Information Management Guideline – Managing Data and Information when Decommissioning Business Applications

Guideline No. CIMS-G012
Version No. 1.0
Approval Date: December 23, 2021

City Clerk's Office

An Information Management Guideline

Subject: Decommissioning

Guideline No.: CIMS-G012

Version No.: 1.0

Issued On: December 23, 2021

Issued By: City Clerk's Office

Keywords: Application, Data, Decommissioning, Information, Management, Records, System

Issued By: Corporate Information Management Services, City Clerk's Office

Contact Information:
Kristie Pratt
Deputy City Clerk
Corporate Information Management Services
City Clerk's Office
City Hall, 13th floor, West Tower
100 Queen Street West
Toronto ON M5H 2N2
Tel: (416) 392-9683

Approval: This Guideline has been approved by:

Version #	Name	Title	Approval Date
1.0	Kristie Pratt	Deputy City Clerk	December 23, 2021

Foreword

City of Toronto Information Management Policies and Standards are the official publication on the policies, standards, directives, guidelines, position papers and preferred practices given oversight under delegated authority of Toronto Municipal Code, Chapter 217, Records, Corporate (City). These publications support the City's responsibilities for coordinating standardization of Information Management in the City of Toronto.

Acknowledgements

This Guideline acknowledges the efforts, subject matter expertise, and oversight provided by the following:

Project Sponsor: **Kristie Pratt** Deputy City Clerk, Corporate Information Management Services, City Clerk's Office

Divisions and Business Units

- Business & Technology Planning, City Clerk's Office
- Corporate Information Management Services, City Clerk's Office
- Technology Services Division

Table of Contents

Foreword *3*
Acknowledgements *4*
1. INTRODUCTION **6**
2. PURPOSE **6**
3. WHEN TO DECOMMISSION **6**
3.1 PROJECT-BASED DECOMMISSIONING 7
3.2 APPLICATION RATIONALIZATION PROJECTS 7
3.3 INFRASTRUCTURE RATIONALIZATION PROJECTS 7
4. LEGACY APPLICATION INFORMATION MANAGEMENT PRE-PLANNING AND ASSESSMENT **8**
5. DATA AND INFORMATION MANAGEMENT SCENARIOS **8**
5.1 MIGRATION OF ALL DATA AND INFORMATION 9
5.1.1. Quality Assurance Validation *9*
5.1.2. Data and Information in Batch Transfer Files *10*
5.1.3. Disposal of Data and Information in Legacy Application(s) *10*
5.2 PARTIAL MIGRATION OF DATA AND INFORMATION 10
5.3 NO MIGRATION OF DATA AND INFORMATION 11
5.4 DIFFICULT TO ACCESS AND/OR INACCESSIBLE LEGACY APPLICATIONS 12
5.5 DATA AND INFORMATION IN TESTING AND DEVELOPMENT ENVIRONMENTS 13
5.6 DATA AND INFORMATION ON BACKUP MEDIA 13
Appendix A: Definitions 14
Appendix B: Decommissioning Planning Checklist 16
Appendix C: Decommissioning Assessment and File Inventory Tool Template 19

1. Introduction

Divisions across the City manage a variety of business applications to provide service delivery. Many of these applications contain documented decisions and other records or data that act as evidence of business transactions and activities. Over time, these applications can become dated, no longer providing key functionality or continued value, and need to be decommissioned.

Decommissioning is a process by which a business application is shut down and removed from use. Applications should be decommissioned when either the application is replaced by a new application covering the same or improved functionality or the application becomes obsolete and no longer supports the business process. An enterprise-wide application rationalization may also lead to an application being selected for decommissioning.

A critical part of the decommissioning process is determining what to do with key business data and information contained within the application. This requires an assessment to confirm what must be retained, migrated, or disposed of, in accordance with City bylaws and policies for managing information responsibly throughout its lifecycle.

City Divisions working with Corporate Information Management Services (CIMS), Technology Services Division (TSD), and/or their Divisional IT can demonstrate compliance with the requirements of this guideline by:

- Assessing and implementing, where required, data and information management requirements in new application acquisition, maintenance, and decommissioning, including conversion and migration of the data and information; and

- Taking into account retention and disposal requirements for data and information contained in an application which is to be decommissioned.

2. Purpose

The purpose of this Guideline is to provide a framework, advice, and an overview of the information management responsibilities of City Divisions when decommissioning technology applications.

3. When to Decommission

The primary factors to consider when decommissioning an application include technology obsolescence, security risks, non-compliance with legislative or legal requirements, a lack of key functionality, or licensing costs. Additional factors include:

- transition to new generation applications;
- project completion or termination;
- structural reorganization;
- transfer of functions due to regulatory and organizational changes;
- Application is no longer supported by vendor;
- Application is too expensive to maintain; and
- Application is incompatible with newer applications and unable to integrate.

The following are common scenarios in which decommissioning projects will occur:

3.1 Project-Based Decommissioning

From an information management perspective, the ideal scenario for decommissioning is that it is considered and planned for in the standard project methodology when developing or acquiring a new application. That way, the necessary assessment and business engagement to include information management requirements will occur.

Projects that implement a new application may be consolidating and rationalizing multiple legacy applications with diverse business owners or simply be acquiring a one-for-one application replacement. In both cases, the previous application can be decommissioned as part of the project.

Note: Project-based decommissioning may have one "go-live" date or may be staggered, as Divisions are on-boarded in stages, affecting when the legacy application(s) involved can be decommissioned.

3.2 Application Rationalization Projects

City Divisions, in conjunction with TSD, may decide to undertake comprehensive surveys to determine which of their applications no longer support core business processes due to the implementation of new applications or any of the other drivers mentioned above.

Assessing the City's application portfolio in aggregate allows the scale of challenges and opportunities to be clearly understood and enables a strategic approach to application lifecycle management.

3.3 Infrastructure Rationalization Projects

City Divisions, in conjunction with TSD, may decide to undertake a comprehensive infrastructure usage assessment as part of their data governance efforts. This process can help to assess the costs and risks associated with retaining data and information in business applications beyond their retention periods and/or maintaining an outdated application versus upgrading to a newer, more efficient one. In particular, certain types of applications may require infrastructure which is expensive and onerous to maintain.

Understanding the infrastructure costs associated with a Division's portfolio of applications, and the value and retention periods of the information housed within, will provide the division the ability to immediately identify cost savings. For example, the over-allocation of high-performance storage for low priority data or the excessive time periods for retention of business data and information may be identified and can be corrected through the decommissioning process.

4. Legacy Application Information Management Pre-planning and Assessment

Decommissioning planning can be complex and Divisions will need to determine what, if any, application linkages and dependencies exist and what information management requirements exist. Information management considerations include:

- Are the data and information in this application duplicated across multiple applications or data repositories? Does it exist in shared drives, websites, or elsewhere? Does the application house business records or transitory records? Determining which data and information are records versus copies (transitory) and where they reside upfront can make the decommissioning process more efficient.

- Is the application a relational database that contains rows, columns, and tables that pull data when queried to create a record? Are these combined data being saved as records, especially if business decisions are being made based on this information?

- Is it integrated with other applications? Are there other application dependencies? If so these need to be explored further to determine impacts to business processes/workflows and information shared between applications before proceeding to decommission.

  See Appendix B for these and other considerations in the Decommissioning Planning Checklist.

5. Data and Information Management Scenarios

Legacy business applications may contain data and information that are considered City records and must be managed accordingly. In consultation with CIMS, Divisions will need to determine what to do with the information in the application being decommissioned. There are a number of factors to consider such as conversion, migration, retention, and disposition. Some information may also need to be retained for long term preservation purposes should it have an extended retention period and/or archival value.

Each scenario below outlines requirements to be met around information management governance including the protection of personal information and record lifecycle management. Risk assessments must also be made to factor in the costs, time, and efforts when deciding to go with a particular scenario. Should decommissioning of a legacy application be taking place within the context of a project, these efforts must be accounted for in the project schedule and resources.

The scenarios presented below represent a sampling of possible situations that may occur when decommissioning applications but are by no means complete. For decommissioning issues not covered by these scenarios, and for other guidance, please contact CIMS at infomgmt@toronto.ca.

5.1 Migration of all Data and Information

Divisional staff, with assistance from CIMS and the system owner/custodian (whether Divisional IT or TSD), should complete an assessment and file inventory of the data and information that will be migrated to the new application (see Appendix C for a template). This includes a metadata mapping and other details such as:

- format of data and information;
- date ranges; and
- retention and disposition schedule information.

Before migration occurs, data cleansing activities may need to take place to ensure the data and information can be located and understood in the new application. Records that are past their retention period should be archived (if applicable) or deleted and any transitory records should be deleted. See Transitory Records Fact Sheet for more information.

Additionally, where personal or sensitive information is being migrated, appropriate precautions (e.g. secure storage mediums, appropriate permissions, encrypted data, etc.) should be put into place to ensure this information is safeguarded throughout the entire migration process.

5.1.1. Quality Assurance Validation

Divisions, TSD, Divisional IT and/or vendors (where applicable) must verify the accuracy of the data and information migrated to the new application against the data and information in the legacy application. A quality assurance and validation plan must be created that defines:

- Roles and Responsibilities
- A Quality Assurance Operator to perform testing
- Error (i.e. defining what constitutes an error)
- Testing size / percentage
- Accuracy threshold
- Testing process / plan
- Error or corruption process if errors are found

- Technical Tools that will be used in the process
- Reporting mechanisms and processes

After the verification is complete, staff should obtain business area sign off that the migration has been completed successfully.

5.1.2. Data and Information in Batch Transfer Files

Batch transfer files refer to the residual files that may be created when TSD or Divisional IT use tools in the delivery of their support services. These residual data recovery and migration files are typically only accessible by TSD staff, and cannot be seen or accessed by users.

- Most batch transfer files contain data and information that are added to an application and then verified.
- Once verified and quality assurance activities for migration are complete, these files can be considered transitory and disposed of by TSD or Divisional IT.

5.1.3. Disposal of Data and Information in Legacy Application(s)

Once quality assurance and validation activities are complete following migration to the new application, and sign off that the migration was successful has been obtained, the data and information in the legacy application can be considered transitory and disposed of according to City of Toronto, Toronto Municipal Code Chapter 217, Records, Corporate (City) s. 217-4 Retention and Disposition.

Divisions should work with CIMS, TSD, and/or their Divisional IT to determine how data and information can be disposed of.

This disposition process should be documented and retained by the Division.

5.2 Partial Migration of Data and Information

For data and information that will be migrated, Divisions must follow all of the requirements listed under section 5.1. Migration of all Data and Information.

For data and information that will be retained in the legacy application, the assessment completed for the partial migration will be sent by the Division to the appropriate CIMS staff who will advise which retention and disposition schedules can be applied to the data and information not included in the migration.

Retention and disposition schedule(s) can be applied in the following manner:

For data and information that must be retained because retention is not yet expired:

- Determine how long the application must remain operational to accommodate the retention schedule.
- If the application cannot remain fully operational, determine if it can be maintained in offline or in a lower-capacity form e.g. Read-Only.
- If maintaining the application in any form is not feasible, determine alternative storage locations e.g. server, external hard drive, or shared drive, until the retention period has expired.

For data and information that can be disposed of:

- Work with TSD or your Divisional IT to apply deletion of data and information in the application;
- Capture and document the date and time this occurred (audit log) and attach it to the assessment; and
- Store the assessment with other Divisional records regarding disposition management.

Each Division is responsible for documenting their own migration and retention and disposition activities outlined in these steps. Divisions should inform CIMS staff once the application has been decommissioned.

Note: For systems that are shared by multiple Divisions, decommissioning may have to take place in multiple phases. Some Divisions may remain in production mode while others will have completed their decommissioning activities and are no longer active in the system. A coordinated approach should be taken including the development of a schedule to determine migration/decommissioning activities and responsibilities.

5.3 No Migration of Data and Information

For data and information that will not be migrated, staff must complete an assessment and file inventory (see Appendix C).

Divisional staff will send the assessment and file inventory to the appropriate CIMS staff who will advise which retention and disposition schedules can be applied to the data and information in the application. The schedule(s) can be applied in the following manner:

For data and information that must be retained because retention is not yet expired:

- Determine how long the application must remain operational to accommodate the retention schedule.
- If the application cannot remain fully operational, determine if it can be maintained in offline or in a lower-capacity form e.g. Read-Only.
- If maintaining the application in any form is not feasible, determine alternative storage locations e.g. server, external hard drive, or shared drive, until the retention period has expired.

For data and information that can be disposed of:

- Work with TSD to apply deletion of data and information in the application.
- Capture and document the date and time this occurred (audit log) and attach it to the assessment.
- Store the assessment with other divisional records related to disposition management.
- Inform CIMS staff once the application has been decommissioned. This can be done in the form of an annual report on decommissioned applications.

5.4 Difficult to Access and/or Inaccessible Legacy Applications

There may be instances where an application is so old the information cannot be accessed easily or accessed at all. In that case and in order for CIMS to provide guidance on retention and disposition requirements, an assessment must be completed (see Appendix C for template). At a minimum, this assessment must answer the following:

- Who owns or owned the legacy application?
- What was the function of the application?
- What data and information are contained in the application?
- Is there linked/contingent data that could be external to the application?
- When was the application last used? If possible, TSD may be able to turn on audit logs or review application user access logging to determine last usage.

Note: Legacy applications should not be kept past their retention period (if known) or longer than necessary. Even if the application is currently inaccessible, it is possible the business may be required to produce data or information for Freedom of Information (FOI) requests or other legal reasons in which case Divisions may be required to recover it through the use of extensive, and often expensive, forensic tools. In such instances, the business area must consider the business value of retaining data and information past its retention period versus the cost of having to potentially recover it.

For data and information that must be retained because retention is not yet expired:

- Determine how long the application must remain operational to accommodate the retention schedule.
- If the application cannot remain fully operational, determine if it can be maintained in offline or in a lower-capacity form e.g. Read-Only.
- If maintaining the application in any form is not feasible, determine alternative storage locations e.g. server, external hard drive, or shared drive, until the retention period has expired.

For information that can be disposed of:

- Work with TSD to apply deletion of data and information in the application.
- Capture and document the date and time this occurred (audit log) and attach it to the assessment.

- Store the assessment with other divisional records regarding disposition management.
- Inform CIMS staff once the application has been decommissioned.

5.5 Data and Information in Testing and Development Environments

Data and information created in testing and/or development environments for the application to be decommissioned can be considered transitory and disposed of accordingly. Note: Divisional staff may need to work with their Divisional IT and/or TSD to delete this data and information.

5.6 Data and Information on Backup Media

Data and information on backup media for the application to be decommissioned falls under existing retention and disposition schedule which is A1550 & 2 Years, respectively. It allows this backup data and information to be destroyed as part of a normal backup process, without requiring a waiting period to proceed with the decommissioning process.

Unique or one-time backups may also be created by TSD or your Divisional IT to mitigate against the risk of an unsuccessful data migration. Once verified and quality assurance activities are completed, these files can be considered transitory and disposed of by TSD or your Divisional IT.

Need Help?

The scenarios presented in this guideline represent a sampling of possible situations that may occur when decommissioning applications. For information management questions/requirements when decommissioning applications not covered here, please contact CIMS.

Contact

For further assistance please contact:
Manager, Policy and Standards
Corporate Information Management Services, City Clerk's Office

Appendix A: Definitions

Application: A computer program designed to help end users perform activities or tasks. (Source: ARMA Glossary, 5th Edition, TR 22-2016)

Backup: Files, equipment, data and procedures available for use in the event of a failure or loss, if the originals are destroyed or out of service. (Source: City of Toronto - Standard for Backup Operations – TSD)

Conversion: process of changing records from one format to another while maintaining the characteristics of the records (Source: ISO 13008:2012)

Data: Any symbols or characters that represent raw facts or figures and form the basis of information. (Source: ARMA Glossary, 5th Edition, TR 22-2016)

Data Cleansing: process of reviewing and correcting data to ensure data are in a standardized format. **Note:** Correction may be carried out for incompleteness, incorrect formatting, obsolescence, duplication, etc. It is often done prior to merging data sets or converting data from one application/database to another. (Source: ISO 13008:2012)

Decommissioning: is a process by which a business application is shut down and removed from use. (Source: City of Toronto)

Disposition: the action taken with regards to recorded information including destruction, transfer to another entity, or permanent preservation at the end of its retention period. (Source: City of Toronto Information Management Glossary)

Information: Data that has been given value through assessment, interpretation, or compilation in a meaningful form. (Source: ARMA Glossary, 5th Edition, TR 22-2016)

Legacy Application: An application kept in archival format or in continued use despite the obsolescence of its operating systems or programming. (Source: ARMA Glossary, 5th Edition, TR 22-2016)

Migration: process of moving records, including their existing characteristics, from one hardware or software configuration to another without changing the format. (Source: ISO 13008:2012)

Obsolete: no longer in use no longer useful; no longer current (Source: Merriam-Webster)

Record: Information however recorded or stored, whether in printed form, on film, by electronic means or otherwise, and includes documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings, photographs and films. (Source: City of Toronto Information Management Glossary)

Retention Schedule: An authority comprising of a description of a body of records, a retention period for those records and a disposition rule stating whether, at the expiry of the retention period, the records are to be destroyed or preserved by the City Archives. (Source: City of Toronto Information Management Glossary)

Transitory Record: A record that meets at least one of the following criteria:

a) Required solely for the completion of a routine action, or the preparation of another record.
b) Not an integral part of a City record (for example, a photocopy of a record or a record filed with other, transitory, records).
c) Not required to meet statutory obligations or to sustain administrative or operational functions.
d) Records that have been transferred to and reviewed by the City Archives, in accordance with the retention schedule, that have insufficient value to warrant retention by the Archives

(Source: Toronto Municipal Code, Chapter 217, Records, Corporate (City) Chapter 217

Appendix B: Decommissioning Planning Checklist

Introduction

This checklist identifies record and information requirements and other considerations for Divisions who are decommissioning their business systems. It can be used for planning and coordination with teams such as Divisional I&T, Technology Services Division, and/or other Divisions who are also using the system.

If you have any questions about the content in this checklist please don't hesitate to reach out to Corporate Information Management Services at infomgmt@toronto.ca.

Division:		Completed by:	
Business Unit:		Date Completed:	
Divisional Contacts:			

Record and Information Management Considerations

Question	Details	Response (Y/N)	Outcome
1. Have application data and information been mapped to an authorized retention and disposal schedule?	• Retention and disposition schedules are issued by Corporate Information Management Services and published under Municipal Code, Chapter 217, Schedule A, Records Retention Schedule. If no authorized retention and disposition schedule exists for the data and information under consideration, please contact CIMS for assistance.		
2. Are the data and information in this application duplicated across multiple applications or data repositories?	• Information may be duplicated across several City applications to provide service delivery. There may be an opportunity to consolidate these repositories at the time of decommissioning and determine which records may be retained if required. Those considered transitory can be disposed of.		

Question	Details	Response (Y/N)	Outcome
3. Is the application a relational database that contains rows, columns, and tables that pull data when queried to create a record?	• Are these combined data being saved as records, especially if business decisions are being made based on this information?		
4. Does the application contain data and information scheduled for long term retention, permanent retention, or archival retention?	• If so, divisions will need to plan for the management of this information and can contact CIMS to discuss digital preservation methods.		
5. Has the metadata and application documentation needed to support the integrity of data and information during migration been identified?	• Divisions will need to consider identifying and defining their metadata requirements.		

Other Considerations

Question	Details	Response (Y/N)	Outcome
6. Have information architectures been reviewed to ensure all dependencies on the data in this application have been resolved?	• For example, an Identity and Access Management Directory may contain data which is needed to verify action/approval metadata in an application workflow.		
7. Does the application function as a source of authority for a high value dataset?	• Does another City division or public sector entity rely on the data in the application, despite business value having ceased for the division?		
8. Does the application contain valuable data and information about businesses	• Is there a reasonable expectation that data in applications about interactions with other governments will need to be maintained on an ongoing basis?		

Question	Details	Response (Y/N)	Outcome
and individual clients' interactions with other levels of governments?			
9. Are there any Open Data sharing agreements in place?	• e.g. requirements for the City to retain data and information for longer to make it available to the public.		
10. Does the application have dependencies on other applications?	• e.g. Where records are dependent on data in other linked applications such as case management files. • If so these need to be explored further to determine impacts to business processes/workflows before proceeding with decommissioning.		
11. Does the application serve multiple Divisions or business areas that may not be decommissioning all data/information at the same time?	• Divisions or business areas may not be able to proceed with all of their decommissioning activities until all users and the application are ready to be decommissioned and should plan accordingly.		

Appendix C: Decommissioning Assessment and File Inventory Tool Template

This template can be found on the Corporate Information Management Services Policies and procedures website: http://insideto.toronto.ca/clerks/policies/files/decommissioning-assessment-file-inventory.xlsx