Information Management Guideline – Data Residency for Cloud Technology

Guideline No.: CIMS-G017

Version No.: 1.0

Issued On: August 21, 2023

Approved On: June 8, 2023

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

Subject: Cloud Technology Data Residency

Keywords: Data Residency, Data, Information, Management, Cloud, Technology, Solution, Storage, Protection, Privacy, Data Centres

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

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

Table of Contents

1. Introduction

The City of Toronto has obligations to protect data and information and to ensure the security of records in its custody or under its control (collectively "City information"). When the City utilizes cloud technology (including but not limited to systems, applications, or repositories) to store City information, City Divisions require guidance on assessing the risks to protecting City information arising from the location(s) of those cloud data centres and how to mitigate such risk. Cloud technology inherently raises the risk that City information may move from one specified location to any other part of the world.

Traditionally, City information has been stored in on-premise servers at the City; the City currently utilizes cloud technology in an increasing role in the delivery of City services. Cloud data centres can be located outside of Canadian borders and larger providers of cloud technology often have functions distributed over multiple data centres. The fact that City information may cross jurisdictional borders through the use of cloud technology raises additional and unique privacy and security concerns not present with on-premises servers that Divisions and project teams must consider when using cloud technology.

Privacy and security requirements for the City are informed by two governing pieces of privacy legislation:

1. The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), with reference to the City's operations generally; and
2. The Personal Health Information Protection Act (PHIPA), with reference to specific City operations which constitute Health Information Custodians (HICs), as defined by PHIPA.

Additionally, the City has specific record retention and security requirements for all City information which are established by the City of Toronto Act, 2006 (COTA).

This Guideline is aligned with the provisions of these pieces of legislation, as well as with the City's Information Management Accountability Policy, the City's IT Cloud Strategy and the Digital Infrastructure Strategic Framework (DISF), which define the roles, responsibilities, and principles required to enable this legislation.

This Guideline provides a mechanism to apply privacy protections to City information stored in cloud technologies.

Foreign Jurisdiction Risk

There is no legislative requirement specifically mandating data residency requirements for City information. City officials must be aware when data is stored outside of Canada, controls may be diminished and additional risks will be introduced, the "Foreign Jurisdiction Risk".

City information, whether personal information or otherwise, when placed outside of Canada will be subject to the laws of foreign jurisdictions. The City will still be obligated to ensure the City information complies with the laws of Ontario and Canada which apply to the City as an Ontario Municipality. Once City information is placed outside of Canada, it is subject to multiple sets of legal regulation, the laws of the jurisdictions in

which it is located and Canadian laws. For example, City information stored in countries belonging to the European Union will be subject to the EU's General Data Protection Regulation (GDPR), subject to its compliance requirements and fines for non-compliance; as well as the relevant provisions of the laws of Ontario and Canada applicable to the City.

The risk of these multiple sets of laws applying to the City information, and potential conflict between these laws, must be managed by using contractual requirements that establish adequate security controls for personal information (PI), personal health information (PHI)—when dealing with HIC operations—, and any other sensitive information; and mechanisms to mitigate any breach of PI, PHI, and other sensitive information; as well as to comply with the specific record management and privacy obligations imposed under COTA, MFIPPA, and/or PHIPA on the City concerning City information.

Successful mitigation of the Foreign Jurisdiction Risk requires the City Division procuring the cloud technology to have suitable measures in the contract to ensure requirements meet MFIPPA and other legislative obligations, e.g., full extraction of all City data if reasonable grounds for concern of a conflict between the City's mandatory legislative obligations and the obligations imposed by the laws of a foreign jurisdiction.

Consultations with Legal Services will be required and there may be a requirement for the Division to engage and retain additional legal advice from practitioners who are qualified to advise in this domain. It may be impossible to address the conflict between the laws of the foreign jurisdictions and the laws of Ontario and Canada applicable to the City. Where this occurs, the cloud technology will not be legally permissible for the City to procure.

City of Toronto Data Residency Direction

The City's DISF (4.3 (3)) prioritizes data centres and service providers located within Canada for the storage of City information, reducing risks and ensuring that City information will remain subject to Canadian security, privacy and data protection regulations and practice.

City Divisions are encouraged to meet data protection obligations by prioritizing storage and transmission of City information within Canada as much as reasonably possible when procuring any form of cloud technology. There are risk mitigation actions City Divisions can take to reduce how much this direction limits their ability to engage vendors in other jurisdictions who can offer the City solutions that support rapid modernization of services and technology.

City Divisions can demonstrate compliance with legislation by:

- Assessing and implementing data and information management best practices in cloud technologies, including data residency requirements and Information Protection Classifications;
- Assessing the risks of storing, accessing and/or transferring data outside of a Canadian jurisdiction; and

- Applying data residency guidelines and policies, along with associated legislative requirements, for City information contained in a cloud technology which is to be:
    i. transferred, stored or accessed in the cloud technology;
    ii. transferred, stored or accessed in another technology; or
    iii. shared with external entities.

Subject Matter Experts in Corporate Information Management Services (CIMS) in the City Clerk's Office, Technology Services Division (TSD), the Office of the Chief Information Security Officer (OC), and/or Divisional IT teams can support City Divisions when completing these activities.

2. Purpose

The purpose of this Guideline is to provide guidance on the Information Management responsibilities for City staff when procuring new cloud technology, or when using cloud technology to process, retrieve, transmit or share data and information, with regards to the location where that City information resides. This Guideline is in place to ensure appropriate Information Management controls are designed, implemented, maintained and leveraged to protect City of Toronto information stored utilizing cloud technology.

The Guideline defines:

- How to ensure compliance with relevant legislation and policy
- Guidelines for enabling appropriate and safe data residency when utilizing cloud technology
- Guidelines for documenting, mitigating, and accepting risk when unable to select cloud technology with a data centre in Canada

3. Application

This guideline is applicable to all City of Toronto Divisions, employees, volunteers and contract employees, including sub-contractors.

This Guideline is intended for use by staff in roles that involve:

- Any technology initiative that has a cloud technology component
- Any data sharing agreement that may use a cloud technology storage application for access, retrieval and/or transmission of City information
- Staff use of cloud technology for tasks that include but are not limited to file transfers, surveys, information collection or distribution, records storage, and/or external data sharing
- Third-party software integrations or middleware providing/enabling services, automation, or artificial intelligence tools for description, tagging, key wording, organization, deduplication, or file manipulation

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 their information. 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.

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.

D. The location in which City employees work from, whether in-office, hybrid, or remote work. This is supported by the Remote Work Policy.

4. Data Residency Principles

While ensuring the use of data centres located in Canada is considered best practice, it will not always be possible to utilize them without limiting the ability of the City to engage some vendors. When using data centres outside Canada, the following principles will help guide project teams:

Principle 1: Proper Application

All information collected, created, or processed in cloud technology (including but not limited to systems, applications, or repositories) in the course of City business ("City information") is subject to privacy legislation, policy, and data residency guidelines based on the level of protection it requires.

- There are six levels of information protection classifications (see the City's Information Protection Classification Standard), ordered from most permissive to least permissive with regards to access and disclosure of that information. Appropriate protections must be applied in accordance with the classifications:
    - **Public Information**: records that are available to the public without restriction.
    - **Routinely Disclosed Information**: records that can be released without a Freedom of Information Request (see the City's Routinely Disclosed Records).
    - **Exempt Information**: records that are exempt under Part 1 of MFIPPA.
    - **Excluded Information**: sensitive or confidential information that has restrictions on its access.
    - **Personal Information:** as defined by MFIPPA, recorded information about an identifiable individual, which includes information related to health matters of an identifiable individual, where not in the custody or control of a HIC.
    - **Personal Health Information**: as defined by PHIPA, identifying information about an individual that is in the custody or control of a HIC.

- City information is subject to COTA, MFIPPA and PHIPA, in addition to City policies and frameworks (see Legislative or Policy Requirements for Data Residency). Some Divisions may also be subject to additional specific legislation dictating privacy requirements for their information handling.

Principle 2: Privacy by Design

The proper application of Privacy by Design principles ensures the inclusion of privacy and data protection into the design specifications at a project's conception in order to facilitate compliance with privacy and data protection principles. Privacy by Design should be the City's default mode of operation. Data residency is applied by design to City technologies, including through the procurement process.

- Data residency should be assessed and standard contractual language built into procurement documentation, contracts, data processing agreements (DPA), and service level agreements (SLAs) when any form of cloud technology is procured, including during non-competitive procurement processes and other cooperative procurement options.
- Systematically integrate information protection into Divisional business practices and technology solution design and implementation, working with CIMS through the Information Management Assessment process.
- Divisions must engage the OC and CIMS when planning a new project or making a substantial change to the way a service collects, uses, discloses or retains Personal Information (PI). Divisions will be guided through conducting a Privacy Impact Assessment and CIMS will assist Divisions with the Information Management, privacy and information collection requirements as required.
- As part of the DISF, cybersecurity risks presented by the use of Digital Infrastructure are to be identified and mitigated, building cyber resilience and trust in the protection of data and digital assets. This includes ensuring encryption of any City data that contains personal information whether in transit, at rest, or in use (4.4 (8)).

Principle 3: Mitigating Risk

Security, control, access and identity management, privacy and modernization risks must be evaluated and mitigated when considering data residency in cloud technologies.

- Security and privacy risks of storage or transmission of personal and/or sensitive information in a jurisdiction outside Canada must be evaluated.
- Private clouds may reduce privacy, security and data protection risks, but may be too costly. Cloud technology outsourced to third parties can be more cost-effective, these forms of outsourced cloud technology will introduce new risks, and may result in non-compliance with legislated obligations for the City. If so, these non-compliant options may not be selected.
- Cloud technology service providers utilizing foreign jurisdictions should provide, at the earliest opportunity, their multi-jurisdictional analysis of the Foreign Jurisdiction Risk, including the specific risk mitigation strategies available in the proposed cloud technology for review by the City's Legal Services.

    - The proposed cloud technology may not be used by the City if cloud technology service providers cannot provide this risk analysis.
- Project teams must consult with Legal, PMMD, CIMS, OC, and TSD to include language in contractual agreements to specify requirements regarding data use and access, encryption, data security, return or disposal of information, retention, breach notifications, auditing, and reporting.
- When unable to create, store, or transmit information in Canada:
    - Project teams develop a risk mitigation plan that outlines all mitigation approaches that will be employed
    - This plan must be documented and reviewed by CIMS, TSD and the OC through the cloud architecture review process
    - Confirm Division Head and Division Legal Representative acceptance of the plan

Principle 4: Divisional Responsibility

Day to day matters of information protection in cloud technology is the responsibility of Divisions.

- Division Heads are responsible for protecting personal privacy in the systems they develop and use to store and access information they create, collect, and steward (see the Information Management Accountability Policy).
- City Divisions must ensure staff, including employees, contractors, and third parties, maintain a level of privacy and information protection awareness appropriate with their responsibilities.
- CIMS will work with Divisions to ensure the requirements of this guideline are understood, integrated into procurement documentation, and communicated to staff.

The City Clerk has been appointed by City Council as the City Official responsible for ensuring that City Divisions meet Information Management legislative requirements and obligations in all aspects of their work.

5. Legislative and Policy Requirements for Data Residency

Although current legislation does not speak to data residency, it provides criteria to determine policy requirements. Prior to use of cloud technology placing City information in foreign jurisdictions, the Division needs to confirm and ensure that suitable contractual measures are in place to eliminate any possibility of the Foreign Jurisdiction Risk resulting in the City not complying with its legislative obligations.

A) Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Ontario's MFIPPA provides individuals with a right of access, subject to limited and specific exemptions, to records under the custody or control of institutions covered by the Act, including the City of Toronto. The purpose of MFIPPA is to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

MFIPPA does not specify requirements for data residency, however, MFIPPA, and the associated regulations, specifically Regulation 823, section 3 includes specific requirements relating to privacy and security:

(1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.
(2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
(3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature and classification of the records to be protected.

Therefore, in addressing data residency, the City should prioritize options which result in the City meeting these standards.

The City must adhere to this act by fully assessing the risks of cloud technology, taking into account the nature of the records to be protected, establishing reasonable measures to prevent unauthorized access, and ensuring that City Staff and retained third parties can only access information they need to perform their duties. Failure to do this will result in failure to comply with the obligations of MFIPPA.

B) Personal Health Information Protection Act (PHIPA)

Ontario's PHIPA and the associated regulation (Ontario Regulation 329/04) set out rules for the collection, use and disclosure of personal health information (PHI). The City must provide individuals with a right to access their PHI, and provide for independent review and resolution of complaints with respect to PHI.

These rules apply to all Health Information Custodians (HICs) operating within the province of Ontario and to individuals and organizations that receive PHI from HICs.

Under PHIPA, a HIC needs to obtain an individual's informed consent to collect, use and disclose PHI.

PHIPA does not specify requirements for data residency, however, the City must adhere to this act by fully assessing the risks of cloud technology and, in most cases, taking into account the nature of the records to be protected. PHI residing in foreign jurisdictions or in cloud technology with poor encryption levels may result in unauthorized access to data and information. Prior to the use of the cloud technology, the Division needs to confirm whether PHIPA applies to the City information held in the cloud technology, and if the cloud technology allows for compliance with PHIPA.

C) City of Toronto Act, 2006 (COTA)

The City is subject to specific record keeping obligations imposed by provisions of the City's fundamental governing legislation, the City of Toronto Act, 2006 (COTA); specifically Section 200 and 201.

The City is required under section 200 to ensure that all records are maintained in a secure and accessible fashion and while those contracted to provide records

management services to the City, by law, adopt this obligation directly (e.g., cloud service providers), this does not release the City from ensuring compliance.

These obligations apply to all copies of City information, for the duration of their lifecycle. For this reason, all records in cloud technology must be:

- Retrievable in a reasonable amount of time;
- In a format that allows the content to be readily ascertained by a person;
- Inaccessible without the City's specific prior consent
- Reasonably protected from unauthorized access
- Destroyed only in accordance with the specific records retention and destruction periods established

These obligations do not directly impose a data residency requirement, however the risks from conflicting laws of foreign jurisdictions and the minimum business requirement of complying with mandatory obligations of the City will need to be assessed and mitigated prior to the adoption of the cloud technology.

D) IT Cloud Strategy

The City's IT Cloud Strategy, adopted in 2018 by City Council, enables TSD to provide oversight of the enterprise-wide adoption of on-demand cloud technology for Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) through governance, compliance and security. It applies to hybrid, private and public cloud types. This strategy is intended to facilitate "digital transformation" by:

- Utilizing cloud technology to improve efficiency and effectiveness;
- Increasing business agility and responsiveness to stakeholders and citizens' desired outcomes in a digital mobile world; and
- Supporting innovation.

The IT Cloud Strategy is based on the principle of "cloud first – but not necessarily cloud". It is premised on the basis that all City information may "go to the cloud", but this possibility is subject to information classification, constraints and controls—meaning that City information will not "go to the cloud" when not appropriate. The IT Cloud Strategy contains data residency guidance which states, "Preferably, all cloud data should be stored in a Canadian multi-zone region under the control of Canadian nationals and subject to Canadian privacy and data protection regulations." (Section 2.1.4).

E) Digital Infrastructure Strategic Framework (DISF)

The City's DISF, adopted by City Council in 2022, sets out the overarching vision for Toronto as a Digital Connected Community. It is a response to the range of opportunities and challenges associated with the use of Digital Infrastructure. Digital Infrastructure includes data collected, stored, or transmitted digitally by the City, including personally identifiable information and non-personal information. The DISF was developed to enhance transparency, accountability and consistency of decision-making, while strengthening the flexibility, safety and efficiency of the City's Digital Infrastructure.

The DISF identifies data residency in Canada as a Strategic Priority, with the following objective: Data residency requirements are applied on new City Digital Infrastructure Initiatives, where appropriate, to enhance privacy and security (section 4.3). Other relevant Strategic Priorities within the DISF include Privacy and Cybersecurity. Implementation considerations within in the DISF include:

1. Ensure that the design, development, procurement, and implementation of Digital Infrastructure considers the issue of data residency at the outset (4.3 (2))
2. Ensure that cloud technology options consider service providers based in, or with facilities located in, Canada (4.3 (3))
3. Ensure encryption of any City data that contains personal information whether in transit, at rest (i.e. in storage), or in use (4.4 (8))

F) Cyber Security Policy

The City's Cyber Security Policy is designed to implement means to mitigate cyber risk while interacting with the City's information and systems. Under its requirements, the City has a legislated duty as a data steward to protect information and staff must ensure that all personal information, regardless of who 'owns' this data, is secured against unauthorized access, collection, use, disclosure or destruction.

6. Risks of Storing City Information in Foreign Jurisdictions

There is currently no direct legal requirement within the privacy legislation the City is subject to regarding data residency. Issues raised by the Information and Privacy Commissioner of Ontario (IPC) highlight some of the fundamental concerns:

Data security:

The security of data stored or managed by cloud technology is the City's obligation. Ensuring the City meets these mandatory legal obligations is a shared responsibility between the data owners (the City) and cloud technology service providers, which the City may retain to assist in its municipal operations. Cloud technology service providers are responsible for the security of the cloud infrastructure and safeguards and City Divisions are responsible for security to, from, and while being utilized by the cloud technology. The risk of this practical "shared responsibility" is that the City's security standards may be degraded.

Threats to data security include insider threats, e.g., cloud architects, administrative staff, subcontractors, and other service providers have the ability to access information without detection or an audit trail; non-segregation of data, "multi-tenancy", e.g., the City may share storage, memory and routing with unrelated organizations; and threats to data retention in cloud solutions, as required by the City's records retention schedules.

Data control and access:

Cloud technology service providers can deploy their technology assets on a global scale. Although cloud technology service providers may have the ability to move a client's data anywhere in the world, as a practical necessity, the City must have the

option to isolate City information to specific jurisdictions prior to the City information being placed in a given geographical region. Control over the location in which City information is located is an important feature because it allows the City to keep data under the laws and policies of a particular jurisdiction(s). Moving data outside of Canada, whether at rest, in-transit, or both, could impact access to the data itself and to user administration, customer support, or other services that are necessary for business continuity.

Cloud technology may generate new types of information, e.g., metadata or joined aggregated data, which may become available to cloud technology service providers, subcontractors, or other third parties. In theory, cloud technology service providers, subcontractors, or other third parties may use these data for unintended or unauthorized purposes, e.g., profiling and marketing. Cloud technology service providers may inappropriately access, manipulate or mine City information stored on the cloud solution for purposes not specified in their contracts. This will result in the City being in conflict with the City's minimum legislative obligations.

Any use of City information for any purpose not specified in the contractual obligations to the City will result in the City not being in compliance with its mandatory basic legal obligations for all City information. Any contractual arrangements with Cloud technology service providers must have sufficient controls to adequately mitigate against these risks.

Data sovereignty and autonomy:

If City information is stored, in transit or in use, outside of Canada, the City may not be able to apply Canadian laws and regulations that protect it from being improperly used. City information may be subject to the laws of the countries in which they are stored, or in transit to and from, including being subject to warrants, court orders or subpoenas from foreign law enforcement agencies. This means sensitive, personal or personal health information could be disclosed to other governments and agencies, which may occur without the knowledge of the City. This may have unforeseen impact on an individual if information is used by a foreign agency or government for purposes not authorized and not intended by the City. Data residency requirements and proper encryption of personal and personal health information helps ensure that the public’s information remains secure and subject to Canadian privacy and information protection regulations, and that Canadian regulations will govern any disputes with cloud technology service providers.

City information held in a cloud technology service provider’s data centre must be under such operational controls, established by contract so that the City will always maintain full control of the City information across the life-cycle spectrum of the technology and digital infrastructure, e.g., product interface, management, access, and ownership of City information. The City may never adopt cloud technology where by its adoption the City will not be able to comply with its statutory obligations to provide individuals with access to their data and to have full and complete control over their personal information, e.g., requesting address or name changes or deletion of data.

7. Implementing Data Residency Guidelines for Cloud Technology

Guidelines for Procurement and Contracts:

- All project teams acquiring, replacing, upgrading, or renewing cloud technology, must undertake a Cloud Architecture Review Board (CARB) Concept and Feasibility Study.
    - The Division Head/Sponsor is accountable for a Cloud Concept/Cloud Feasibility Study. The Customer Relationship Manager (CRM) is responsible for facilitating its development by the business (budget) owner, including liaising with the Cloud Technology Services Broker (Manager Cloud & Internet Services), Enterprise Architecture (EA), Finance & Contract Management (FCM), CIMS, and OC.
- Through the CARB process, Divisions work with CIMS to complete an IM Assessment. This process identifies those areas of Information Management, Privacy and Access to be built, by-design, ensuring cloud data residency and Information Management requirements are accounted for in technology design and procurement documentation.
- Through the CARB process, the OC (CISO@toronto.ca) must be consulted for guidance relating to security requirements and whether a Privacy Impact Assessment is required for the new cloud technology.
- Following the CARB process, TSD must be consulted when procuring out of the box or custom cloud technology. This includes completing and submitted a Technology Authorization Procurement Plan (ITAPP).
- Project teams should consider data residency guidelines and requirements when looking at feature availability and vendor credibility. Leading cloud technology service providers subject their services and processes to multiple third-party audits and meet numerous internationally recognized industry certifications, such as ISO 27001, to provide assurance to their clients. They also have significant budgets to maintain, patch and secure their cloud infrastructure.
- City Divisions should employ a Security and Privacy by Design approach when procuring cloud technology. This means data protection, residency and privacy should be built into the technology RFP, procurement, design, and integrated in the technology when it is created.
- When creating an RFP or reviewing cloud technology, either CSA CSTAR, ISO 27001 or SOC 2/3 certification is recommended for all cloud technology service providers, regardless of size. In the absence of compliance to CSA CSTAR, ISO 27001 or SOC 2/3, sufficient security controls can be specified individually in a procurement document, such as an RFQ, RFP, purchasing agreement or contract, on the advice of CIMS and the OC.
- Use of standard contractual clauses when procuring a cloud technology mitigates risks associated with cloud technology services. CIMS, TSD, OC, Legal Services, and PMMD can assist in identifying the appropriate standard contractual clauses to include. Contracts, including an RFP, RFQ, Schedule B, Service Level Agreement, and non-competitive procurement and cooperative purchasing processes should have provisions that address:

        - Governing law and jurisdiction
        - Limits on information collection, use and disclosure
        - Treatment of confidential information (including personal information or personal health information)
        - Information retention and destruction
        - Information ownership
        - Data processing (including duration of processing, nature and purpose, obligations and rights, sub-processing, etc.)
        - Security management (including encryption, logging and auditing)
        - The availability of audit results
        - Breach incident response, management and notification
        - Enforceable remedies for non-compliance
        - Limits on the jurisdictions in which the information may be stored
        - Limits on subcontracting
        - Periodic risk assessments such as vulnerability assessments, etc.
        - Cyber liability insurance
        - Employee awareness and training
    - Clauses detailing ownership, stewardship and access to City information ensure City information and data remain in the legal custody of the City and those with access to City information and data are limited, including subcontractors of the cloud technology service provider and cloud technology service providers providing remote customer support functionality.
    - Clauses that compel the cloud technology service provider to notify and disclose of all unauthorized access to City information, including breaches or access made under court order, where applicable, within a specified timeframe, and unless the provider is prohibited from doing so by law. As part of cloud technology procurement, the City may request that cloud technology service providers provide their procedures for navigating the conflict between their contractual obligations and applicable laws.
    - Clauses detailing precise information and records management requirements ensure the cloud technology service provider is able to retain, requisition, return, and destroy City information based on City Information Management policies, guidelines, and standards.
    - Cloud technology service providers must be given express contractual consent from the City to conduct any analytics on City information with an applied protection category. This applies to any use or analysis of the City information beyond the stated purpose of the provisioned software or service.

Guidelines for Applying Legislative Requirements:

1. Legislative requirements specific to the City of Toronto, including COTA, MFIPPA and PHIPA, must be reviewed and complied with. In cases where this guideline conflicts with legislation, the legislation must take precedence.
2. City Divisions should employ a Security and Privacy by Design approach when applying applicable legislation to requirements gathering and the procurement process. Security and Privacy by Design is the view that security and privacy cannot be assured solely by compliance with regulatory frameworks, they must be

embedded in the design of cloud technology and supporting RFPs, contracts, and SLAs.

3. Corporate Information Management Services (CIMS) (cisp-consults@toronto.ca) may be consulted prior to planning the procurement cloud technology, to ensure privacy, access, and information management legislative requirements are considered as early as possible, are understood, and met.
4. Cloud technology that creates, stores, or transmits personal information must abide by MFIPPA requirements, including requirements concerning collection, use, disclosure, right of access, and ability to correct or file statements of disagreement (consult the CIMS' Information Collection unit – forms@toronto.ca).
    - MFIPPA provides individuals with a unique right of access to their personal information held in City information, in rights to file corrections and statement of disagreement. Any cloud technology must be compatible with the City's obligations to this.
5. Cloud technology that creates, stores, or transmits personal health information, in relation HIC operations, must abide by PHIPA obligations for collection, use, disclosure, etc. (consult the City's Information Collection unit – forms@toronto.ca).

Guidelines for Applying City Policy Requirements:

1. All cloud technology projects must review TSDs Cloud Computing Framework and complete the cloud architecture review process.
2. All data and information assets created in, migrated to, or more generally, stored in the cloud should be classified as per the Information Protection Classification Standard before migration or creation on the cloud. Divisions can work with CIMS to ensure their information assets are classified and the risk level is understood.
3. Cloud technology procurement and design must align with the TSD IT Cloud Strategy.
4. Security controls implemented for data and information assets created in, migrated to, or more generally, stored in the cloud must meet or exceed security controls set out by the City's Office of the Chief Information Security Officer (OC)
5. Any cloud technology procurement activity resulting in the migration of personal, personal health, or sensitive information must consult the OC to determine if Security Testing and Risk Assessments, e.g., Privacy Impact Assessment (PIA) or Threat Risk Assessment (TRA), is required prior to migration to the cloud.
6. Divisions planning to procure or use cloud technology that collects personal or personal health information, a mix of personal information and business, professional, or public office information should consult with CIMS' Information Collection Unit (forms@toronto.ca) for advice on compliance requirements.
7. City information created in, migrated to, or more generally, stored in the cloud must be encrypted while at rest, in-transit, and while processing in cloud environment(s).
8. The most secure and appropriate security controls should be used in accordance with the assigned information protection classification categories, outlined in the Information Protection Classification Standard.
    - City information classified as Public can be stored in cloud technology without particular additional restrictions; however there may be security requirements that must be considered before implementation, addressed through mechanisms such as a TRA.

- Limit the cloud storage of City information with high risk protection classification categories applied to it
- Canadian servers should be selected, where possible, for any City information stored utilizing cloud technology

9. The City must always maintain administrative access to and control of City information. In order to ensure adequate controls regarding access to City assets, cloud technology services for vital records or data must be designed to ensure that the City effectively controls the provisioning and revocation of credentials used to access the service.

8. Compliance

Consequences of non-compliance with legislative or policy requirements include potentially exposing Torontonians to harm, damage to the City of Toronto's trust, credibility, and reputation, financial impacts, and other liabilities that may occur as a result.

Any exception to this guideline must be documented and reviewed by CIMS, TSD, and the OC through the cloud architecture review process, and any resulting risks identified, must be assessed, documented, and accepted by Division Heads and their Divisional Legal Representatives. This may include the development of risk or incident management plans.

9. References

The following sources were used in the development of this Guideline:

1. City of Toronto, Technology Services Division (2019): Choosing the Right Cloud Guideline
2. Province of Ontario (2006): City of Toronto Act
3. City of Toronto, Office of the Chief Information Security Officer (2021): Cloud Security Policy
4. City of Toronto, Technology Services Division (2022): Digital Infrastructure Strategic Framework
5. Government of Canada (2018): Government of Canada White Paper - Data Sovereignty and Public Cloud
6. Information and Privacy Commissioner of Ontario (2011): IPC Privacy by Design – Foundational Principles
7. Information and Privacy Commissioner of Ontario (2012): IPC Privacy Investigation Report PC 12-39
8. Information and Privacy Commissioner of Ontario (2016): IPC Thinking About Clouds
9. City of Toronto, City Clerk's Office (2023): Information Management Accountability Policy
10. City of Toronto, City Clerk's Office (2023): Information Protection Classification Standard (CIMS)
11. Province of Ontario (1990): Municipal Freedom of Information and Protection of Privacy Act, 1990
12. Province of Ontario (2004): Personal Health Information Protection Act, 2004
13. Province of Alberta (2023): Service Alberta – Data and Information Security in the Cloud

Contact

For further assistance please contact:

Robert Ambra (Robert.Ambra@toronto.ca)
Manager, Policy and Standards
Corporate Information Management Services, City Clerk's Office

Appendix A: Definitions

Application/Software: A computer program designed to help end users perform activities or tasks.

Cloud: A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction

> **Public Cloud Model:** Cloud resources (that is, hardware, software and infrastructure) are owned and operated by a third-party cloud service provider (CSP). Organizations consume IT services over the Internet from a shared pool of resources that are logically separated from one another.
>
> **Private Cloud Model:** A vendor hosts IT resources exclusively for a client.
>
> **Hybrid Cloud Model:** A combination of unique but connected private and public cloud models (i.e., part of the cloud technology can reside in a private model and part in a public model).

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.

Data at Rest: Electronic Information which is stored physically in any electronic form (e.g., databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

Data Centre: A physical room, building or facility that houses IT infrastructure for building, running, and delivering applications and services, and for storing and managing the data associated with those applications and services.

Data centers have evolved from privately-owned, tightly-controlled on-premises facilities housing traditional IT infrastructure for the exclusive use of one company, to remote facilities or networks of facilities owned by cloud technology service providers housing virtualized IT infrastructure for the shared use of multiple companies and customers.

Data in Transit: Electronic Information that is transmitted over public or untrusted networks such as the internet and data which flows in the confines of a private network such as a corporate or enterprise Local Area Network (LAN).

Data Residency: The physical or geographical location of an organization's digital information while at rest.

Data Sovereignty: In relation to Canada, "data sovereignty" is Canada's right to control access to and disclosure of its digital information subject only to Canadian laws.

Data Steward: A business leader and/or subject matter expert designated as accountable for:

1. The identification of operational and business intelligence data requirements within an assigned subject area

2. The quality of data names, business definitions, data integrity rules, and domain values within an assigned subject area

3. Compliance with regulatory requirements and conformance to internal data policies and data standards

4. Application of appropriate security controls

5. Analyzing and improving data quality

6. Identifying and resolving data related issues. Data stewards are often categorized as executive data stewards, business data stewards, or coordinating data stewards.

Digital Infrastructure: All technology assets that create, exchange or use data or information in a digital form as a part of their operation, as well as all data collected or used by the aforementioned technology assets. Examples of Digital Infrastructure include:

- Physical objects and structures such as cameras, sensors, and broadband networks
- Software systems such as mobile applications, websites, digital payment systems, customer relationship management applications, and legacy technology systems
- Fixed devices such as computers and digital kiosks
- Mobile devices such as robots, vehicles and cellphones
- Data collected or stored digitally by the City, including personally identifiable information and non-personal information (administrative data, geospatial data etc.)
- Systems whose functions may rely on computer generated data such as machine learning systems and artificial intelligence

Digital Infrastructure Initiatives: The use of Digital Infrastructure in City operations, including the provision of services to the public, the procurement of Digital Infrastructure by the City, or regulations of the City which address Digital Infrastructure.

Disposition: The actions taken with regard to inactive City records as determined by an appraisal pursuant to legislation, regulation, or administrative procedure. Actions include destruction, or designation as archival records, or as permanent records.

Information: Data that has been given value through assessment, interpretation, or compilation in a meaningful form.

Migration: The process of moving information from one system to another.

Personal Health Information: Identifying information about an individual in oral or recorded form, if the information is both: 1. in the custody or control of a City Staff member, who as a result, or in connection, of this Staff member performing their workplace responsibilities to the City in relation to any of the following tasks: {(a)acting as a health care practitioner; a health service provider; placement co-ordinator; medical officer of health; or, (b)operating in whole or in part, a hospital; psychiatric facility; independent health facility/community health facility; community health/mental health centre, program, or service; long-term care home; care home; home for special care; retirement home; pharmacy; laboratory/specimen collection centre; or ambulance service}; and; 2. the information: (a) relates to the individual's physical, or mental health; providing health care to the individual; health care payments; health care eligibility;

eligibility for health care coverage; (including the identity of the individual's health care provider; the identity of the individual's substitute decision-maker; health history of the individual's family; and health number); or, (b) is a plan setting out the home and community care services a health service provider would provide to the individual.

Personal Information: Recorded information about an identifiable individual, such as (but not limited to): address, race, religion, gender, family status, employment history, medical history, blood type, DNA, any identifying number assigned to the individual, personal opinions or views of an individual about another individual, correspondence of a personal or confidential nature from an individual. For more information, refer to the personal information interpretation under MFIPPA, S.2.

Privacy by Design: To build privacy and data protection, into the design specifications and architecture of information and communication systems and technologies at the beginning, in order to facilitate compliance with privacy and data protection principles.

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.

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

Vital Records: Records that are essential to the City's functions and ongoing business operations and that are impossible and/or expensive to replace, such as accounts receivable records. Vital records are irreplaceable because they give evidence of the City's legal status, financial status, and/or basic operations.