Information Handling When Decommissioning Systems and Applications

FOIP and Information Management, Enterprise Information Management

Version: 1.0

Approved by: Maureen Towle, Executive Director, Enterprise Information Management	**Owner:** Enterprise Information Management
Approval date: June 1, 2019	**Review date:** June 1, 2021
Contact: SA.InformationManagement@gov.ab.ca	**Policy Instrument type:** Procedure

Contents

Procedure Statement

This procedure is to be used by individuals decommissioning Government of Alberta (GoA) systems and applications to ensure that information management (IM) obligations (e.g., the proper application of records retention and disposition schedules) are met.

Authority

- *Government Organization Act*
- Records Management Regulation

Scope

This standard applies to all departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards and commissions as defined in schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

Agencies, boards and commissions that are not contained within schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this standard.

Departments requiring an exception must follow the Chief Information Security Officer exception process. Please contact your Sector Information Security Officer (SISO) to discuss the exceptions process; if your department is not part of a sector, please contact Service Alberta, Enterprise Information Management.

Procedure Description

This procedure:

- provides a high-level overview of scenarios that would require the migration of GoA data and information; and
- outlines an overview of the steps involved in each scenario.

NOTE: For the purpose of this guidance, the term “data and information” also encompasses records in the custody and/or under the control of the GoA, regardless of location or format. “Data and information” and “records” may be used interchangeably within this guide.

Procedure Specification

The scenarios presented in this procedure represent a sampling of possible situations that may occur when decommissioning systems and applications, but are not exhaustive. For decommissioning issues not covered by the presented scenarios, or for further guidance on the decommissioning of systems and applications, please contact the appropriate IM professional (e.g., a department’s senior records officer) or Enterprise Information Management.

For support with the disposition of electronic records, please contact the appropriate IM professional and/or Transfers, Storage and Disposition.

When the decommissioning of a system or application involves the full or partial migration of data and information, there may be questions regarding the specific handling of User Acceptance Testing (UAT)/Development Environments, Backups and Batch Transfer Files. For guidance regarding the specific handling of UAT/Development Environments, Backups, and Batch Transfer Files, please refer to **Other Considerations**.

IMPORTANT: Any systems, applications or data and information that are, or are reasonably anticipated to be, subject to litigation holds or access requests under the *Freedom of Information and Protection of Privacy Act* must not be altered, migrated or disposed of until all relevant holds have been lifted.

Cases may exist where it is possible to derive secondary use from anonymized data and information. Determinations regarding potential secondary use must be completed prior to decommissioning. For support with secondary use cases, please contact the Open Government team.

Scenario One: Migration of all Data and Information

- Refer to the Digital Records Conversion/Migration Standard.
- IMT staff must complete an inventory of the data and information that will be migrated to the new system or application; if an inventory has already been completed, its accuracy must be verified. At a minimum, the inventory must include:
    - type of data and information;
    - date ranges; and
    - records retention and disposition schedule information.
- IMT staff must verify the accuracy of the data and information migrated to the new system or application against the data and information in the old system or application (guidance on this process is available in the Digital Records Conversion/Migration Standard).
- After the verification has been completed, IMT staff must obtain business area sign off that the migration has been completed successfully.
- IMT staff must apply records retention and disposition schedule Backup Systems – 2003/043-A001, item 2: Data Recovery and Migration Files to the data and information in the old system or application. IMT staff must:
    - contact the appropriate IM professional for assistance;
    - submit the inventory, along with the summarized Records Inventory Form (TDS2549), to Transfers, Storage and Disposition for importation into the Inactive Records Information System (IRIS);
    - retain the data and information in the old system or application for 30 days after verification has been completed—access to the old system or application can be restricted during this time; and
    - ensure that data and information with the final disposition of archive (i.e., a record of enduring value as identified by an approved records retention and disposition schedule that must be transferred to the Provincial Archives of Alberta for permanent retention) is handled in accordance with established policy instruments and procedures.
        - For support with the disposition of electronic records, please contact the appropriate IM professional and/or Transfers, Storage and Disposition.
- After the 30-day waiting period required by records retention and disposition schedule Backup Systems – 2003/043-A001 has elapsed, IMT staff are able to securely destroy the data and information in the system or application being decommissioned
    - IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed.
    - Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.

- IMT staff will inform the IM professional once the system or application has been decommissioned—this can be done in the form of an annual report on decommissioned systems and applications.

Scenario Two: Partial Migration of Data and Information

NOTE: This guidance applies only if **ALL** data and information remaining in the system or application have met their retention period. If a system or application contains data and information that is not being migrated and has not yet met its retention, the system or application must remain operational.

- Refer to the Digital Records Conversion/Migration Standard.
- IMT staff must complete an inventory of the data and information that will be migrated to the new system or application; if an inventory has already been completed, its accuracy must be verified. At a minimum, the inventory must include:
    - type of data and information;
    - date ranges; and
    - records retention and disposition schedule information.
- IMT staff must verify the accuracy of the data and information migrated to the new system or application against the data and information in the old system or application (guidance on this process is available in the Digital Records Conversion/Migration Standard).
- After the verification has been completed, IMT staff must obtain business area sign off that the migration has been completed successfully.
- In cases where only a portion of the data and information in a system or application have been migrated to a new system or application, an analysis of the data and information retained in the old system or application must be completed by IMT staff; at a minimum, this analysis must answer the following:
    - who owned the old system or application?
    - what was the function of the system or application?
    - when was the system or application last used?
    - what data and information are contained in the system or application?
- IMT staff will send the analysis of the old system or application to the appropriate IM professional.
- The IM professional will select the applicable records retention and disposition schedule for the data and information not included in the migration (in the old system or application).
- IMT staff must apply the records retention and disposition schedule selected by the IM professional to the inventory. IMT staff must:
    - submit the inventory, along with the summarized Records Inventory Form (TDS2549), to Transfers, Storage and Disposition;
    - retain the data and information in the old system or application for 30 days after verification has been completed—access to the old system or application can be restricted during this time; and
    - ensure that data and information with the final disposition of archive (i.e., a record of enduring value as identified by an approved records retention and disposition schedule that must be transferred to the Provincial Archives of Alberta for permanent retention) is handled in accordance with established policy instruments and procedures.

        - For support with the disposition of electronic records, please contact the appropriate IM professional and/or Transfers, Storage and Disposition.
- After the 30-day waiting period required by records retention and disposition schedule Backup Systems – 2003/043-A001 has elapsed, IMT staff are able to securely destroy the data and information in the system or application being decommissioned
    - IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed.
    - Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.
- IMT staff will inform the IM professional once the system has been decommissioned—this can be done in the form of an annual report on decommissioned systems and applications.

Scenario Three: No Migration of Data and Information

- There may be cases where a system or application becomes obsolete (e.g., too expensive to maintain, incompatible with newer systems, no longer supported by vendor, etc.) and the data and information contained within the system or application are not migrated.
- IMT staff must complete an inventory of the data and information that will not be migrated to the new system or application; if an inventory has already been completed, its accuracy must be verified. At a minimum, the inventory must include:
    - type of data and information;
    - date ranges; and
    - records retention and disposition schedule information.
- Data and information in an obsolete system or application that are not migrated and have met their retention need to be destroyed under the appropriate records retention and disposition schedule.
- The IM professional will determine which records retention and disposition schedule must be applied to the data and information in the obsolete system or application and:
    - submit the detailed inventory along with the summarized Records Inventory Form (TDS2549) to Transfers, Storage and Disposition; and
    - IMT staff and the IM professional will work together to determine the appropriate approach to the destruction of the data and information.
    - IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed—Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.
- Data and information in an obsolete system or application that are not migrated and have a final disposition of archive must be handled appropriately.
    - For support with the disposition of electronic records, please contact the appropriate IM professional and/or Transfers, Storage and Disposition.
- A Statement of Acceptable Risk (SOAR) must be completed and signed off by the appropriate information controller in instances where data and information have not met retention.
    - Information controllers should consult with Enterprise Information Management during this process.

Scenario Four: Inaccessible Data and Information

- There may be cases where the system or application to be decommissioned cannot be accessed to identify or migrate its contents.

- In cases where a system or application cannot be accessed, an analysis of the data and information retained in the old system or application must be completed by IMT staff; at a minimum, this analysis must answer, to the best of their abilities, the following:
    - who owned the old system or application?
    - what was the function of the system or application?
    - when was the system or application last used?
    - what data and information are contained in the system or application?
- IMT staff will send the analysis of the old system or application to the appropriate IM professional.
- A Statement of Acceptable Risk (SOAR) must be completed and signed off by the appropriate information controller in instances where data and information have not met retention.
    - Information controllers should consult with Enterprise Information Management during this process.
- The IM professional will submit a request to the Alberta Records Management Committee (ARMC) to use records retention and disposition schedule Unsalvageable Damaged Records – 2011/002-A002.
    - This records retention and disposition schedule is used because there is a possibility that the data and information could be recovered by using extensive, and often expensive, forensic tools. In such instances, the business area must consider the value of the data and information against the cost of potentially recovering them.
- Once the ARMC has allowed the use of the records retention and disposition schedule, the IM professional will submit a detailed inventory based on their analysis along with the summarized Records Inventory Form (TDS2549) to the Transfers, Storage and Disposition team for importation into IRIS.
- IMT staff and the IM professional will work together to determine the appropriate approach to the destruction of the data and information.
    - IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed—Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.
- IMT staff will complete the decommissioning process.

Other Considerations

When the decommissioning of a system or application involves the full or partial migration of data and information (i.e., Scenarios One and Two), there may be questions regarding the proper management of UAT/Development Environments, Backups and Batch Transfer Files. This section provides an overview of how to manage data and information contained in UAT/Development Environments, Backups and Batch Transfer Files.

Data and Information Contained in User Acceptance Testing (UAT) and Development Environments

- Data and information created in testing and/or development environments must be disposed of under the records retention and disposition schedule Administrative Records Disposition Authority (ARDA) – 1986/050-A017. Item 0830.01 states:
    - Computer Test Runs
        - Output generated as a result of a verification of computer programming, processing, or evaluation of hardware; output that cannot be certified as a production item by the user of the computer system. Excludes runs,

current systems development/modification or representative test information.
    - IMT staff must contact the Transfer, Storage and Disposition team for additional assistance. IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed—Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.
- IMT staff will complete the decommissioning process.

Backups

- Data and information in backups fall under records retention and disposition schedule Backup Systems – 2003/043-A001, item 1: Routine Backups.
    - The data and information can be destroyed or overwritten as soon as they are no longer required.
    - The records retention and disposition schedule allows IMT staff to destroy the data and information as part of a normal backup process, without requiring a waiting period. IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed—Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.

Batch Transfer Files

- "Batch Transfer Files" refers to the residual files that may be created when IMT staff use tools in the delivery of their support services. These residual data recovery and migration files are typically only accessible by IMT staff, and cannot be seen or accessed by users.
- Most batch transfer files contain data and information that are added to a system or application and then verified. Decommissioning batch transfer files is similar to the migration of information outlined in Scenario One:
    - IMT staff must apply records retention and disposition schedule Backup Systems – 2003/043-A001, item 2: Data Recovery and Migration Files to the data and information in the old system or application. To properly apply the records retention and disposition schedule, IMT staff must:
        - contact the Transfer, Storage and Disposition team for assistance; and
        - retain the data and information in the old system or application for 30 days after verification has been completed—access to the old system or application can be restricted during this time.
    - After the 30-day waiting period required by records retention and disposition schedule Backup Systems – 2003/043-A001 has elapsed, IMT staff are able to securely destroy the data and information in the system or application being decommissioned
        - IMT staff must inform Transfers, Storage and Disposition that the data and information has been securely destroyed.
        - Transfers, Storage and Disposition will add documentation of the destruction to their electronic file for preservation.
- There is no requirement to inform the IM professional about batch transfer files, unless they have been found abandoned.

Definitions

Migration:

The process of moving records, including their existing characteristics, from one hardware or software configuration to another without changing the format.
(Source: ISO 13008: 2012 (E) – Digital records conversion and migration process)

Record:

(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.
(Source: *Freedom of Information and Protection of Privacy (FOIP) Act*)

Note: Once recorded in a system or application, data falls under the *FOIP Act* definition of a record, and must be managed accordingly. As per the definition of record in the *FOIP Act*, hardware and software are not considered records; however, they are considered government assets, and must be disposed of in accordance with legislated requirements and best practices.

Records Retention and Disposition Schedule:

A records retention and disposition schedule is a legal authority that describes the records under the control of a government organization, specifies how long and where they must be kept as they progress through the phases of their life cycle, the format in which the records must be stored and what their final disposition will be (destruction or archival preservation) at the end of their life cycle.
(Source: Developing Records Retention and Disposition Schedules)

Compliance

Consequences of non-compliance with this standard could result in the loss of information, damage to Government of Alberta's reputation, exposure of Albertans to harm and/or incurrence of unnecessary costs.

- Depending on the severity of non-compliance, either informal or formal requests and/or follow-ups may be made by Enterprise Information Management, Corporate Internal Audit Services, Corporate Information Security Office, Office of the Information Privacy Commissioner, and/or Public Service Commission.
- Legislated disciplinary action (i.e., *Public Service Act*) may be taken depending on the severity of non-compliance.

References and Supporting Resources

- Digital Records Conversion/Migration Standard
- Records Inventory Form TDS2549
- Records Retention and Disposition Schedules
  - Administrative Records Disposition Authority (ARDA) – 1986/050-A017
  - Backup Systems – 2003/043-A001
  - Unsalvageable Damaged Records – 2011/002-A002
- Statement of Acceptable Risk (SOAR)