Cloud Directive

Issued by: Chief Information Officer & Director and Contract Rules Compliance Monitor, Procurement Services
Revision date: February 18, 2022
Effective date: March 30, 2015

Preamble:

This directive applies to all members of the McGill University community that acquire or use Cloud Services for Enterprise Data or Research Data.

The objectives of this directive are to:

- Ensure that Personal Information, personal health information, proprietary information and intellectual property (IP) are protected;
- Ensure that McGill University complies with applicable laws (e.g., Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information), regulations and standards (e.g., Payment Card Industry Data Security Standard);
- Complement and support other McGill policies, directives, procedures and standards, namely, but not limited to the following:
  - Procurement Policy,
  - Policy on the Approval of Contracts and Designation of Signing Authority,
  - Policy on Enterprise Data Governance,
  - Standard on Enterprise Data Governance,
  - Standard on Enterprise Data Classification,
  - Policy on the Responsible Use of McGill Information Technology Resources,
  - Secure Use of McGill Administrative Systems Directive, and
  - Regulation on the Conduct of Research.

1. Terms and Definitions:

   For the purposes of this directive, the following words and expressions have the respective meanings described below. Any capitalized word and expression not otherwise defined in this Policy has the meaning described in the Policy on the Responsible Use of McGill Information Technology Resources.

   1.1. "**Authorized User**", as defined in the Policy on the Responsible Use of McGill Information Technology Resources.
   1.2. "**Cloud**" means the Internet.
   1.3. "**Cloud Service**" means services delivered on demand over the Internet. These services provide access to applications and resources, without the need for internal infrastructure or hardware.
   1.4. "**Cloud Services for Enterprise Data**" means resources or services provisioned in the Cloud that have been approved by McGill for a specific Data Classification, and where the Cloud Service has been assessed by Procurement Services and IT Services, in conjunction with Legal Services where required.
   1.5. "**Cloud Services for External Public Data"** includes Public Enterprise Data and Public Research Data.
   1.6. "**Cloud Services for Research Data"** means resources or services provisioned in the Cloud directly by Researchers for the purpose of conducting research. For the purpose of clarity, this does not include administrative activities to support research.
   1.7. "**Confidential Data**", as defined in the Policy on the Responsible Use of McGill Information Technology Resources. This includes **Regulated Enterprise Data**, **Protected Enterprise Data**, **Regulated Research Data,** and **Protected Research Data.**
   1.8. "**Data Classification**", means the following 3 classes of data: regulated, protected or public.
   1.9. "**Data Trustee**", as defined in the Policy on Enterprise Data Governance. Researchers are by default Data Trustees for their Research Data, unless otherwise determined by a Data Trustee designated by the Policy.
   1.10. "**Enterprise Data**", as defined in the Standard on Enterprise Data Classification.
   1.11. "**Institutionally Owned/Managed Device**", as defined in the Secure Use of McGill Administrative Systems Directive.
   1.12. "**IT Credentials**", as defined in the Policy on the Responsible Use of McGill Information Technology Resources.
   1.13. "**IT Services**", as defined in the Policy on the Responsible Use of McGill Information Technology Resources.
   1.14. "**McGill IT Resources**", as defined in the Policy on the Responsible Use of McGill Information Technology Resources.

1.15. "**PCI**" means the Payment Card Industry. It consists of all merchant organizations, which store, process and transmit payment cardholder data (e.g., credit cards).
1.16. "**Personal Information**", as defined in the Policy on the Responsible Use of McGill Information Technology Resources (e.g., any element from student records, employee records, patient records, donor information, and personal health information).
1.17. "**PHI**" means personal information that relates to the health of a person (e.g., medical, and pharmaceutical records).
1.18. "**Protected Enterprise Data**", as defined in the Standard on Enterprise Data Classification.
1.19. "**Protected Research Data**" means Research Data whose protection and use are governed by contract, or any McGill regulation, policy or directive because of its confidential nature.
1.20. "**Public Enterprise Data**", as defined in the Standard on Enterprise Data Classification.
1.21. "**Public Research Data**" means Research Data that is deemed accessible to the public and is not confidential.
1.22. "**Regulated Enterprise Data**", as defined in the Standard on Enterprise Data Classification (e.g., Personal Information, PHI, and payment card data).
1.23. **"Regulated Research Data"** means Research Data whose protection and use are mandated by law, regulation (e.g., Personal Information, PHI).
1.24. "**Research Data**", as defined in the Policy on Enterprise Data Governance. For the purpose of this directive, Research Data specifically excludes PCI data.
1.25. **"Researcher",** as defined in the Regulation on the Conduct of Research.

2. Principles:

2.1. Data can have varying degrees of sensitivity, and thus varying levels of security and data protection must be put in place accordingly. Some data may be stored in the Cloud, but not shared or synced to some devices.
2.2. Although some Personal Information is always considered sensitive (e.g. medical and salary information), any Personal Information can be considered of higher sensitivity depending on the context. The degree of protection required by the Cloud Service is determined based upon the applicable regulation, the sensitivity of the Personal Information, the purposes for which it is to be used, its quantity and distribution and the medium on which it is stored.
2.3. Not all Cloud Services and Cloud Service providers are equally diligent about cyber security and privacy management practices. Due diligence and a risk assessment are required if **Confidential Data** is involved. Significant security and privacy risks are associated with consumer-level services.
2.4. Privacy laws applicable in Quebec place obligations on McGill University and on McGill University's Cloud Service providers, which are very distinct from the obligations placed on individuals and even private companies. All contracts where Personal Information may be hosted or accessed by a Cloud service provider and their subcontractors must comply with the contract requirements set in Quebec privacy laws for public bodies.
2.5. University policies require the retention of information for operational and regulatory compliance needs. One such obligation is the duty to know what data is stored where and how it is preserved (e.g., backups). Not all Cloud Services provide adequate backups and as such, are not suitable to host single master copies of Enterprise Data and Research Data.
2.6. Usage of **Confidential Data** must respect security principles, namely, but not limited to:
2.6.1. Principle of "Least privilege", i.e. sharing on a need to have basis, granting only the minimum privileges required to perform the task and for the duration of such task. Only share **Confidential Data** with other Authorized Users with a legitimate need to have access for the role and their level of responsibility. The Confidentiality of the Data accessed shall be preserved and the Data shall be used solely for the purposes for which access was intended.
2.7. Authorized Users must comply with the Confidentiality obligations of the Policy on the Responsible Use of McGill Information Technology Resources.
2.8. Authorized Users are responsible for their determination of the Data Classification to which their data belongs and for the consequences of an incorrect determination by them. When in doubt, Authorized Users must defer and comply with the advice of IT Services, Procurement Services and Legal Services in determining the Data Classification to which their data belongs.
2.9. Storage of IT Credentials is a specific case of data storage, as it provides access to other data that may fall under another data classification including regulated. The level of protection required of IT Credentials shall correspond to the level of protection required by the Data Classification to which the credential provides access. Notwithstanding the above, IT Credentials that provide access to the **Regulated Enterprise Data** and **Regulated Research Data** must not be stored in the Cloud unless the solution has been assessed by IT Services, in consultation with Legal Services where required.

3. Acquiring Cloud Services: (i.e., service accounts, contracts)

3.1. Prior to acquisition, written approval is required from Data Trustees, on the appropriateness of using the Cloud, to store, process, or transmit **Confidential Data.**

3.2. If you acquire a Cloud Service to store, process or handle data (regardless if the solution is free), then the provider becomes a supplier of the university. If the service provider handles Personal Information, the service provider needs to incorporate the most recent version of McGill's Privacy Addendum in the contract.

3.3. **Cloud Services for Enterprise Data** are assessed and approved jointly for use by Procurement Services and IT Services, in conjunction with Legal Services where required, in accordance with the Cloud Service acquisition process. Such approval includes proper due diligence, including the completion of a privacy assessment, IT assessment by IT Services with the implementation of safeguards, and a contract assessment. The approval assumes on-going monitoring by the responsible unit and observance by Authorized Users of the safeguards put in place.

3.4. **Cloud Services for Research Data** are assessed by the Researcher for use, in conformity with McGill's Research Ethics Board. The Cloud Services provider must be selected in accordance with the Procurement Policy and the contract must be signed and reviewed in accordance with the Policy on the Approval of Contracts and Designation of Signing Authority. **Cloud Services for Research Data** can only host or access Research Data. Researchers must ensure proper due diligence, including the completion of a risk assessment and the implementation of safeguards. Evidence of proper due diligence by the Researcher must be kept for the duration of the contract with the Cloud Services provider and for three years thereafter. Authorized Users shall consult the Chief Information Officer or delegate for guidance on due diligence.

Table 1. Who is responsible to perform due diligence in the Cloud Services Acquisition Process

Data	Due Diligence Assessment[1]	
	Privacy Assessment	IT & Contract Assessment
Cloud Services for Enterprise Data	Procurement, Legal & IT Services	
Cloud Services for Research Data	Research Ethics Board[2]	Researcher
Cloud Services for External Public Data	Due diligence not required	

[1] *Solution assessment requires due diligence by performing a privacy assessment, IT assessment & contract assessment.*

[2] *Research Ethics Board (REB), Research Ethics and Compliance (IRB)*

3.5. IT Services will support requesters in the Cloud Service acquisition process upon request.

3.6. **Confidential Data** must always undergo the Cloud Service acquisition process.

3.7. If a supplier providing services to McGill University uses a Cloud Service as part of its operations, the provider of this Cloud Service becomes a sub-contractor to the supplier. The use of sub-contractors must be addressed in the supplier's contract (including legal compliance, cyber security requirements, allocation of liability, responsibility, and costs relating to actions of sub-contractors or their products).

3.8. The use of a McGill University purchase order is mandatory for the acquisition of Cloud Services. In particular, payment by Pcard or personal credit card (and subsequently reimbursed by McGill University) is not allowed, unless written approval is received from Procurement Services.

4. Using Cloud Services:

4.1. When **Regulated Enterprise Data** or **Protected Enterprise Data** is stored in a Cloud Service, it can synchronize only to Institutionally Owned/Managed Devices (e.g., mobiles, laptops and desktops) if the communication channel is encrypted and the Institutionally Owned/Managed Device is protected by password or other IT Credential. If the synchronization application does not store a local copy onto your device but only provides access to data while connected, then this restriction (Institutionally Owned/Managed Device) does not apply as long as the communication channel is encrypted and the device is protected by password or other IT Credential.

4.2. You are responsible to use Cloud Services only in a manner and for the use it was intended and approved. Procurement Services must describe in writing the approved use of all **Cloud Services for Enterprise Data**. It is your responsibility to consult with IT Services and Procurement Services in case you wish to change the use of such Cloud Service. If you circumvent the safeguards and monitoring capabilities put in place by, or at the request of IT Services, or knowingly allow such circumvention to occur your responsible unit and yourself, as an individual, are accountable and responsible for any resulting data breaches and security incidents related to this data.

4.3. Even if permitted under this directive to store **Regulated Enterprise Data** or **Protected Enterprise Data** in a specific Cloud Service, a valid business need, in line with the scope presented and approved by Data Trustees, is required to share data

(e.g., Human Resources data) internally or externally, therefore controlling the number of systems hosting sensitive data to limit cybersecurity exposure.

5. Enforcement / Compliance:

5.1. Any data that may have been previously hosted in Cloud Services that violate this directive needs to be relocated promptly to a service that is compliant with this directive and/or use of the non-compliant service shall be discontinued. The responsible unit must ensure that data on the non-compliant Cloud Services has been deleted once the relocation is completed.

5.2. Any violation of the provisions of this directive may lead to a disciplinary offence and, where appropriate, shall be dealt with under the regulations, policies, code, or collective agreement to which the Authorized User is subject.

5.3. If you acquire or use a Cloud Service and bypass the Cloud Service acquisition process, your responsible unit and yourself, as an individual, are accountable and responsible for any resulting data breaches and security incidents related to this data. In certain cases, this includes fines, financial responsibility for data breach notification, and any other steps to remediate damages. The responsible unit and yourself, as an individual, are also subject to the discontinuance of such Cloud Service and held accountable and responsible for all related costs in addition to the costs of migrating the Data to a McGill compliant Cloud Service.

5.4. Any individual who has reasonable cause to believe that there has been a breach of this directive shall report the matter to the Office of the Chief information Officer (CIO). Anonymous reporting, such as per the Policy on the Disclosure of Wrongdoing, is accepted but you are reminded that sufficient details need to be provided to allow the proper investigation of the matter at issue while minimizing any disruption caused by such investigation.

5.5. If data falls within more than one of the Data Classification, the level of protection required of such data shall be the one that corresponds to the higher level of protection.

5.6. IT Services may verify compliance, by Authorized Users and responsible units, with this directive from time to time.

6. Review:

6.1. This is a living document that will be updated as security and privacy risks evolve over time.