UNIVERSITY OF TORONTO | Information Security

Office of the Chief Information Security Officer

Third-party data location guidelines

Guideline on third-party data location

Purpose and intent

This guideline provides insights and actionable, risk-based guidance for managing the university's data location concerns when using third-party services.

Data location (i.e., the physical geographic location of data stored on servers, databases or data centres) is increasingly important due to global privacy regulations and access laws. Data stored or processed in third-party systems — regardless of physical location — carries inherent risks of unauthorized access by foreign or malicious actors.

Third-party services (platforms not owned, operated or developed by the university — e.g., cloud storage or external software) are subject to this scrutiny.

Rather than treating this as a stand-alone risk, the university integrates it into a broader strategy for managing unauthorized access. This includes due diligence in vendor selection, robust contractual protections, strong security and privacy controls and alignment with institutional data governance practices.

The intent of this guideline is to:

- Clarify the university's position on data location and its associated risks.
- Provide a structured approach for staff, librarians and faculty to evaluate and mitigate risks related to data access and jurisdictional exposure.
- Support data trustees (individuals responsible for overseeing access to and protection of institutional data — see definition in the Data Management Guideline) and decision-makers in selecting and managing third-party services based on data sensitivity and geopolitical context.
- Reinforce the importance of using institutional tools and practices that uphold the university's standards for data protection, privacy and regulatory compliance, rather than unapproved personal or third-party tools.

This is an interim guideline while a more comprehensive guideline is being developed on managing the security and privacy risks of third-party tools and systems.

Scope and applicability

This guideline applies to all academic and administrative units, third-party agents of the university and any other university affiliate that is authorized to access institutional or research data, services or systems.

Beyond awareness, this guideline empowers stakeholders to make informed decisions that balance operational needs with the imperative to safeguard institutional data, while ensuring alignment with legal, ethical and institutional responsibilities.

This guideline is written in accordance with the university's Information Security Control Standard and the Policy on Information Security and the Protection of Digital Assets.

Understanding the context

The information technology world, including higher education, has long moved past solely relying on "on-premise" systems (infrastructure hosted and managed by the university on its own property) to enable institutional missions.

This has led to a rise in concerns related to third-party service provider privacy and security practices, specifically when third-party technology services used by universities are either hosted or owned by companies located outside of Canada. Such services may be subject to foreign laws requiring the service provider to share university data with foreign governments with or without the university's knowledge or consent.

This creates potential risks of losing control over sensitive information like student records, research data and internal communications, especially when the hosting country has different privacy laws or data access requirements than Ontario or Canada.

While the above examples reference international contexts, risks may also exist when data is stored in other provinces within Canada that have different legal or privacy frameworks.

When using third-party technology services, access by foreign governments is just one of many security and privacy risks that need to be considered. Additionally, this risk needs to be measured in the context of broader trade-offs involving cost, performance and access to best-in-class technological solutions.

The risk stemming from sharing data with third-party service providers is managed like any other information security risk. It is addressed through careful selection of third-party providers, binding contractual terms, enhanced business processes, strong data management practices and appropriate use of security and privacy controls, rather than treating data location as a separate category of risk.

Risk assessment

The first step in evaluating the actual risk of unauthorized access to data, because of using third party service providers, is analyzing both the likelihood of such access and the potential impact.

Institutional offices such as Information Security, the Freedom of Information and Protection of Privacy (FIPP) Office, and Research Security have subject matter experts who perform and guide

these risk assessments. Staff or units considering a new tool or third-party service should contact these offices to initiate a risk assessment.

The institutional Information Security team offers information security risk assessments as a service.

Key considerations for risk assessments include:

1. **Geopolitical context:** Understand the legal and political environment of the third-party's jurisdiction. Compare local privacy laws to Canadian standards and assess how they are stronger, weaker or equivalent.
2. **Contractual protections:** Review the third party's privacy and security commitments, history of compliance and organizational maturity. Consider their track record with privacy and security incidents and the strength of their legal and compliance teams.
3. **Security posture:** Examine the third party's technical safeguards, known vulnerabilities, and history of security breaches. Review their security documentation and certifications.
4. **Data sensitivity:** Classify the data based on its type, volume, level of classification and potential value to foreign entities. Consider the consequences of unauthorized access or disclosure.

Actions to address risk

There are many examples of university enterprise solutions designed with security standards and data protection as foundational principles. Whenever possible, use existing enterprise solutions (centrally supported tools that have been reviewed for security and privacy standards). These solutions have undergone privacy and security risk assessments that evaluate both vendor-provided controls and internal processes to identify and mitigate potential risks. They are also governed by standardized contractual agreements that include enhanced provisions for data privacy, security and data location, helping ensure alignment with institutional policies and regulatory requirements.

It is essential to apply appropriate security safeguards to any tool or service adopted. Institutional Information Security and divisional IT teams should be consulted for guidance on the adoption of these safeguards.

Foundational security measures include:

- **Contractual protections:** Include the university's standard contractual protections, ensuring the vendor will require disclosure of any unauthorized access to data, including access under court orders (except where prohibited by law). It is also important to assess new or evolving risks as agreements are renewed, even with long-standing partners.
- **Third-party risk management:** Before entering a contract, conduct a third-party risk assessment and privacy impact assessment (as applicable), ensuring the third party meets security, privacy and compliance requirements. Conduct regular third-party reviews to monitor risks throughout the engagement period and as the environment changes.

- **Gap mitigation:** Address identified security and privacy gaps with clear mitigation plans. Any unaddressed risks should be formally accepted by the appropriate authority, typically the data trustee. Review accepted risks at least annually to determine whether they should continue to be accepted.
- **Data location strategy:** Choose the most appropriate option for data storage and processing based on the risk involved: on-site hosting, cloud services or use of sovereign cloud services, if applicable. Where foreign government access is a significant concern, prioritize on-site or sovereign cloud options.
- **Encryption:** When appropriate and based on the data sensitivity, use encryption with exclusive control of decryption keys.

Ultimately, the course of action will depend on the decision made by the data trustee, based on a comprehensive risk assessment that includes privacy and security. The Office of the Chief Information Security Officer (CISO) is available to support this process and may intervene if the risks span multiple units or have broader implications beyond the authority of a single data trustee.

Resources

- Policy on Information Security and the Protection of Digital Assets
- Information Security Control Standard - Information Security at University of Toronto
- Data Management Guideline (defines the data trustee role and related responsibilities)