Information Management Guideline – Digital Records Conversion and Migration

Guideline No.: CIMS-G018

Version No.: 1

Issued On: October 19, 2023

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

Subject: Information Management

Keywords: Conversion, Migration, Data, Digital, Information Management, Records, System, Storage, Protection, Formats, Metadata

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 (CIMS)
- **Divisions & Business Units:**
  - Corporate Information Management Services (CIMS), City Clerk's Office
  - Office of the Chief Information Security Officer (OC)
  - Technology Services Division (TSD)

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
Kristie.Pratt@toronto.ca

Contents

1. Introduction

Digital conversion refers to the process of changing records from one record format to another while maintaining the characteristics of the record. Digital migration refers to the process of moving records, including their existing characteristics, from one hardware or software configuration to another without changing the format.

Digital record formats include, but are not limited to:

- Word processing application files, e.g., DOCX, PDFs or TXT files;
- Spreadsheet application files or structured data, e.g., PDF/A, CSV, XLSX, XML;
- Image files, e.g., TIFF, JPG, PNG;
- Graphics, e.g., TIFF, PDF;
- Video files, e.g., Motion JPEG 2000, MOV, AVI, MPEG-4;
- Audio files, e.g., WAV, AIFF, FLAC; and
- Email messages, e.g., MSG, PST, and XML email preservation format.

Digitally converting and/or migrating City information may occur over the course of different City initiatives and may be driven by:

- A strategic Information Management process,
- A proactive information governance initiative,
- The decommissioning of a system or application or a technology modernization,
- Ensuring the preservation of and continued access to records that must be retained for long-term preservation purposes, and
- Business continuity planning.

Additionally, there may be legislated requirements to manage records with long-term, archival, or permanent retention.

City staff are responsible for ensuring Information Management requirements are in place to preserve the authenticity and integrity of digital information and metadata during the conversion and migration process. This guideline is based on International Organization for Standardization (ISO) 13008:2022 Information and documentation — Digital records conversion and migration process, which specifies the planning requirements and procedures for the conversion and/or migration of digital records in order to preserve the authenticity, reliability, integrity and usability of records.

City Divisions configuring new solutions must plan for the management of existing data, which is a key deliverable of projects. This planning will ensure that the data populating the new system is fit for purpose.

This guideline provides a framework to support assessment of the degree of difficulty, required level of effort, planning and performance of this work to ensure it is neither underestimated nor accounted for too late in the process.

As digital record formats and requirements evolve, City Divisions should take a proactive approach to ensuring records stay accessible and usable (i.e., you can find, open, work with, understand, and trust them) for the duration of their lifecycle, often referred to as digital continuity.

2. Purpose

This Guideline provides a framework, advice and an overview of the Information Management responsibilities for City staff when:

- Converting digital records from one format to another; and
- Migrating digital records from one hardware or software configuration or solution to another.

Following this Guideline will ensure:

- A consistent approach when migrating and converting digital records;
- The integrity and authenticity of digital records by providing evidence of business activities, decisions or transactions; and
- A consistent approach to the long-term preservation of digital records.

This Guideline builds on the City's Information Management Accountability Policy, and the Digital Infrastructure Strategic Framework's, commitments to "A Well Run City", “Democracy and Transparency”, “Digital Autonomy”, and “Privacy and Security”, which includes the management of City records and information to:

- Enable high quality, resilient and innovative public services; and
- Support the use of data and evidence to inform decision-making.

3. Application

This Guideline applies to all City of Toronto Divisions, employees, volunteers and contract employees involved in the process of converting digital records and/or migrating digital records between technology solutions, whether ad-hoc projects or programs for regular and ongoing conversion or migration. This Guideline may also be useful to those managing or implementing the technical aspects of conversion and/or migration by providing a better understanding of key risks to the continuity and integrity of information, but is not intended to be a technical standard for conversion and migration.

This Guideline does not apply to:

A. **Elected Officials**
Management of Elected Officials' information is at the discretion of the appropriate Elected Officials.

B. **Accountability Officers**
The City's Accountability Officers include the Auditor General, Integrity Commissioner, Lobbyist Registrar, and Ombudsman. The City of Toronto Act requires that the Officers independently perform their duties and establish confidentiality requirements for information in their custody or control. These confidentiality requirements are recognized in Toronto Municipal Code Chapter 3, Accountability Officers, and the City's Protection of Accountability Officers' Information Directive developed to safeguard the confidentiality of the Officers' information and records.

C. **Agencies and Corporations**
The City of Toronto encourages City Agencies and Corporations to review, adopt, or update this Guideline as appropriate to their business needs.

4. Scope

This Guideline should be applied when converting and/or migrating digital records, and the metadata used to describe and/or arrange them, to another digital format or digital environment. This Guideline is not meant to provide guidance to staff during the digitization of physical records (see the Creating and Managing Digitized Records Standard), or the decommissioning of business applications (see the Managing Data and Information when Decommissioning Business Applications Guideline).

5. Drivers

A variety of drivers can compel a Division to convert or migrate its digital records. When an application is being decommissioned, its records may have lengthy retention requirements, requiring the Division to convert or migrate those records while the supporting systems are still viable. Divisions might also choose to convert or migrate records proactively due to operational factors relating to record volume, access, storage efficiency, business and technology cycles, or organizational change (such as restructuring).

The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) provides staff and the public with a “Right of Access”. The right of access applies to existing records, in whole or in part, that fall within the custody or control of the City. The City must manage its information and records so that staff and the public can easily search, access, and use them, in accordance with this legislation and associated policies. For the most part, City records should be made available to the public, media, agencies and other City Divisions (with limited and specific exceptions). Converting or migrating these

digital City records may be a driver in allowing the City to carry out these responsibilities under MFIPPA.

Conversion Drivers

Conversion is defined as the process of changing records from one format to another. Some examples of drivers that could require digital conversion include:

- Format change: for example, digital records stored in a proprietary format are converted to an open file format, such as a conversion of a .docx file to PDF/A.
- Format obsolescence: for example, digital records stored in an obsolete but still readable word processing format are converted to a current word processing format.
- Interoperability: for example, digital records are converted to a format that ensures seamless interoperability with IT infrastructure.
- Legal issues: records are converted according to existing explicit legal or regulatory requirements concerning formats or service providers.

Migration Drivers

Migration is defined as the process of moving records from one hardware or software configuration to another without changing the format. Some examples of drivers that could require digital migration include:

- The need to migrate records from one structure to another. For example, records existing in several legacy databases might be restructured into a new consolidated database (e.g., from Oracle to SQL Server).
- The platform in which the records were created is changing and the records need to be migrated to the new platform. For example, records might need to be moved from a Microsoft Windows platform to a UNIX platform.
- Migration is a practical option from a business perspective (e.g., to introduce a new system with improved functionality).
    - For example, a migration of records might be needed to support a change from a legacy technology solution to a new cloud technology, reflecting new business practices, or to move records from a shared drive to a records management system.

In extreme circumstances, organizations might be compelled to convert or migrate records in response to regulatory or legal actions.

6. Risks when Converting and/or Migrating Digital Records

Prior to conversion and/or migration, City staff are responsible for ensuring all information is stored in a manner designed to ensure its accessibility, integrity,

confidentiality, and authenticity. Conversion from one storage medium to another must include adequate controls to support these requirements.

When converting or migrating digital records, there is a risk to physical and logical security. Physical security means access control to buildings, rooms and physical IT assets; logical security means access control to the platform in which the conversion or migration is being undertaken. The conversion and migration process should not result in any unintended change to existing access rights to the data. Access controls must be thoroughly tested as part of the implementation plan.

The conversion or migration of digital records from one technology environment to another can alter the content, context, sequence or structure of the records. If this occurs, the Division might risk non-compliance with both recordkeeping requirements through loss of the records' reliability, integrity and authenticity. With each successive format conversion, the possibility of data loss or corruption increases. An effective digital conversion and migration plan can be used to identify all characteristics of the records that shall be preserved after the records have been converted or migrated.

There is additional risk when digital records contain personal and personal health information. For example risks to privacy may be introduced when converting digital records, as the project may unintentionally expose information in the digital record through actions such as data transformations or new data joins. City Divisions must work with Corporate Information Management Services and the Office of the Chief Information Security Officer to ensure appropriate assessments are in place to protect information. If you have questions or concerns about identifying personal information or risks related to privacy obligations, please contact privacy@toronto.ca. For questions or concerns about identifying personal health information or risks related to personal health information privacy obligations, please contact the appropriate Health Information Custodian.

7. Best Practices when Planning for Digital Records Conversion and/or Migration

Primary factors to consider when converting or migrating digital City records include:

- Defining the information and the associated metadata in scope (including records retention schedules and identifying personal information),
- The risks to digital continuity, privacy and security; and
- Non-compliance with legislative or legal requirements; and lack of key functionality in the target technology.

Additional factors include:

- Engaging the Office of the Chief Information Security Officer (OC) for a Privacy Impact Assessment
- Ensuring Digital Rights Management access permissions and monitoring access controls are enabled;
- Structural reorganization (e.g., ensuring access and permissions for the digital records are appropriately changed based on new structures, roles & responsibilities);
- Incompatibility with newer systems and inability to integrate;
- Redundant and duplicate material;
- Inaccuracies, including data or metadata loss;
- Metadata or digital records requirements for compliance with the Accessibility for Ontarians with Disabilities Act (AODA)

When planning to convert and/or migrate digital records, consider the following best practices before beginning the process:

Risk – Identify potential project risks related to data conversion and migration as early in the project life cycle as possible, e.g., converting to new formats may impact stored personal information. Document these initially identified risks in the project charter and clearly communicate their mitigation plans, potential consequences to project sponsors and stakeholders.

Communicate – Prevent confusion and/or misinterpretation by effectively communicating every detail and step of the planned migration/conversion process, and educating stakeholders on the outcomes of the process.

Engage – Involve business owners and other relevant stakeholders to understand business continuity and functional requirements for their records and metadata before, during and after conversion and migration. Successful migrations are often executed with the use of Subject Matter Experts (SMEs) of the original application. Increased complexity in file structure and formats make this expertise invaluable.

Backup – Following a full-scale backup, system backups should be taken incrementally to allow the project team to revert back to any point in the system's life.

Auditing – Proper audit log management ensures the security, integrity, and compliance of City digital records, including sensitive, personal information or personal health information (PHI). Audit logs should be maintained, appropriately retained, and all relevant activities and changes must be captured during the conversion or migration.

In the context of PHI, ensure that the project understands the specific requirements for auditing under the Personal Health Information Protection Act (PHIPA).

Approval – Identify the Divisional or project authorization needed to verify that the conversion and migration process has been appropriately planned and successfully performed in compliance with relevant policy and procedures (e.g., this Guideline, records retention policy, metadata standards, Divisional conversion and migration procedures, etc.).

8. Guidelines for Digital Records Conversion and Migration:

The key to a successful conversion and/or migration of digital records is thorough planning and preparation, as well as careful execution and testing to ensure the records are transferred correctly and are functioning as expected in the destination systems or applications. Digital records may be migrated without the need for conversion or converted without the need for migration. Identify these requirements early in the project. Section 8 of this Guideline provides details on converting and/or migrating digital records. Section 9 of this Guideline provides details on managing metadata when converting and/or migrating digital records.

1. Create an inventory of the digital records to be converted and/or migrated: Begin by identifying the records that need to be converted and/or migrated, including their format, the source solutions or applications they are currently stored in, and the destination/target solutions or applications they will be moved to. The "Inventory" tab on the Decommissioning Assessment and File Inventory Tool may help you document. For assistance inventorying the digital records, contact Record Services. This includes an inventory of the metadata (described in section 9.1). The inventory may also include the information protection classification of the digital records being converted and/or migrated (see Information Protection Classification Standard).
2. Classify the digital records. Identify the applicable retention schedule(s) of the digital records to be converted and migrated. The inventory will enable the identification of any records or data eligible to be authorized for disposition in accordance with the schedule, as well as what digital records must be retained and for how long in the destination application. For assistance classifying the digital records, contact infomgmt@toronto.ca.
3. Assess the quality of the digital records: Before proceeding with the conversion and migration, it is important to assess the quality of the digital records and metadata to ensure that they are complete, accurate, and consistent. This may include reviewing the data for errors, inconsistencies, or missing values, and taking steps to correct any issues that are identified.

4. Develop a conversion and migration plan: The most important factor in a successful conversion/migration is careful planning of every detail, step, stakeholder, and resource needed to execute the conversion/migration of the digital records. A conversion and migration plan should aim to reduce the risk of degradation of the content, context, legal authenticity, and structure of the records to an absolute minimum.
    - Once the digital records have been inventoried and assessed, develop a detailed conversion and/or migration process plan.
    - The plan should outline steps to convert and migrate the digital records, as well as any resources or tools that are required.
    - Additionally, a methodology for comparing the content, context, legal authenticity, and structure of the converted/migrated digital records with the source digital records should be established so problems can be identified, corrected, and validated.
    - Identify records that have relationships with other records or are linked and establish whether existing relationships or links could be compromised by the conversion or migration. Establish safeguards to protect these links during the conversion or migration. There may be instances where new linkages must be created, e.g., when converting or migrating personal information, to ensure re-identification of individuals or profiles does not occur under incorrect conditions.
    - Determine whether the significant properties—the characteristics of the digital record or object, e.g., the appearance of the record, its formatting, colours, fonts, etc.—contributes to its meaning as a digital record. If appearance is integral to the meaning, the plan should address how to maintain it. Once conversion or migration is complete, document any changes to the appearance of the record.
    - Define the selected target formatting of the digital records. Project teams should avoid proprietary formats where possible to ensure target data can be used consistently over time, without restriction.
    - Configure the migration/conversion software (if needed)
5. Obtain approval: Once documented, obtain approval of the conversion or migration plan from the authorized person or body.
6. Test a sample: Perform the conversion and migration process testing on a sample copy of the records. Test cases must avoid using live data to ensure original files are not deleted or altered, and to ensure any legislative and policy requirements are met.
7. Full Test: Perform a controlled, full-volume test of the activities required when converting or migrating records to the target solution. This is an end-to-end test

of the entire record conversion and/or migration process and the records on the new system or in the new format. It includes, but is not limited to, testing the processes and procedures planned for the conversion/migration, the new solution data, business rules, and technology. This may be less important in small low-risk project but is especially important in large high-risk projects where many users may be impacted by unforeseen events resulting from the migration.

8. Convert the digital records: If conversion is necessary, follow the conversion plan to convert the records to the desired format. This may involve using conversion tools or scripts, or manually reformatting the records.
9. Validate the converted digital records: After the records have been converted, it is important to validate them to ensure that they have been converted correctly, are in the desired format, and are accurate and complete. This may involve comparing the converted records to the original records or testing the records in the target solution or application.
    - This is an important time to consult with stakeholders (data users, stewards, etc.) to aid in the digital record validation. Data users will be better suited to notice discrepancies in the information they routinely work with.
10. Migrate the digital records: If migration is necessary, follow the migration plan to transfer the records to the destination system or application. This may involve using data migration tools or scripts, or manually transferring the records.
11. Test and validate the migrated digital records: After the records have been migrated, it is important to test and verify that they have been transferred correctly and are functioning as expected in the target solution or application. This may involve running test queries or scenarios to ensure that the records are being accessed and used correctly.
12. Document the completed conversion and/or migration process: This documentation should demonstrate that all records, including those created while the conversion/ migration activities were in progress, have been converted/migrated.
    - Document the steps that were taken during the conversion and migration process, including an issues log containing issues or challenges that were encountered and how they were addressed (e.g., lost or corrupted data, inconsistencies, technical failures, etc.). This documentation will be useful for future reference and for troubleshooting any issues that may arise. It will also ensure that the organization continues to possess complete, accessible and authentic records throughout their full retention period, including those created while the conversion/migration activities were in progress. Artefacts the project should create during this documentation process include, but are not limited to:

- Data dictionaries
- Data maps
- Table structures
- System documentation

13. Where applicable, dispose of the source digital records: The source records may need to be disposed of once the validation is complete and all problems are fixed, and such decisions and subsequent actions are auditable, documented, validated, and approved by the appropriate authority. Contact CIMS to ensure that all legislative and policy requirements are met before any source records are destroyed and that records destruction is documented and approved.
14. Refer to the Managing Data and Information when Decommissioning Business Applications Guideline if your solution or application must be decommissioned.
15. Monitor and maintain the migrated digital records: After the records have been successfully migrated, it is important to ensure that they remain accurate, complete, and consistent. This may involve regularly reviewing and updating the records, implementing processes to manage changes or updates to the records, and/or establishing an appropriate standard of data quality in the target solution.

9. Guidelines for Managing Metadata during Conversion and Migration:

Metadata is information that describes the characteristics and context of digital records. This can include such things as the date and time the digital record was created or what sort of access and permissions are assigned to the digital record in order to prevent unauthorized access. In the context of digital records conversion and migration, there are two areas of focus: event history metadata and the digital record's metadata.

Event history metadata documents the conversion and/or migration process and provides the information that allows one to demonstrate that a record, having gone through the conversion or migration process, continues to be authentic, reliable, and usable and that the meaning and context of the data is preserved. Every conversion or migration process should create an event history metadata for the individual records being converted or migrated.

Separately, conversion and migration processes must ensure that the metadata about the records continues to be persistently linked to the converted or migrated record. Without an adequately defined metadata structure, digital preservation initiatives cannot be sufficiently supported. For more information on metadata requirements for managing records, see the City's Records Management Metadata Standard and ISO 23081-2, which identifies generic types of metadata that are required to fulfil the requirements for managing records.

1. Inventory the metadata associated with the digital records to be converted and/or migrated: Begin by identifying the metadata associated with the records, including any metadata standards or schemas that are being used. Take inventory of your current metadata and determine what needs to be converted and migrated, for example, ensuring that any metadata required for AODA compliance remains intact. This will help you understand the scope of the project and allow you to prioritize which metadata should be converted first. For more information on standardizing metadata, contact the Vocabulary and Metadata Program (CIMS) at cvsupport@toronto.ca.
    a. Define what metadata and data are needed to reproduce a complete and reliable record so that this data can be protected during the conversion or migration.
    b. Define what metadata are needed in order to identify and use the record so that the record can be searched for and accessed after the conversion or migration.
2. Assess the quality and current state of the metadata: As with the digital records themselves, it is important to assess the quality of the metadata to ensure that it is complete, accurate, and consistent. This may include reviewing the metadata for errors, inconsistencies, or missing values, and taking steps to correct any issues that are identified.
3. Disposition of metadata: Determine the disposition of the originating version of the record's metadata. At a minimum, they will be removed from the source system and retained until the new version of the digital records has been integrated into the target system. Whether this version continues to be maintained for a specified or indefinite period or destroyed should be informed by the City's records policies. For assistance classifying the metadata, contact CIMS.
4. Develop a plan for managing metadata during the conversion and migration process: Before starting the conversion process, it is important to plan out the entire process and identify the specific goals and objectives of the migration. This helps ensure that the conversion is smooth and successful. Develop a plan for how the metadata will be managed during the conversion and migration process, including any tools or processes that will be used to convert or migrate the metadata.
    a. Define what metadata and data are needed to retain the ability to reproduce a complete and authentic record so that this data can be protected during the conversion or migration.
    b. Define what metadata are needed in order to identify and use the record so that the record can be searched for and accessed after the conversion or migration.

c. Document any attributes of the record that should not be converted to the new format, or migrated to the new system, and state the reason.

d. Document relationships in metadata to be maintained during conversion/migration. The "Metadata" tab on the Decommissioning Assessment and File Inventory Tool may help you document. Examples of relationships include:
   i. Internal relationships, i.e., within the document, such as a document containing a linked spreadsheet or images;
   ii. Functional relationships, e.g., between records documenting related aspects of the business;
   iii. Aggregational relationships, e.g., documents aggregated to files/folders;
   iv. Structural relationships, e.g., between records and creating agents, or business;
   v. Systematic relationships between records and control tools, e.g., business classification schemes, disposition authorities, access and security controls, and mandates (these control tools contain contextual information which informs the meaning of the record).

e. During conversion/migration, the existing event history metadata should be migrated with the record in order to ensure the ability to affirm the authenticity of the record. Every conversion or migration process should create event history metadata for every individual record converted or migrated.

f. Ensure any legacy metadata not captured in the target solution's standard metadata fields is still captured and accounted for in a custom field(s), so it is retained. If metadata cannot or will not be migrated (system limitations, volume, etc.), please contact CIMS to determine if the digital records may be destroyed.

5. Obtain approval: Once documented, obtain approval of the metadata conversion and/or migration plan from the authorized person or body.
6. Convert and migrate the metadata: Follow the conversion and migration plan to convert and migrate the metadata to the desired format and destination. This may involve using conversion or migration tools, or manually reformatting and transferring the metadata.
7. Validate and test the converted and migrated metadata: After the metadata has been converted and migrated, it is important to validate and test it to ensure that it has been transferred correctly and is functioning as expected in the destination system or application, including the relationships between the metadata and digital records (documented in step 9.3.d). This may involve comparing the

converted metadata to the original metadata or testing the metadata in the destination system or application.

8. Document the metadata conversion and migration process: Document the steps that were taken to manage the metadata during the conversion and/or migration process, including any issues or challenges that were encountered and how they were addressed. This documentation will be useful for future reference and for troubleshooting any issues that may arise. It will also ensure the process can be repeated or modified in the future if necessary.
9. Consider ongoing maintenance: Digital metadata will require ongoing maintenance and updates. Make sure to put processes in place to ensure that the metadata remains accurate and up-to-date.

9. References

- Acquisitions Policy for the City of Toronto Archives
- CDC Unified Process Practices Guide: Data Conversion
- Digital Preservation Policy
- Information Management Accountability Policy
- ISO 13008:2022 – Information and documentation — Digital records conversion and migration process
- ISO 23081-2 – Records Management Metadata for Records
- Managing Data and Information when Decommissioning Business Applications Guideline
- Municipal Code Chapter 217, Records, Corporate (City)
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA)
- Privacy Impact Assessment Policy
- Protection of Privacy Policy
- Records Management Metadata Standard
- Responsible Record-Keeping Directive
- Schedule A – Records Retention Schedule, Chapter 217 of the Toronto Municipal Code.

10. Guideline Approval

Approval provided by Kristie Pratt, Deputy City Clerk, effective October 19, 2023.

11. Guideline Review

The City Clerk's Office will review this Guideline and its effectiveness as needed.

Appendix

Appendix A: Definitions

Authoritative Record: The record that is considered the official City Record for evidentiary purposes.

Authenticity: In the context of this guideline, refers to a record being what it purports to be. In the case of digital records, it refers to the trustworthiness of the digital record as a record.

City Record: A record created or received in the course of City administration or delivery of City services. Also includes records that were created or received in the course of City of Toronto predecessor municipalities' administration or delivery of City services. These include records created, accumulated, and used by a member of Council in the course of the responsibilities specifically imposed on a member of Council under the City of Toronto Act, 2006.

Data: Facts represented as text, numbers, graphics, images, sound, or video. Data is the raw material used to represent information, or from which information can be derived.

Digital Conversion: The process of changing records from one format to another while maintaining the characteristics of the records, i.e., preserving their authenticity, reliability, integrity and usability. This may include the appearance of the record, its formatting, colours, fonts, etc.

Digital Migration: The process of moving records, including their existing characteristics, from one hardware or software configuration to another without changing the format.

Digital Record: Data or information that is fixed in a non-human readable format that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference.

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.

Integrity: In the context of this guideline, refers to a record being protected against unauthorized alteration.

Linked Data/Records: Structured data which is interlinked with other data so it becomes more useful through semantic queries.

Metadata: Data describing context, content, and structure of records and their management through time. Metadata can describe the properties of a document. For example, the following information about a document is typically recorded: Title (or name of the document), Date (the document was created), and Created By (document

creator). These descriptors are known as 'metadata'. Metadata facilitates search, identification, and the management of information.

Open Format File: A file format with no restrictions, monetary or otherwise, placed upon its use and can be fully processed with at least one free/open-source software tool. Patents are a common source of restrictions that make a format proprietary. Often, but not necessarily, the structure of an open format is set out in agreed standards, overseen and published by a non-commercial expert body.

Proprietary Format: A proprietary file format is one that a company owns and controls. Data in this format may need proprietary software to be read reliably. Unlike an open format, the description of the format may be confidential or unpublished, and can be changed by the company at any time. Proprietary software usually reads and saves data in its own proprietary format. For example, different versions of Microsoft Excel use the proprietary XLS and XLSX formats. When a format is proprietary, the onus is on the user to confirm permission to use for conversion or migration.

Physical Record: Refers to the original (physical) record that was used to create a digitized record. Examples of physical records include microfilm, microfiche, paper documents, photographs, drawings, plans, etc.

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. This includes City records.

Reliability: In the context of this guideline, refers to the ability of a record to be trustworthy as evidence and have the ability to stand for the facts it is about.

Retention Period: The retention rule stating how long a record must be retained by the City.

Retention Schedule: An authority comprising 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 of Toronto Archives.

Significant Properties: Characteristics of digital and intellectual objects that must be preserved over time in order to ensure the continued accessibility, usability and meaning of the objects and their capacity to be accepted as (evidence of) what they purport to be.