, etc.
- duplicate audio or video recordings;
- electronic copies of e-mail messages and other electronic documents; and
- prints of microfilmed or imaged documents, e-mail messages or other electronic documents that are not the file copies for filing systems.

Date Range: **Media:** Paper Microfilm Electronic
Other: Audio-visual

Legal Reference: **FOIP Ref :**

Closure Criteria: Superseded or obsolete	**Retention On-site:** 0 Year(s)	**Retention Off-site:** 0 Year(s)
Concurrence Conditions:	**Final Disposition:** Destroy	

Items to be cancelled:

None

Reason for Amendment A001: Minor Change to Item Title, Description and Number

5 * External Publications

External publications include books, magazines, periodicals, pamphlets, brochures, journals, newspapers and software documentation, whether printed or electronic, obtained from sources outside an organization. If they will have no future value, they can be discarded after use. Copyrighted information contained in these publications belongs to the publisher under copyright laws, not to the Government of Alberta, despite the fact that the government has purchased the publication.

NOTE:The master copies of publications produced by or for an organization are not transitory and should be filed. Extra copies of obsolete internal publications are transitory. They are examples of duplicates. The Government of Alberta holds the copyright for publications that were developed and issued by or for government organizations.

Date Range:	**Media:** Paper Microfilm Electronic **Other:** Audio-visual
Legal Reference:	**FOIP Ref :**

Closure Criteria: Superseded or obsolete	**Retention On-site:** 0 Year(s)	**Retention Off-site:** 0 Year(s)
Concurrence Conditions:	**Final Disposition:** Destroy	

Items to be cancelled:
None

Reason for Amendment A001: Minor Change to Item Title, Description and Number

6 * Information of Short-Term Value

Documents with information of short-term value contain information that is of little or no interest, or importance to an office or is useful for only a brief period of time after which it has no further value. These documents do not have to be filed and can be routinely disposed of once employees are finished with them. Some examples are

- routine notices or memos regarding holidays or special events circulated to all staff or posted in public folders;
- insignificant or inconsequential information items concerning routine administrative or operational matters;
- other issues not pertaining directly to your office or not requiring you to act;
- personal messages and information; and
- routing slips and opened envelopes.

NOTE: The business units where these types of records originate should retain a *file copy* if the records document their activities and have some future value.

Date Range:	**Media:** Paper Microfilm Electronic **Other:** Audio-visual
Legal Reference:	**FOIP Ref :**

Closure Criteria: Superseded or obsolete	**Retention On-site:** 0 Year(s)	**Retention Off-site:** 0 Year(s)
Concurrence Conditions:	**Final Disposition:** Destroy	

Items to be cancelled:
None

Reason for Amendment A001: Minor Change to Item Title, Description and Number

COMMENTS

Reason for Amendment A001: The Transitory Records Schedule is amended to make the content consistent with the publication: "Official and Transitory Records: A Guide for Government of Alberta Employees" (2002). The items have been rearranged into alphabetical order and renumbered, some item titles have been modified and the item descriptors have been simplified. No changes were made to the closure criteria, retention periods or final disposition of any of the items. (G. Evans, October 17, 2002) The

Provincial Archives concurs. W.M. (October 28, 2002) (TRANSFER) 8/1/2007 Comments: Please amend to include all GoA ministries SRO: Hollow,Damian. (TRANSFER) 8/7/2007 Comments: Please add GoA as secondary org. SRO: Hollow,Damian.

Appendix E

Managing Electronic Mail in the Government of Alberta

Dated February 2005

Information
Management

Managing Electronic Mail in the Government of Alberta

February 2005

GOVERNMENT OF ALBERTA

Produced by

Information Management Branch
Government and Program Support Services Division
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web sites:
http://www.im.gov.ab.ca
http://www.gov.ab.ca/foip
http://www.pipa.gov.ab.ca

ISBN 0-7785-3692-0

Contents

1. Introduction 1

Purpose 1
Scope 2
Implementation 2
Overview 2

2. Government of Alberta Policies On E-mail 4

Authorized use of Government of Alberta e-mail systems 4
Acceptable use of e-mail 4
Transmission of personal information via e-mail 5
Managing e-mail as records 5

3. Establishing E-mail Guidelines and Practices In Ministries 7

Integrating the management of e-mail with other records and information management practices 7
Security of systems and e-mail 9
Ensuring the reliability and authenticity of e-mail 11
Complying with FOIP 11
Monitoring of e-mail 12
Usage practices 13
Roles and responsibilities for managing e-mail 13
Training 14

4. Managing E-Mail At the Desktop 15

Follow your ministry's security and usage practices 15
Manage e-mail messages as records 15
Regularly delete transitory records 16
Identify who is responsible for a message 17
Manage all your e-mail folders 17
Make your e-mail effective 18
Use caution when opening attachments 18
E-mail while out of the office 18

Appendix 1: Identifying and Deleting Transitory Records 19

Appendix 2: Ten Ways to Make E-Mail Effective 20

Appendix 3: Sample Ministry Guidelines and Practices 23

Appendix 4: Glossary 28

Appendix 5: Resources 31

1. INTRODUCTION

Electronic mail (e-mail) is an integral part of doing business today and has replaced a large number of telephone calls, memos and letters.

Although e-mail has helped improve business communications, it is a significant contributor to the perception of "information overload." Many people are unsure of how to manage their e-mail effectively: they don't know what to keep, what to delete, and how to organize the messages they do keep.

It makes good business sense to manage e-mail records. For government, it is also a legislated requirement.

Purpose

The purpose of this guide is to

- bring together existing policies and legislation that govern the management of e-mail in the Government of Alberta;
- describe guidelines and practices that should be established at the ministry level; and
- provide some tips to help individual employees manage e-mail more effectively.

The advice provided will help ministries develop effective practices that comply with relevant legislation related to government records, including the following:

- *Records Management Regulation* governs how records must be managed and the process for approving how long they must be retained. This Regulation also governs the disposition of records – either through destruction, or transfer to the Provincial Archives of Alberta.
- *Historical Resources Act* establishes the Provincial Archives and governs the permanent preservation of government records of archival value to ensure they are available to Albertans in the future.
- *Freedom of Information and Protection of Privacy Act* (FOIP) governs the collection, use and disclosure of personal information, how personal information must be handled and protected, and the right of the public to access records in the custody or under the control of ministries.
- *Health Information Act* governs the collection, use and disclosure of health information, how health information must be handled and protected, and the right of the public to access health records in the custody or under control of health care providers defined under the Act, including the Ministry of Health and Wellness. The Act does not apply to health records retained by other ministries.
- *Electronic Transactions Act* gives electronic signatures and records the same legal status as their paper-based counterparts.

- *Alberta Evidence Act* provides rules on the admissibility of paper records in court proceedings. The *Act* also includes electronic records.
- *Government Emergency Planning Regulation* requires ministries to create plans for business resumption, including the identification and handling of records needed for business resumption after emergencies and the protection of assets, financial records and other records maintained by the ministry.

All of this legislation means that ministries must have in place recordkeeping practices and procedures. This document places e-mail within the context of these requirements.

Scope

These policies and guidelines apply to all authorized users of Government of Alberta e-mail systems. They apply whether the user is using government equipment, their own equipment, or equipment belonging to a third party.

Electronic mail or "e-mail" is electronically transmitted information created on, or received by, a computer system. An e-mail message consists of at least three components – the "envelope" or mail header data, the message content, additional information (metadata) in the message "properties" and frequently attachments as well.

Implementation

These policies and guidelines form part of the government's broader Information Management Framework being co-developed by the Office of the Corporate Chief Information Officer and Government Services. Implementation details will depend on each ministry's individual business requirements, organizational culture and technology architecture.

Overview

This guide contains three main sections:

- The Government of Alberta Policies on E-Mail describes existing government policy and legislation that affects the management of e-mail.
- Establishing E-mail Guidelines and Practices in Ministries provides advice on best practices related to managing e-mail within individual ministries. Ministries are responsible for developing appropriate recordkeeping systems and user guidelines that include the handling of e-mail records.
- Managing E-Mail at the Desktop identifies practices that can help individual employees manage e-mail on a regular basis, whether at their desk or using mobile computing technology.

The policies and guidelines are accompanied by some useful tools in the appendices to this guide including:

- Identifying and Deleting Transitory Records: Employees can use this diagram to help them decide which records they must retain and integrate into their ministry's records management systems and which records they may delete.

- Ten Ways to Make E-Mail Effective: Contains some practical advice to help make e-mail effective and to reduce information overload.

- Sample Ministry Guidelines and Practices: Shows one example of best practices at the ministry level for documenting practices and responsibilities to help employees manage e-mail.

- Glossary: Defines some of the terms used in the policies and guidelines related to managing e-mail messages as records.

- Resources: A list of useful resources related to the management of e-mail.

Note: Several documents listed in this document are available on the Shared Repository (SHARP) (http://www.sharp.gov.ab.ca). This site is accessible to Government of Alberta employees (firstname.lastname@gov.ab.ca) and also to extended stakeholders (i.e. agencies, boards and commissions), consultants contracting with the Government of Alberta and employees of other governments who are registered users of the SHARP web site.

2. GOVERNMENT OF ALBERTA POLICIES ON E-MAIL

Several policies relate to the use and management of e-mail in the Government of Alberta. These policies concern

- the authorized use of the Government of Alberta e-mail systems;
- the acceptable use of e-mail;
- the transmission of personal information via e-mail; and
- managing e-mail as records.

Authorized use of Government of Alberta e-mail systems

Access to Government of Alberta e-mail systems will be based on business needs and will normally be provided to all employees of the Government of Alberta.

The Government of Alberta Information Technology Security Policy allows access to government e-mail systems by staff of other organizations if there is a clear business need for the services and the individuals are contracted by or acting as an agent for a ministry.

Acceptable use of e-mail

The Government of Alberta Internet and E-Mail Use Policy describes the conditions of use by Alberta Government employees of both the Internet and e-mail. Key components of this policy are:

- Authorized users of government e-mail systems are encouraged to use e-mail systems and tools to fulfil their employment duties and to support their ministry's business goals.
- Personal use of e-mail systems is permitted, provided the use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain.
- Users must not bring disrepute to the Government of Alberta.
- Use of the network and e-mail must not conflict with responsibilities outlined in the Official Oath of Office and the Code of Conduct and Ethics for the Public Service of Alberta.
- Users must not violate applicable laws and are expected to use discretion and good judgement when using e-mail systems.
- All users, including remote access users connecting to government systems through the Internet, must take reasonable precautions to safeguard government systems and not to cause damage to government systems.
- Ministries may initiate investigations of e-mail use as warranted.

Transmission of personal information via e-mail

The Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile was adopted by Deputy Ministers in September 2001 and later updated in July 2002 to include implementation guidelines for ministries.

The policy states that any documentation or records containing personal information must not be externally transmitted by electronic mail or facsimile unless

- personal identifiers have been removed;
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other means are employed by both the sender and the recipient to ensure confidentiality is maintained.

The policy also requires that

- automatic address substitution should not be used (e.g. some Internet Service Providers configure e-mail systems to resend mail to another address that may be similar such as joe@xyz.com instead of jo@xyz.com); and
- a statement about inadvertent transmission and receipt should be attached to all e-mail messages sent outside of the Government of Alberta that contain sensitive, personal, confidential or privileged information (e.g. This communication is intended for the use of the recipient to whom it is addressed, and may contain confidential, personal and/or privileged information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. A communication received in error, or subsequent reply, should be deleted or destroyed).

Further details about this policy and its implementation are available from the Office of the Corporate Chief Information Officer.

Managing e-mail as records

In addition to these policies, various statutes and regulations affect the management of e-mail records.

E-mail messages created or compiled on, or sent or received on Government of Alberta e-mail systems are records of the government. These records

- are the property of the Government of Alberta;
- must be managed according to the provisions of the Records Management Regulation and any records management policies, standards and procedures issued by the Alberta Records Management Committee (ARMC) and Alberta Government Services (the ministry responsible for the government's records management program); and

are subject to both the access provisions and the protection of privacy provisions of the *Freedom of Information and Protection of Privacy Act*.

Ministries are responsible for collecting, creating and capturing records that adequately and properly document their organization's

- functions;
- policies;
- decisions;
- procedures;
- resource expenditures;
- operations; and
- delivery of services.

Ministries are also responsible for storing, organizing and retaining these records in such a way that they are available for

- planning and decision-making;
- program and service delivery;
- meeting their obligations to the Legislature to account for their activities, including audits where applicable;
- meeting requests for access to government records by the public, business and other external groups; and
- recovery and business resumption in cases of emergencies or disasters.

Like other records, e-mail records must be managed to meet these requirements.

3. ESTABLISHING E-MAIL GUIDELINES AND PRACTICES IN MINISTRIES

Records in e-mail systems can be managed successfully by application of a combination of policies, management procedures, systems design and user training.

Ministries should establish clear guidelines and practices for managing e-mail relating to

- integrating the management of e-mail with other records and information management practices;
- protecting the security of the e-mail system and messages;
- ensuring the reliability and authenticity of e-mail records;
- compliance with freedom of information and protection of privacy requirements;
- the ministry's practices for monitoring e-mail; and
- roles and responsibilities for managing e-mail.

> E-mail is no longer a messaging system. It is a record-generating and communicating system vital to the business process. The question is whether it is being managed with the same thought and attention that go to other record-generating media. (Ken Withers, "Managing Electronic Mail: The Legal Case," 2001)

The development of such guidelines will require a team approach with the involvement of various groups including IT, FOIP, records management, human resources and business units. See the Sample Ministry Guidelines and Practices (Appendix 3) for an example of how such guidelines and practices can be brought together in a simple form. Ministries should ensure the guidelines and practices are communicated to staff and that training is provided, as needed.

Integrating the management of e-mail with other records and information management practices

The management of e-mail records should be integrated with other records and information management practices for records in the custody or under the control of each ministry.

The best way to do this at the present time is to implement Electronic Information Management (EIM) applications that are designed to manage electronic records through their lifecycle. These types of systems can integrate records management and desktop applications, so that the ongoing capture, organization, retrieval and disposition of electronic records become a routine part of electronic work processes. A corporate Electronic Information Management (EIM) initiative is under way to define GoA requirements and to establish common support tools and practices.

Depending upon the specific applications, EIM technology can address document naming conventions, version control, authentication, workflow, records classification, security, privacy, and records disposition according to approved records retention and disposition schedules. Many EIM applications can also handle the management of paper records with file folder and box level information.

The Government of Alberta's Information Management Framework (IMF) supports this approach. As part of the IMF initiative, the Office of the Corporate Chief Information Officer and the Information Management Branch (Alberta Government Services) are undertaking work that will help ministries implement these systems.

Until EIM integrated systems are in place, ministries and employees must use existing technology to manage e-mail records and other electronic records. There are a couple of approaches to do this, and areas will have to examine the advantages and disadvantages of each approach for different groups of records. Most business units will use a combination of:

1. **Printing and filing** e-mail messages in the existing records management system. Most business units still retain the official records of their programs in paper or microfilm form.

2. Organizing **shared electronic directories** in which to file e-mail messages, word processing documents, spreadsheets and other types of electronic records. Many areas find this approach useful for locating documents quickly, sharing information, and work in progress.

The advantages and disadvantages of each follow:

- **Printing and filing e-mail messages in the existing records management system.**

  The advantages of this option are:

  - It is easy to implement, especially where well-designed and well-understood filing systems already exist.
  - It integrates related records and information from multiple sources in one place.
  - E-mail options can be set to automatically print distribution, receipt and other required information.
  - Standards and procedures are already in place both for organizing and for properly disposing of hard copy records.
  - In existing systems for paper records, various drafts, work in progress, background materials and reference copies of documents are usually housed in individual workstations, clearly separated from business unit filing system.

  The disadvantages of this option are:

  - The ability to search for, retrieve, or re-transmit documents electronically is lost when messages are deleted from the e-mail system after printing.
  - The possible perception by program and IT staff that this method does not use technology to advantage.

- **Managing e-mail electronically**. This requires program staff, records management staff and network administrators to work together to plan and design electronic directory structures for the business unit. Often the best approach is to implement a structure that is substantially similar to the existing filing system.

  The advantages of organizing and storing e-mail in shared network directories are:

  - It's generally quick and convenient for users to move e-mail messages to electronic directories, especially with shortcuts to the folders most often used.
  - Users have convenient and consistent access to all the related records in the directories they are authorized to access.
  - E-mail records are more easily searched and can be re-transmitted and printed as needed.

  The disadvantages of managing e-mail electronically are:

  - Unless security conditions are stringent, users could have much easier access to records and information that should not be available to them.
  - Directories that contain e-mail messages and final versions of other electronic records may also contain drafts and background materials.
  - Significant effort is required to manage the retention and disposition of electronic records from shared directories according to approved records schedules and auditable procedures.
  - Unless the business process is fully automated, and all records are in electronic form, it will be necessary to coordinate filing systems for records in paper and other media with those in electronic format; and
  - Migration strategies are required to ensure future readability and security of stored e-mail records.
  - Any electronic folders with records that have archival value cannot be preserved in the Provincial Archives in electronic form at this time.

Regardless of which approach ministries use for managing e-mail messages, users must have a clear understanding of how to decide which e-mail messages they need to retain and how to store them. Filing systems, whether for paper or electronic records, need to be kept up-to-date, and procedures for disposing of records appropriately must be established and followed.

Security of systems and e-mail

Information technology systems, including e-mail, must conform to the Government of Alberta Information Technology Security Policy.

Most e-mail systems are designed for easy communications, while employing some standard security measures such as access controls, authentication of users, confidential mailboxes and activity reports.

There are several security risks associated with using e-mail to conduct business. These risks include

- the downloading of viruses that infect computer systems;
- the simple misdirection of e-mail to unintended recipients;
- the non-delivery of e-mail; or
- redirection of government e-mail to non-government mail systems (for example, home computers or other public access systems).

Ministries should take all appropriate physical and technical security measures to protect the information transmitted over e-mail.

Practices and guidelines should help users understand the nature of security related to e-mail. Security and back-up measures that are in place for the e-mail system in order to protect records from alteration, loss, or inappropriate destruction may include the following:

- **Virus Protection:** Users should be aware of the virus protection that is provided automatically and of the risk posed by viruses, including 'trojans' that can open their system's confidential files. The guidelines should also identify practices related to the types of attachments that should not be opened and the virus protection that is required for home computers that are used for ministry work.
- **Back-up Procedures**: Back-up measures are usually established for e-mail systems for security and disaster recovery purposes. These permit information to be restored should the system crash or if the e-mail system is damaged in some other way. Users should understand the nature of and timing of ministry back-up procedures. Users should also understand how long back-up versions of e-mail are retained.
- **Password Protection**: Passwords or other access controls protect e-mail systems and workstations from unauthorized users. The guidelines should give users basic advice on choosing and updating passwords and how to protect their passwords.
- **Message Protection and Authentication Controls**: Employees should be made aware that e-mail communication can be forwarded, intercepted, printed and stored by others, thus there is no way to guarantee privacy. Message protection and authentication prevent others from changing an e-mail message once it has been received by at least one recipient. The controls require users to send a new message with new transmission and receipt data if they wish to change the content of a message. The use of these control measures should be explained to users as a vital support within the system for the authentication and version control over e-mail.
- **Security Labels**: Protocols for the use of security labels such as "confidential," should be explained to users. Such labels can be attached to e-mail by senders to alert recipients about special privacy or security handling requirements. The guidelines should describe the circumstances where these measures may be employed and the practices to be used in particular circumstances.
- **System and Audit Trails**: System audit trails automatically record the circumstances surrounding log-in attempts, creation, transmission and receipt, filing and retrieval, updates, and deletion of messages in an e-mail system or on a network. Such practices

should be used where business needs make them appropriate and users should be informed about them.

- **Encryption**: Users should be made aware of the encryption methods available to them, and the ministry practices for using encryption. If encryption methods are available, appropriate safeguards to recover encrypted messages must be in place. Employees should be told very clearly that the communications system is not encrypted by default.

Ensuring the reliability and authenticity of e-mail

Reliability, authenticity, and integrity are the characteristics used to describe trustworthy records from a legal and records management perspective. Ministries need to consider these characteristics when planning and implementing practices related to the management of e-mail.

If e-mail might be used as evidence in court, for claims, or in others types of legal proceedings, it is essential to demonstrate the reliability, authenticity and integrity of the record.

- **Reliability**. A reliable record is one in which the content can be trusted as a full and accurate representation of the transaction, activity or fact to which it attests, and can be depended upon in the course of subsequent transactions.
- **Authenticity**. An authentic record is one that can be proven to be genuine and to have been created or sent by the person who claims to have created and sent it.
- **Integrity**. The integrity of a record refers to it being complete and unaltered.

To ensure the reliability, authenticity and integrity of messages created or received through e-mail systems, ministry procedures should ensure that

- information identifying the creator, receiver, date, and transmission of the message is maintained;
- the e-mail cannot be altered and, if it is forwarded, the original message cannot be changed.
- an audit trail is recorded;
- if electronic signatures are used, they are provided via approved methods, can be verified and are retained as part of the message, as prescribed in the *Electronic Transactions Act*; and
- rules concerning the authenticity and integrity of electronic records are followed, as set out in the *Alberta Evidence Act*.

Ministry practices should be explicit in providing users with guidance on maintaining the content, structure and context of electronic messages.

Complying with FOIP

Any records in the e-mail system are in the custody or under the control of the ministry and, thus, may be included in a request for information under the *Freedom of Information and Protection of Privacy Act*.

FOIP Bulletin Number 12:"E-Mail: Access and Privacy Considerations" can assist ministries in complying with their obligations under the FOIP Act by highlighting the access and privacy protection issues raised by e-mail.

Employees may be asked to search their e-mail to locate information pertinent to an access request. Information that has already been permanently destroyed under an approved records retention and disposition schedule need not be recovered (e.g. back-up tapes will likely not need to be searched).

The same rules apply to e-mail as to other types of information subject to an access request. No information that may be responsive to a FOIP request may be destroyed after the request has been received until the request has been completed and all applicable review periods have expired. This remains the case even where approved records retention and disposition schedules are in place.

The Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile prohibits the external transmission of personal information via e-mail unless

- personal identifiers have been removed; or
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other acceptable means are used by both the sender and recipient to ensure confidentiality and protection of privacy are maintained.

The ministry's practices should indicate methods that staff can use when sensitive personal information must be sent by e-mail. For example, one method would be to ensure the personal information is contained in an attachment and to password protect the attachment.

Monitoring of e-mail

E-mail systems are routinely monitored for capacity and storage to maintain the efficiency of the system. However, the ministry's guidelines should clearly state under what conditions the system administrator and other authorized individuals will monitor an individual's e-mail messages. These conditions should take into account the following factors:

- users of the system may have some expectation of privacy;
- general monitoring of e-mail communications for unspecified purposes should not be allowed;
- there will be no secret monitoring or search, except as permitted by law; and
- all collection, use and disclosure of personal information involving an e-mail system will be done in accordance with the legal requirements of the *Freedom of Information and Protection of Privacy Act*.

If monitoring takes place, system users should be asked to help to design the process, be fully informed as to the tools used and how they will operate, and how the collected information will be used.

Usage practices

Ministries should also establish common usage practices that support the effective and efficient use of e-mail. The usage practices will vary depending on the nature of the business and the organization, but could include the following:

- Establish who is responsible for managing the e-mail record. This is especially important in work groups within a ministry or in other instances where many people might receive the same e-mail message. Records should be managed as they relate to business activities of the ministry and as they relate to the activities of the business unit with primary responsibility. This can avoid duplication of effort.
- Ensure that when dealing with sensitive information, the e-mail is sent to the correct recipient(s). This is particularly important if the e-mail is being sent to a long distribution list. Some common practices related to this issue include
    - ensuring the e-mail addresses of recipients are correct;
    - verifying that a distribution list is up-to-date and that the recipients for a particular message are authorized to receive the message before sending it to the entire list; and
    - not forwarding another author's e-mail message to a discussion group, Listserv™, newsgroup or posting it on an electronic bulletin board without the author's permission.
- Review the hidden text in electronic documents before attaching them to e-mail messages to ensure that incorrect or inappropriate information is not conveyed to the recipient. This is especially important if comments have been added or the change-tracking feature has been used to track revisions to the document. The document properties should also be checked to ensure that they reflect the correct title, author and other details.
- Implement practices to reduce the "clutter" or volume of e-mail traffic on a system. Some usage practices for employees in this regard are
    - using "reply to all" only when appropriate (i.e. when all recipients of the original message need to see the reply); and
    - if possible, posting attachments in one location (e.g. an Intranet, shared drive or public e-mail folder where everyone has access to the drive) and "point to them."
- Give guidance on how to handle junk mail (also known as spam), chain letters, e-mail scams and unsolicited attachments. For example, many organizations warn staff not to respond to junk mail as this can verify the e-mail address to the sender making it more valuable and resulting in more junk mail.

Roles and responsibilities for managing e-mail

A section of each ministry's guidelines should address the responsibilities of business managers, program staff, support staff, network administrators, technical staff, and records management staff in regard to the various aspects of managing e-mail.

Business managers should be responsible for ensuring that the records related to their functions, activities and transactions are managed appropriately. It is their responsibility to ensure staff are actually managing e-mail appropriately.

All **users** should be charged with specific responsibilities. These would generally be comprised of the following:

- retaining records of government business, in the format and media required by the ministry and organized in a way that makes them accessible to those authorized to know the contents;
- removing records of personal business and transitory records from e-mail systems on a regular basis;
- protecting all e-mail records from unauthorized disclosure to third parties and from inadvertent loss or destruction;
- protecting personal information in e-mail messages according to the requirements of the *Freedom of Information and Protection of Privacy Act* and government policy; and
- disposing of e-mail records according to approved records retention and disposition schedules.

Systems administrators, FOIP Coordinators, records management and program staff should cooperate in establishing information management rules and best practices for the e-mail system.

Training

Orientation and training should be offered to employees on the general use of e-mail and policies specific to e-mail. Users should have access to training, as needed, to ensure they understand the characteristics of e-mail, the features provided in their work setting and their responsibilities related to the management of e-mail.

The following types of training will be needed by staff:

- training on the basic, intermediate and advanced functions of the ministry's e-mail system;
- training on identifying transitory records (a model training program was instituted at the ministries of Environment, Sustainable Resource Development, and Energy – other ministries may also offer training);
- training on how to manage e-mail records in a manner that is consistent with the ministry's preferred method of managing electronic records (e.g. in electronic records and document management systems, in shared drives, within the e-mail system, in print); and
- training on the ministry's practices (e.g. usage and security).

Managing Information @ Work awareness session materials have been developed to assist ministries.

4.
MANAGING E-MAIL AT THE DESKTOP

Recent studies suggest that employees spend an average of 49 minutes a day managing e-mail, with almost a quarter spending more than an hour a day managing e-mail. (Gartner, 2001)

Most people complain about the number of e-mail messages they receive each day and the time devoted to processing them. While this feeling of "information overload" has many causes – such as receiving unnecessary junk mail – one cause is related to the fact that we all have to manage these messages.

If you set up some basic procedures, you can reduce the anxiety of dealing with this responsibility. Here are some practices that individual users can put in place to help manage e-mail at the desktop.

Follow your ministry's security and usage practices

Learn about the security and usage practices that have been set up in your ministry. These practices will cover things like

- how the ministry integrates the management of e-mail records with other records;
- tools such as passwords, back-ups, virus protection and encryption to protect the integrity of electronic mail and to protect confidential or sensitive information;
- compliance with freedom of information and privacy requirements; and
- other advice on how to manage e-mail effectively.

Manage e-mail messages as records

It is every employee's responsibility to manage e-mail messages as records. Records are evidence of business activities and transactions and can be in any medium or format, including electronic media such as e-mail.

There are two categories of records: official and transitory. Official records are those that

- are required to maintain business operations;
- document and provide evidence of business transactions;
- protect the rights of citizens and the government;
- provide evidence of compliance with accountability or other business requirements; or
- will have some future business, legal, research or archival value to the government and people of Alberta.

Official records should be organized and filed in ministry filing systems. Some examples of such records include

- policies and directives;

- correspondence related to the business of the ministry;
- work schedules and assignments;
- agendas and minutes of meetings;
- any record that initiates, authorizes or completes a business transaction; and
- final reports or recommendations.

If the e-mail message documents government business, you must manage it in the same way you would manage records in other media such as paper. Follow your ministry's guidelines for managing electronic mail and records – in folders within e-mail, within broader electronic records and document management systems, or by printing off records to include in the manual system. If you are unclear about the procedures, talk to the records management contact or Senior Records Officer in your ministry.

Regularly delete transitory records

A significant number of e-mail messages are transitory or temporary in nature and do not merit long-term retention. Transitory messages can be routinely deleted from your e-mail system.

The government's Official and Transitory Records: A Guide for Government of Alberta Employees includes a helpful description of the range of transitory records. The categories that relate most closely to e-mail are:

IMPORTANT

There is personal judgment involved in deciding what is a transitory record.

The categories described here are examples.

Sometimes what appears as a simple message actually documents an administrative or operational activity.

If you are not sure, ask the Senior Records Officer in your ministry.

- **Information of Short-Term Value**: This category includes records containing information that is either of no importance or value to a ministry, or that is only of immediate or short-term use and has no future value. This category would include personal messages and announcements that are not related to the conduct of ministry business. These messages should be routinely deleted as transitory records.

Examples: Simple messages which are the equivalent of a telephone message slip asking a person to contact another person or to coordinate a lunch appointment with a friend; announcements of social events such as retirement parties or a notice concerning holiday celebrations; shared calendars and daily diaries and information notes of little consequence such as sending a birthday or congratulatory message to a relative.

- **Duplicate Documents**: Duplicate documents are exact reproductions of records where
  - nothing has been added, changed or deleted;
  - the documents were created and used only for convenience or reference purposes; and

- the master version of the document has been filed in a records or information system and is scheduled for disposition along with that record series.

Examples: Some examples of duplicate documents in e-mail systems might be a finished document sent to all employees to inform them of a new departmental program, activity or approach to an issue. It could also be a "cc" copy of a message or document sent to the employee.

- **Draft Documents and Working Materials**: These documents are records that contain information that has been used to create a master record. Once a master record has been produced and incorporated into a records or information system, most draft and working materials become transitory records. However, if the draft material documents a policy development process or the basis for assuming an administrative or operational approach, the documents should be incorporated into the records or information system and scheduled as part of a records series.

IMPORTANT

Drafts and working materials should be **retained** if they were used in the preparation of:

- legislation;
- legal documents;
- policies, standards, guidelines and procedures;
- audit reports; or are
- accounting working papers.

Examples: Drafts of correspondence; reports and other documents; calculations; research materials; rough notes; editing and formatting notes; and rough documents.

Identify who is responsible for a message

Some messages, especially messages that are sent to an internal group, may not need to be managed by everyone in the group. For example, if you have a committee or task force working on project, try to decide early on in the process who is going to be responsible for managing the e-mail records of the group. This might save everyone time!

Manage all your e-mail folders

Make sure you manage all your folders – Inbox, Sent Items, Deleted Items, Drafts, and other folders you have created within your e-mail system. While most people manage their "inbox," many forget to manage the records in their "sent items" folder. Since you initiated the messages in your "sent items" folder, it is probably the most important folder to manage and the one most ignored by users.

Empty your "deleted items" folder regularly. If you don't empty the "discarded items" folder, the records remain on the system and are in the custody and under the control of your ministry and remain accessible under the *Freedom of Information and Protection of Privacy Act*. Also, any personal messages you deleted will remain on the system if you don't empty the "deleted items" folder.

Try managing information as it comes in, so you don't have to spend long hours doing it at the end of the week or when you receive a message from the systems administrator informing you that you have exceeded your allocated amount of space on the e-mail server.

Make your e-mail effective

Remember that your colleagues have to manage their e-mail too. Making effective use of e-mail can help everyone better manage information. A tool you can use to help you make your e-mail effective is Ten Ways to Make E-Mail Effective (Appendix 2).

Use caution when opening attachments

Attachments are a serious security threat because of their potential for damage. They can automatically scan the user's address book and send an infected message to the addresses. As well, viruses can be attached to any type of file. The majority of e-mail users open attachments without question, or even have their software open all attachments upon receiving them.

Security precautions for handling attachments include avoiding opening unsolicited attachments, regardless of the sender. As well,

- check with the sender about the authenticity of an attachment before opening it;
- save the attachment to your computer or disc and then scan it with anti-virus software;
- turn off the e-mail function that automatically opens attachments.

E-mail while out of the office

Using the *out of the office* auto reply is a handy way to alert clients and staff of your absence, but there are security aspects involved.

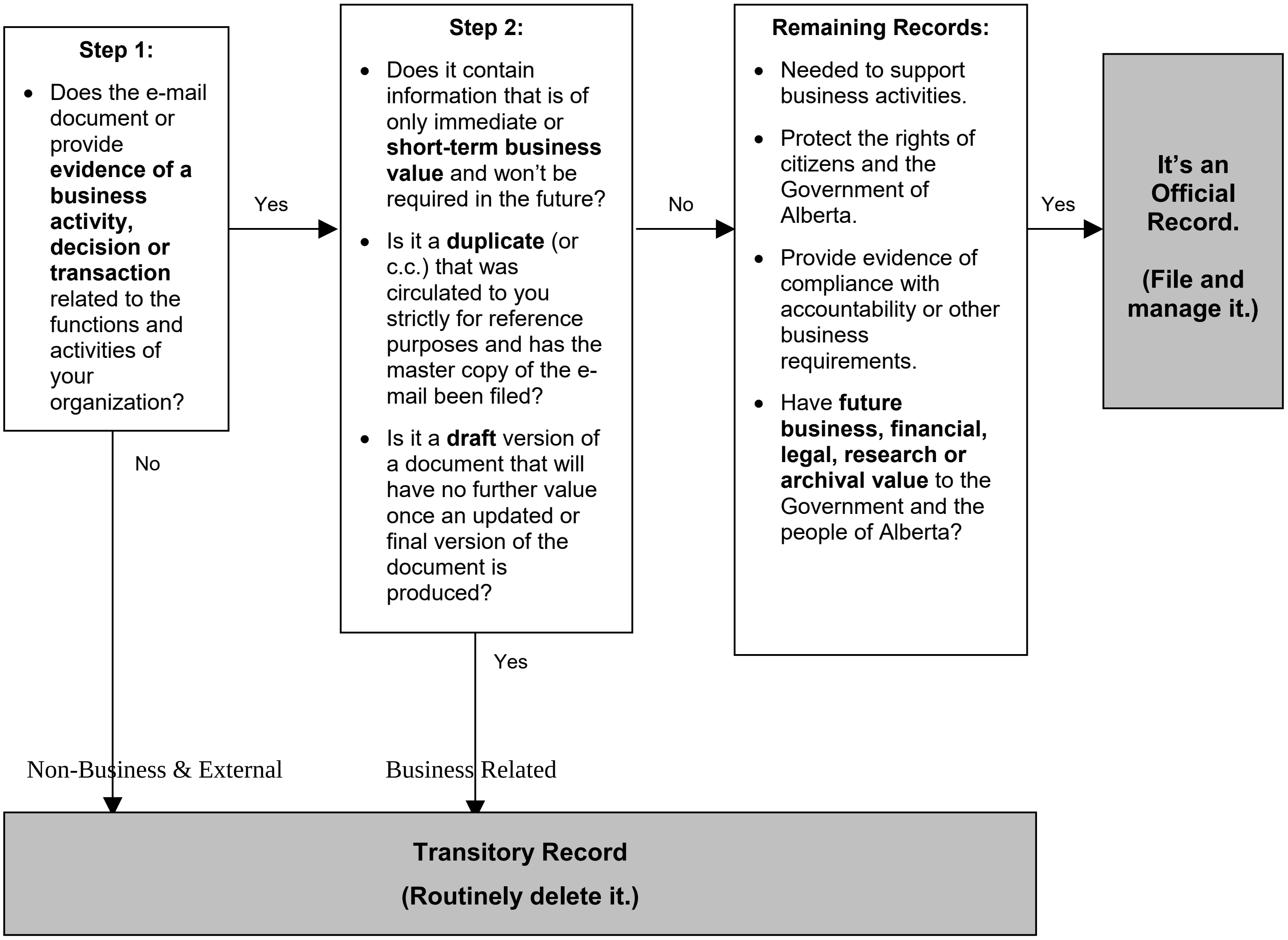
- Alerting people to your absence allows for knowledge of your whereabouts that you might not want known. For example, "I will be out of the office for 2 weeks while in Europe" is valuable information for home invaders.
- If your e-mail uses the reply-all function and you receive department wide e-mail, your *out of the office* reply will spam your own department.
- Consider the appropriateness of using the auto-forwarding feature while you are away and forwarding official government e-mail to your own personal e-mail.

A practical method of keeping up with your e-mail is to appoint a designated person to access your e-mail while you are gone. This can be done by setting up your inbox properties without giving away your password.

APPENDIX 1: IDENTIFYING AND DELETING TRANSITORY RECORDS

What information do I need to keep?

You need to distinguish between official records that document and provide evidence of government business transactions, and will have future value, and transitory records that are temporary in nature and have little administrative or operational value. The diagram below can help you identify records that are considered "transitory" and, thus, can be deleted.



Step 1:

- Does the e-mail document or provide **evidence of a business activity, decision or transaction** related to the functions and activities of your organization?

Step 2:

- Does it contain information that is of only immediate or **short-term business value** and won't be required in the future?
- Is it a **duplicate** (or c.c.) that was circulated to you strictly for reference purposes and has the master copy of the e-mail been filed?
- Is it a **draft** version of a document that will have no further value once an updated or final version of the document is produced?

Remaining Records:

- Needed to support business activities.
- Protect the rights of citizens and the Government of Alberta.
- Provide evidence of compliance with accountability or other business requirements.
- Have **future business, financial, legal, research or archival value** to the Government and the people of Alberta?

It's an Official Record.

(File and manage it.)

Transitory Record

(Routinely delete it.)

The government's Official and Transitory Records: A Guide for Government of Alberta Employees includes a helpful description of the range of transitory records.

Appendix 2: Ten Ways to Make E-Mail Effective

Everyone seems to complain about the volume of e-mail they receive. Here are 10 tips to make your e-mail effective and easier to process for the recipient of your message. The general guideline is, "use common sense when creating and sending e-mail!"

1. **Keep the message as short as possible.**

   While there is no specific size limit, long and complex messages are hard to read, waste time and may be ignored. A message should be as short as possible while providing the recipients the information they need. One subject per message is a good general rule.

2. **Use a short, descriptive subject line.**

   Put yourself in the place of the reader when selecting the wording of the subject line. Will the subject line help them sort the message and prepare them for what they are about to read?

3. **Clearly state the primary audience.**

   State the primary audience at the beginning of the message.

   For example, if the message is to unit supervisors, but all staff are copied (e.g. "cc"), then stating the intended audience will help others understand why they are receiving the message. In this case, "Attention: Unit Supervisors" at the top of the message will help.

4. **Clearly state the importance or urgency of your message.**

   Put this information at the beginning of the message or use features built into e-mail systems such as MS Outlook.

5. **Put an "action requested" line at the top of the message.**

   For example:
   Action: Reply by 4:30 p.m., January 10, 2004

6. **Avoid jargon and acronyms.**

   This is particularly important when sending e-mail to an audience that may not be familiar with jargon and acronyms commonly used in your work group. If using acronyms in the message to keep the message short, spell out the full term the first time followed by the acronym in parentheses.

7. **Format messages for easy reading.**

   Keep the layout and structure of the e-mail simple and avoid complex formatting and graphics.

   Also, when people read electronically, they tend to scan more than when they read printed information. So, it's a good idea to keep your paragraphs short to facilitate scanning.

8. **Avoid "reply to all."**

   Be careful using "Reply-to-All" when responding to a message, particularly if the original message was sent to a large audience. "Reply-to-All" is only needed where the reply is important and relevant to the *majority* of recipients of the original message.

9. **Do not send large attachments. Post once and point.**

   Although your dedicated connection to the Internet may be quite fast, a recipient outside of your ministry may have a slow connection. Attachments should only be sent to people who have an active need for the majority of information in the attachments, and if the information is too much to include in the body of a message. If the information is only of possible interest, it is better to post the information to an area accessible to the appropriate audience, such as on an Internet site available to the public or on an Internet site where access is restricted to specific individuals (e.g. an extranet).

   Generally speaking, avoid sending a file that is over 1MB in size, unless you know that the recipient has a fast connection or, if it is very important and e-mail is the only way to get the information there quickly. If the file is very large, you could compress it before sending it, or deliver it in another way (e.g. on an Internet or Intranet site or on CD-ROM).

   Always review the hidden text in electronic documents before attaching them to e-mail messages to avoid conveying incorrect or inappropriate information. This is especially important if comments have been added or the change-tracking feature has been used to track revisions to document.

   If you use the change-tracking feature in Microsoft Word or other software, it is highly recommended that you also use the "Accept Changes" function before releasing your document to the public (e.g. e-mailing it to stakeholders or posting it to a web site). If you fail to "Accept Changes," Word keeps your earlier drafts, which might contain sensitive or incorrect information, within the document. Anyone can view this information by turning on the "Highlight Changes" feature in Word.

   You should also check the document properties to ensure that they reflect the correct title, author and other details about your document.

10. Use distribution lists sparingly.

Use the right distribution list for each message. When there are many lists it is easy to select the wrong one.

Before you use a list, check to see who is on it and verify its accuracy. When creating distribution lists, limit each list to those individuals who are likely to need the same type of information. This may be based on organization (such as all people in a unit), function (all managers and directors) or specific interest (a temporary work group for a project).

Keep the list up-to-date. People often change jobs and e-mail addresses. This is particularly important for people outside the ministry who you contact infrequently.

Also remember to keep your e-mail professional in both content and tone. Remember, it could subject to a FOIP request.

APPENDIX 3: SAMPLE MINISTRY GUIDELINES AND PRACTICES

This section contains an example of ministry guidelines and practices related to e-mail. Additional or alternative guidelines and practices could be added based on the business needs of the ministry.

Topic	Guidelines and Practices
Integrating e-mail records with other records management practices	The normal practice for managing e-mail records in the ministry will be to integrate them into existing folders on shared drives that parallel our traditional paper records management classification structure. At both the corporate and business level, folders will be established in the electronic shared drive file structure that parallel the ministry's records classification system for paper records and are linked to approved records retention and disposition schedules. The Senior Records Officer and IT services will provide advice on the "set up" of public folders and linkage to schedules. Drafts, duplicates and reference documents will not be filed in directories containing completed versions and official records. Until such folders are established, it is the policy of the ministry to print and file all e-mail (except transitory and personal). Each business unit must establish responsibility for managing messages stored in electronic form according to approved records management policies and records retention and disposition schedules. Only authorized staff will have authority to delete records from corporate and business level folders, using documented, auditable procedures.
Protecting the security of the system and messages	**Protection against viruses** Virus protection can occur at three levels: when the e-mail message first enters the government's e-mail system, when it reaches the ministry's network, and at the desktop level. Given the risk of viruses in today's environment, employees should • not open attachments that are from unknown senders or that have an ".exe ," ".vbs," or ".bat" extension; and • regularly update the virus protection on the desktop. This can be done by….[insert details]

Topic	Guidelines and Practices
	Back-up Procedures The ministry performs “back-up” procedures every night. Electronic files (including e-mails) that are created/received AND deleted the same day will not be backed up on the system, and thus are irretrievable through back-up procedures. **Password Protection** The use of the password is a shared responsibility of individual employees and IT administrators. You should: • Not share passwords with other employees. To do so exposes you to responsibility for actions that others may take using the password and your ID. • Change your password regularly (every three months) when prompted by the system. • Select a password for your screen saver (that way, if you are away from your desk, others cannot access confidential information in your files). Alternatively you can “lock” your computer if your operating system provides this feature (e.g. available in Windows 2000). **Message Protection and Authentication Controls** E-mail records are the property of the Government of Alberta. These records should NOT be left on machines where they may be accessible by others. Therefore, do not download your e-mail to any non-government machine (except your home computer). If you download e-mail at home, you MUST delete messages as you review them and ensure that no Government of Alberta messages remain on your home system. Access to the ministry’s e-mail from non-government machines should generally be avoided. Attachments may be left on machines in libraries, kiosks and other places without you realizing it. Remote access to e-mail from outside of the ministry should be done only with security protocols that allow for two-level authentication. Do NOT forward e-mail from the Government of Alberta account to a personal account such as hotmail.com. Apply the “confidential” flag on outgoing messages where appropriate to alert recipients about special privacy or security handling requirements.

Topic	Guidelines and Practices
	Encryption The ministry does not have a standard for encryption of messages. Before you attempt to encrypt messages, please consult IT services to ensure encrypted messages are accessible if required in the future.
Compliance with FOIP legislation	**Access** All records, including e-mail records, in the custody or under the control of the ministry may be subject to access by the public on request. If the ministry receives a request to access information, all employees may be asked to search their personal e-mail folders, in addition to public folders and shared drives, to comply with the request. It is unlawful to knowingly delete any message related to a request for access to information until the request has been satisfied and all periods of appeal have been exhausted. **Privacy** Personal information contained in e-mail must be protected. Under normal circumstances, sensitive personal information should not be sent though e-mail so that privacy of the information is protected. If you must send personal information through e-mail, you should • ensure that the personal information is contained in an attachment; • password protect the attachment; • notify the recipient of the password for the attachment using a different method of communication (e.g. telephone); and • request a confirmation of receipt from the recipient of the message.
Monitoring e-mail	The ministry will regularly monitor the e-mail system for potential threats to security and the functioning of the system. The normal practice of the ministry is not to monitor individual e-mail messages for unspecified purposes. However, we may investigate the content of individual e-mail messages • if we suspect a violation of any policy, law, the Official Oath of Office or the Code of Conduct and Ethics for the Public Service of Alberta agreed to by all employees. Potential violations might include safety violations, illegal activity, misuse of

Topic	Guidelines and Practices
	corporate resources, racial discrimination, and sexual harassment. • for the purpose of evaluating an employee's performance or activities. Employees will be consulted before any monitoring is done. • if it is necessary for another staff member to access an employee's work-related e-mail messages when the employee is working out of the office, on vacation, or is away due to illness. Employees will be asked for access to their e-mail prior to their absence from the office whenever possible.
Usage practices for e-mail	E-mail can make communication with colleagues and clients easier. Employees are encouraged to make use of this vehicle. However, too much of a good thing can create problems. To make sure the system continues to run smoothly, the following is suggested: • Use "reply to all" only if all recipients of the original message need to receive your reply. If not, reply only to the sender of the original message. • Use the ministry Intranet and shared drives, or the ministry's Internet or secure extranet site, as much as possible to "post messages" that others can view. This keeps the number of attachments to a minimum. • If sending attachments outside of the ministry, ensure that the receiver can receive and read the attachment, and check for any hidden text that may contain incorrect or sensitive information. For example, delete inappropriate comments and review the document properties to verify the title, author and other details. If the change-tracking feature in Microsoft Word or other software has been used, you must also use the "Accept Changes" function, otherwise the receiver will be able to view earlier drafts of your document by turning on the "Highlight Changes" feature in Word. • Do NOT respond to junk mail, spam or other types of unsolicited messages. This includes chain letters sent to you by someone you know. If you respond to these messages, the information can be used to generate more "junk" mail messages. The best advice is: "ignore them and delete them without reading them." • Do NOT send jokes or other non-work related programs as attachments as they use up considerable system resources.

Topic	Guidelines and Practices
Roles and responsibilities for managing e-mail	Individual managers in the ministry will be held accountable for the management of e-mail records by their employees. Managers must ensure that employees have training to be able to properly manage their e-mail records. Managers must also establish a regular review with employees to ensure that e-mail records as well as other records are being managed according to ministry guidelines and practices. The management of e-mail records, along with other records management responsibilities will form part of each manager's performance evaluation. All users of the ministry's e-mail system have the following responsibilities: • Users should remove personal and transitory records from personal mail boxes on a regular basis. • All other records (i.e. not personal or transitory) will be stored in the appropriate folder, format and media required by the ministry and organized in a way that makes them accessible to those authorized to know the contents. • The disposition of e-mail records must be done according to approved current records retention and disposition schedules.
Other	All electronic communication generated, stored or handled by the government servers/microcomputers (including back-ups) is the property of the Government of Alberta. Any personal messages (not about government business) should be routinely deleted from the systems.

APPENDIX 4: GLOSSARY

Authentication Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).

Bulletin Board System (BBS) Before the Web took over the world, computer hobbyists and companies often communicated with other techies via electronic bulletin board systems, or BBSs.

The Web has largely replaced BBSs for most purposes, though some individuals and companies still maintain their systems or even connect them directly to the Web.

E-Mail Electronic Mail — are messages sent from one person to another via computer. They are usually text, but can include attached files, HTML codes, voicemail messages, etc.

E-mail can also be sent automatically to a large number of addresses (see also Mailing List).

E-Mail Scams There are a wide variety of scams being perpetrated on the Internet using email.

One type is the false virus warning or hoax. These often take the form of a warning not to open an e-mail with a certain subject line, and asking you to pass on the warning. These are almost always scams and are designed to waste resources by resulting in millions of copies of the warning using bandwidth and filling up e-mail storage. Most antivirus web sites have pages listing hoaxes (for example: http://securityresponse.symantec.com/avcenter/hoax.html). People should always make sure an e-mail warning is not a hoax before forwarding it.

Another common scam is the “get rich quick” scam or requests for donations of money.

Encryption Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key.

HTML HyperText Markup Language — The language used to create Hypertext documents for use on the World Wide Web. HTML files are meant to be viewed using a World Wide Web Client Program or browser. HTML is also an alternative for sending formatted text messages in some e-mail systems.

Listserv™ The most common kind of Internet mailing list. Listserv® is a registered trademark of L-Soft International, Inc.

Mailing List A system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the mailing list. In this way, people who have many different kinds of e-mail access can participate in discussions together.

Newsgroup A worldwide system of discussion groups, with comments passed among thousands of machines.

The system, also called USENET, is decentralized, with over 10,000 discussion areas, called newsgroups.

Official Record An official record is a record that has some future administrative, financial, legal, research or historical value to the government and is therefore retained and filed in a recordkeeping system.

Personal Information Personal information is defined in section 1(n) of the FOIP Act as recorded information about an identifiable individual, including but not limited to:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information, or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

Record Record is defined in section 1(q) of the FOIP Act as "a record of information in any form, and includes notes, images, and audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records."

Recordkeeping Manual or computerized information system which captures, manages and provides access to records over time.

Records Retention and Disposition Schedule Legal documents that describe different series of government records, establish how long they must be retained and what their final disposition will be, either destruction or archival preservation.

Transitory Record A transitory record is a record containing information of temporary value which does not have future administrative, financial, legal, research, or historical value to the government. This may include duplicate records, draft documents, working materials, external publications, blank forms, and temporary notes provided that they do not have long-term value.

Trojan Horse In computers, a Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming in such a way that it can get control and do its chosen form of damage, such as allowing someone else to access your computer over the Internet. See also Virus.

Virus A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Most viruses can also replicate themselves and are distributed by disks or over networks and the Internet. All computer viruses are manmade. Even a simple virus is dangerous because it can use up resources and even damage or delete all information on your system. See also Trojan Horse.

APPENDIX 5: Resources

Looking for more information related to the management of e-mail? The sources listed below can help.

Note: Several documents listed in this appendix are available on the Shared Repository (SHARP) (http://www.sharp.gov.ab.ca). This site is accessible to Government of Alberta employees (name@gov.ab.ca) and also to extended stakeholders (i.e. agencies, boards and commissions), consultants contracting with the Government of Alberta and employees of other governments who are registered users of the SHARP web site.

E-mail and Information Management

Office of the Corporate Chief Information Officer, and Alberta Government Services, Information Management Branch.
Government of Alberta Information Management Framework.
http://www.im.gov.ab.ca

E-mail and IT Security

Office of the Corporate Chief Information Officer.
Using E-mail: Detailed Risks and Controls.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=4442

Office of the Corporate Chief Information Officer.
Using E-mail: Managing the Risks.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=4441

Office of the Corporate Chief Information Officer.
Government of Alberta Information Technology Security Policy.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=3078

E-mail and Public Access

Alberta Government Services, Access and Privacy Branch.
FOIP Bulletin Number 12: "E-Mail: Access and Privacy Considerations."
http://www.gov.ab.ca/foip/guidelines_practices/bulletins/bulletin12.cfm

E-mail Use

Office of the Corporate Chief Information Officer.
Government of Alberta Internet and E-mail Use Policy
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=2007

Commonwealth Films. **The Plugged-in Mailbox: E-mail Uses and Misuses.** (Video and Guide). http://www.commonwealthfilms.com/s/1_10_39.asp

Employee Code of Conduct

Alberta Personnel Administration Office.
Code of Conduct and Ethics for the Public Service of Alberta.
http://www.pao.gov.ab.ca/legreg/code

Legislation – available on the Queen's Printer at http://www.qp.gov.ab.ca

- *Alberta Evidence Act*
- *Electronic Transactions Act*
- *Freedom of Information and Protection of Privacy Act*
- *Health Information Act*
- *Historical Resources Act*
- *Government Emergency Planning Regulation*
- *Records Management Regulation*

Managing E-mail

National Archives of Canada.
E-mail Management in the Government of Canada.
http://www.collectionscanada.ca/information-management/060404_e.html

ARMA International (Association for Information Management Professionals) Lenexa, Kansas

- **E-Mail Rules**: **A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communications.** Nancy Flynn and Randolf Kahn, 2003 ISBN: 0-8144-8188-9. http://www.arma.org/bookstore/productdetail.cfm?ProductID=1383
- **Guideline for Managing E-mail**, ARMA International, 2000. ISBN: 0-933-887-91-4. http://www.arma.org/bookstore/productdetail.cfm?ProductID=1045
- **Legal Obstacles to E-Mail Message Destruction**, ARMA International Educational Foundation, 2003. http://www.armaedfoundation.org/images/LegalObstaclesToEmailDestructionV634.pdf.
- **Managing Your E-Mail Thinking Outside the Inbox** by Christina Cavanagh 2003 ISBN: 0-471-45738-8. http://risk-management.argospress.com/book-0471457388.htm
- **E-mail, Voicemail and Instant Messaging: A Legal Perspective.** (IMJ Read & Learn Course) http://www.arma.org/learningcenter/onlinecourses/courselising.cfm?CourseID-20

- **Requirements for Managing Electronic Messages as Records (ANSI/ARMA 9-2004)** ARMA International ISBN 1-931786-22-4. http://www.arma.org/bookstore/productdetail.cfm?ProductID=1499

- Natural Resources Canada. **Guidelines on Managing Electronic Mail Messages**, 2004. http://www.nrcan.gc.ca/em-ce/email-e.htm

Protecting Personal Information and Privacy

Office of the Corporate Chief Information Officer.
Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile.
https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=3546

Alberta Government Services, Access and Privacy Branch.

- **FOIP Guidelines and Practices.**
  http://www.gov.ab.ca/foip/guidelines_practices
- **FOIP Bulletin Number 12: "E-Mail: Access and Privacy Considerations."**
  http://www.gov.ab.ca/foip/guidelines_practices/bulletins/bulletin12.cfm

Records Management

Alberta Government Services, Information Management Branch.

- **Official and Transitory Records: A Guide for Government of Alberta Employees**.
  http://www.im.gov.ab.ca/publications/pdf/OfficialTransitoryRecordsGuide.pdf

Web Sites

The following web sites offer guidelines, forms, books, newsletters, training tools, workshops, discussion forums, software and other resources relating to the development, implementation and enforcement of e-mail policies.

- **Treasury Board of Canada Secretariat Information Management Resource Center: E-mail Management.**
  http://www.cio-dpi.gc.ca/im-gi/references/email-courrier/email-courrier_e.asp

- **Email-Policy.com**

  http://www.email-policy.com

- **ePolicy Institute**

  http://www.epolicyinstitute.com

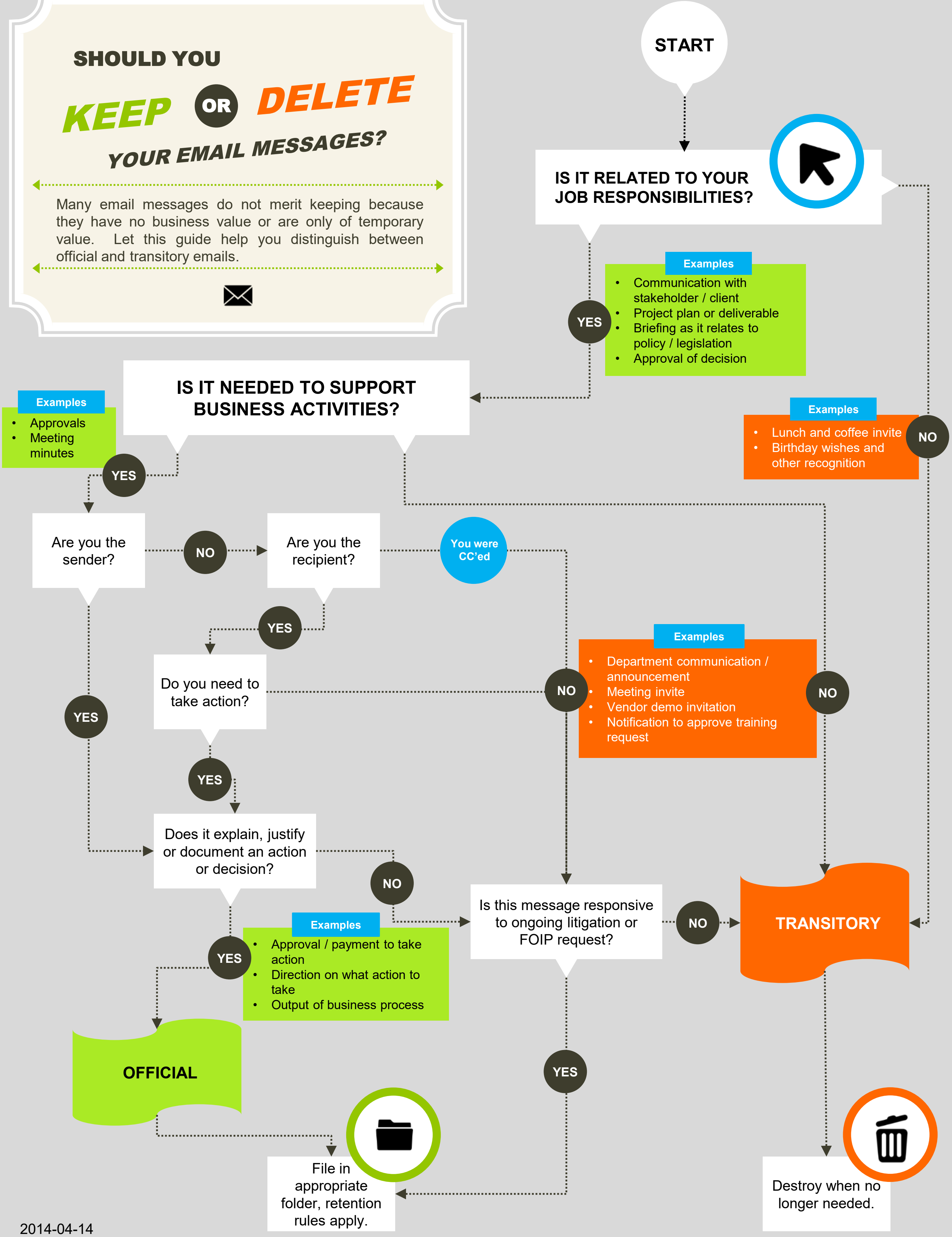
Appendix F

Email Decision Diagram

Dated April 14, 2014

SHOULD YOU *KEEP* OR *DELETE* YOUR EMAIL MESSAGES?

Many email messages do not merit keeping because they have no business value or are only of temporary value. Let this guide help you distinguish between official and transitory emails.



START

IS IT RELATED TO YOUR JOB RESPONSIBILITIES?

YES

Examples
- Communication with stakeholder / client
- Project plan or deliverable
- Briefing as it relates to policy / legislation
- Approval of decision

NO

Examples
- Lunch and coffee invite
- Birthday wishes and other recognition

IS IT NEEDED TO SUPPORT BUSINESS ACTIVITIES?

Examples
- Approvals
- Meeting minutes

YES

Are you the sender?

NO

Are you the recipient?

You were CC'ed

YES

Do you need to take action?

NO

Examples
- Department communication / announcement
- Meeting invite
- Vendor demo invitation
- Notification to approve training request

NO

YES

YES

Does it explain, justify or document an action or decision?

NO

YES

Examples
- Approval / payment to take action
- Direction on what action to take
- Output of business process

OFFICIAL

Is this message responsive to ongoing litigation or FOIP request?

NO

TRANSITORY

YES

File in appropriate folder, retention rules apply.

Destroy when no longer needed.

2014-04-14

Appendix G

“Electronic Records Reduction” – Email from Doris Burandt to TRANS-ORG ALL

Dated June 29, 2017

From:	Doris Burandt <Doris.Burandt@gov.ab.ca> on behalf of Barry Day <Barry.Day@gov.ab.ca>
Sent:	June 29, 2017 11:08 AM
To:	_TRANS-ORG ALL
Subject:	Electronic Records Reduction

The Records and Information Management (RIM) team is launching Phase 1 of the Electronic Records Improvement Project. This phase will target My Documents and Outlook transitory records. By reducing transitory records in these areas, we can save both time and money for our department - but we need you to help us succeed.

Our goal is to reduce 25% of the My Documents and Outlook accounts storage by December 1st.

To achieve this, we're asking you to participate in a short, one-hour training session to learn how you can reduce your digital footprint. Training will be available in classroom or online via Live View.

You'll be offered tips and tricks to help you, as well as ongoing support from the RIM team. The top 25 individuals who reduce their storage by the greatest percentage will be entered into a draw for one of three $50 Apple gift cards.

Please take a few moments to register for the short training, which can be found by searching under 'TRAINING' for Electronic Records Reduction – The Fundamentals. You can also read through the brochure or visit the Electronic Records Reduction site and learn how easy it is to reduce your digital footprint.

Thank you for your support and cooperation.

Barry