Cloud Data Directive

Issued by: Chief Information Officer
Revision date: August 26, 2016
Effective date: March 30, 2015

Preamble:

This directive applies to all members of the McGill University community that acquire or use Cloud services for Institutional Data.

Cloud data storage & file hosting services are internet hosting services designed expressly to host user files and data. They support storing, synchronizing, sharing, and searching of documents. Many service providers provide data storage & file hosting services through an "as-a-service" offering (e.g., "software-as-a-service" or "SaaS", "infrastructure-as-a-service" or "IaaS"). Examples of file hosting services include Box, Dropbox, Google Drive, iCloud, and OneDrive.

The objectives of this directive are to:

- Ensure that Personal Information, personal health information, proprietary information and intellectual property (IP) are protected;
- Ensure that the university complies with applicable laws, regulations (e.g., *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*) and standards (e.g., Payment Card Industry Data Security Standard);
- Complement and support other McGill policies and directives, namely, but not limited to the following:
  - Policy on the Responsible Use of McGill Information Technology Resources,
  - Procurement Policy,
  - McGill University Records Retention Schedule,
  - Enrollment Services Information Security Reminder; and
- Educate the McGill University community about the differences between enterprise and consumer class solutions and how their terms of service and technology affect their suitability for hosting specific types of data.

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**" is a member of the McGill University community who is an employee, student, alumni, appointee or other individual who has been granted permission, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of McGill IT Resources.
   1.2. "**Cloud**" means the Internet.
   1.3. "**Confidential Institutional Data**" means any Regulated Institutional Data or Protected Institutional Data.
   1.4. "**Data Trustee**" means a senior University official or their delegate with management responsibility for a defined subset of Institutional Data. There is one Data Trustee per subset of Institutional Data.
   1.5. "**Enterprise file synchronization and sharing**" (EFSS) means a range of capabilities that enable one to synchronize and share files across multiple devices.
   1.6. "**File Syncing**" (short for "synchronization") means a process whereby changes to an electronic file are automatically replicated to all copies of the file(s) associated with it and vice versa.

1.7. "**Institutional Data**" means any Regulated Institutional Data, Protected Institutional Data or Public Institutional Data.

1.8. "**IT Credential**" means a proof of identity, such as secret passwords, biometrics, X.509, digital certificates, key cards, and USB tokens, which control access to information systems. Many systems at McGill are accessed through the combination of McGill username/password, or McGill ID/Minerva PIN.

1.9. "**IT Services**" means the McGill units that deliver information technology services on campus and report to the Chief Information Officer (CIO).

1.10. "**McGill IT Resources**" means all Data, software, hardware, communications systems, storage systems, networks and devices connected to or making use of the University Network, regardless of who administers them.

1.11. "**McGill-provisioned Cloud Services**" means Cloud services that have been approved by McGill for a specific data category, where a contract was signed, and the Cloud service was deployed and integrated within McGill's IT infrastructure. This contrasts with Self-provisioned Cloud Services. For example, "OneDrive for Business" is a McGill-provisioned Cloud Service (enterprise-level Cloud data storage service) while "OneDrive" is a Self-provisioned Cloud Service (consumer-level file hosting service).

1.12. "**PCI**" means the Payment Card Industry. It consists of all merchant organizations, which store, process and transmit payment cardholder data (e.g., credit cards).

1.13. "**Personal Information**" means information concerning a natural person that allows the person to be identified as provided for in applicable Canadian and Quebec privacy legislation (e.g., student records, human resource records, donor information, personal health information, and certain clinical research data).

1.14. "**PHI**" means personal health information (e.g., medical, and pharmaceutical records).

1.15. "**Protected Institutional Data**" means information whose protection and use is governed by contract, or any McGill regulation, policy or directive because of its confidential nature (e.g., proprietary information, documents critical to the University's operation, and financial records).

1.16. "**Public Institutional Data**" means information that is open to the public and is not confidential.

1.17. "**Regulated Institutional Data**" means information whose protection and use is mandated by law, regulation, or industry requirement (e.g., Personal Information, PHI, and payment card data).

1.18. "**Research Data**" means the recorded information and material, both physical and electronic, commonly accepted in the relevant scholarly community as necessary to validate research findings including, but not limited to, research proposals, laboratory records, progress reports, internal reports, and presentations and includes all information or records of any sort related to the application for, performance of, data obtained from, conclusions and outcomes reached in the research in question. Research data is considered by the University to be Institutional Data.

1.19. "**Self-provisioned Cloud Services**" means resources or services provisioned in the Cloud directly by end users without the involvement of IT Services. This contrasts with McGill-provisioned Cloud Services. For example, "OneDrive for Business" is a McGill-provisioned Cloud Service (enterprise-level Cloud data storage service) while "OneDrive" is a Self-provisioned Cloud Service (consumer-level file hosting service).

In summary, the following relationships exist between the above-described data categories:

<table>
<tr><td rowspan="2">Institutional Data</td><td rowspan="2">Confidential Institutional Data</td><td>Regulated Institutional Data</td><td rowspan="2">Research Data</td></tr>
<tr><td>Protected Institutional Data</td></tr>
<tr><td></td><td>Non-Confidential Institutional Data</td><td>Public Institutional Data</td></tr>
<tr><td>Non-Institutional Data (non-work data)</td><td colspan="3"></td></tr>
</table>

For additional background information, please refer to:

- "ISO/IEC 17788 - Information technology — Cloud computing — Overview and vocabulary Abbreviations", http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html,

- "The NIST Definition of Cloud Computing - Special Publication 800 – 145", http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf,
- "Cloud Computing Synopsis and Recommendations - Special Publication 800 – 146", http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf,
- "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

2. Principles:

2.1. Not all data is created equal. Varying levels of security, identity and data protection must be put in place based on the degree of sensitivity of the data. 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 to be given in the Cloud is determined by the amount, intended use and access rights (distribution), format (including linkages) and storage method.

2.3. Not all Cloud services and Cloud service providers are created equal. Due diligence and a risk assessment are required if **Regulated Institutional Data** or **Protected Institutional Data** is involved. Significant security and privacy risks are associated with consumer-level file hosting services.

2.4. Privacy laws applicable in Quebec place obligations on Cloud Service providers and on McGill, which are very distinct from the obligations placed on individuals and even private companies. For example, all contracts where Personal Information may be hosted or accessed by a Cloud service provider must comply with minimum standards approved by Legal Services.

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 master copies of Institutional Data. In particular, Documentum is McGill's on-premises enterprise content management platform and is most appropriate to host master copies of Institutional Data.

2.6. Usage of Institutional 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 for the duration of such task. Only share **Regulated Institutional Data** or **Protected Institutional 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 it was accessed.

2.6.2. Principle of "**Segregation of duties**", i.e. the objective identification and evaluation of risks should be performed by a different person than the person ultimately responsible to accept the risk.

2.6.3. Principle of "**Secure state by default**", i.e. default configuration should be safe, e.g. by default files should be private, not public.

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 will be held responsible for their determination of the data category to which their data belongs and for the consequences of an incorrect determination by them. Authorized Users must rely on and comply with the advice of IT Services and Procurement Services in determining the data category to which their data belongs. The first point of contact is IT Services.

2.9. Storage of IT Credentials is a specific case of data storage. Storage of credentials in the Cloud is extremely risky, in particular, if credentials permit access to **Regulated Institutional Data** or **Protected Institutional Data.** The level of protection required of IT Credentials shall correspond to the level of protection required by the data to which the credential provides access. However, if you have access to other people's Personal Information you must not store your IT Credentials in the Cloud.

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

    3.1. If you acquire/use a Cloud service provider to handle **Regulated Institutional Data** (regardless if the solution is free), then the provider becomes a supplier of the university. The service provider needs to sign the most recent version of McGill's Quebec Privacy Addendum available from Procurement Services. Calls for tenders also need to incorporate McGill's Quebec Privacy Addendum.
    3.2. Cloud services intended to store **Regulated Institutional Data** must be assessed by Procurement Services and IT Services, in conjunction with Legal Services where required. The first point of contact is Procurement Services.
    3.3. **McGill-provisioned Cloud Services** are approved jointly by Procurement Services and IT Services for use. Such approval includes proper due diligence, including the completion of a risk assessment by IT Services and the implementation of safeguards. The approval assumes on-going monitoring by the responsible unit and observance by Authorized Users of the safeguards put in place.

    3.4. **Regulated Institutional Data** must not be stored on **Self-Provisioned Cloud Services.**
    3.5. **Protected Institutional Data,** with the exception of Research Data, must not be stored on **Self-Provisioned Cloud Services**. For Research Data, Authorized Users must ensure proper due diligence, including the completion of a risk assessment and the implementation of safeguards. Evidence of proper due diligence must be kept for the duration of the cloud services and three years thereafter. Authorized Users shall consult the CIO for guidance on due diligence.
    3.6. **Public Institutional Data** may be stored on **Self-Provisioned Cloud Services**.
    3.7. If a **vendor providing services to McGill** uses a Cloud service as part of its operations, the Cloud service provider becomes a sub-contractor to the vendor. The use of sub-contractors must be addressed in the vendor's contract (including allocation of liability, responsibility, and costs relating to actions of sub-contractors or their products).

4. Using Cloud services:

    4.1. Prior to initiation, written approval from Data Trustees is required to store, transmit, or process **Regulated Institutional Data** in the Cloud.
    4.2. When **Regulated Institutional Data** or **Protected Institutional Data** is stored in a Cloud service, it can synchronize only to institutionally-owned devices (e.g., mobiles, laptops and desktops) if the communication channel is encrypted and the institutionally-owned 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 devices) does not apply as long as the communication channel is encrypted and the device is protected by password or other IT Credential.
    4.3. If you use any **McGill-provisioned Cloud Services** in a manner that circumvents the safeguards and monitoring capabilities put in place by, or at the request of IT Services, or knowingly allow such circumvention to occur you, as an individual, and your responsible unit, are accountable and responsible for any resulting data breaches and security incidents related to this data.
    4.4. Even if permitted under this policy to store **Regulated Institutional Data** or **Protected Institutional Data** in a specific cloud service, a valid business need is required to share data (e.g., Human Resources data) internally or externally.

5. Specific rules for Pre-approved Cloud services:

Data	**Regulated Institutional Data** Personal Information not otherwise regulated	**Regulated Institutional Data** Personal health information (PHI)	**Regulated Institutional Data** Payment Card data (PCI)	**Regulated Institutional Data** other	**Protected Institutional Data** non-research	**Protected Institutional Data** research	**Public institutional Data**	**Non-Institutional Data**
Self-Provisioned Cloud Services	no	no	no	no	no	yes with due diligence *	yes	yes
McGill-provisioned Cloud Services	depends on contract	depends on contract	depends on contract	depends on contract	depends on contract	depends on contract	yes	yes
Microsoft Office 365 - Exchange - OneDrive for Business - Video - Yammer Enterprise	yes	yes with consent **	no	no	yes	yes	yes	yes
Microsoft Azure	yes	yes with consent **	yes with approval	yes with approval	yes	yes	yes	yes

(*) See paragraph 3.5

(**) See paragraphs 5.1.1 and 5.3.1

5.1. Microsoft Office 365 Exchange, OneDrive for Business, Video, and Yammer Enterprise

5.1.1. **Regulated Institutional Data** solely subject to Canadian and Quebec privacy legislation is allowed to be stored on Office 365. PHI is allowed with user consent provided Legal Services vets the consent form. Other Regulated Institutional Data (e.g., payment card data) is not allowed to be stored on Office 365. Such data, as mandated by other laws, regulations, or industry requirements require stricter security controls. File Syncing is subject to section 4.2. Sharing is subject to section 4.4.

5.1.2. **Protected Institutional Data** is allowed to be stored on Office 365. File Syncing is subject to section 4.2. Sharing is subject to section 4.4.

5.1.3. **Public Institutional Data** is allowed to be stored on Office 365. File Syncing is unrestricted.

5.1.4. **Non-Institutional Data** (non-work data) is allowed. File Syncing is unrestricted.

5.1.5. With the exception of Microsoft Office 365 Exchange, Office 365 is not suitable to host master copies of Institutional Data. Other Office 365 products do not have provisions for the retention of information for operational and regulatory compliance as described in section 2.5. The master copy needs to be hosted on systems with adequate backups or in paper form.

5.2. Microsoft Office 365 Video

5.2.1. You may not use content prohibited by law, regulation, governmental decree or violate the rights of others. In particular, permission needs to be secured for copyrighted materials and consent

obtained from subjects appearing in the video. Consult Communication and External Relations for guidance.

5.3. Microsoft Azure

5.3.1. **Regulated Institutional Data** solely subject to Canadian and Quebec privacy legislation is allowed to be stored on Microsoft Azure. PHI is allowed with user consent provided Legal Services vets the consent form. Payment card data is allowed with prior approval from the PCI Compliance Steering Committee. Other Regulated Institutional Data is allowed with prior approval from data trustees and with proper due diligence.

5.3.2. **Protected Institutional Data** is allowed to be stored on Microsoft Azure.

5.3.3. **Public Institutional Data** is allowed to be stored on Microsoft Azure.

5.3.4. **Non-Institutional Data** (non-work data) is allowed to be stored on Microsoft Azure.

5.3.5. Use of Microsoft Azure does not change anything in your unit's internal information retention procedures (for operational and regulatory compliance as described in section 2.5).

6. Other Cloud services:

6.1. Any data that may have been previously hosted in Cloud services that violate this directive needs to be relocated promptly to a Cloud service that is compliant with this directive, and the responsible unit must ensure that data on the non-compliant Cloud services has been deleted once the relocation is completed.

7. Compliance:

7.1. A violation of the provisions of this directive may constitute 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.

7.2. If you acquire or use a **Self-Provisioned Cloud Service** for storing **Regulated Institutional Data** or **Protected Institutional Data,** you, as an individual, and your responsible unit, are accountable and responsible for any resulting data breaches and security incidents related to this data. In certain cases, this includes financial responsibility for data breach notification, any other steps to remediate damages and conviction of individuals for the specific statutory offence and fines. You, as an individual, and your responsible unit are also subject to the discontinuance of such **Self-Provisioned Cloud Service** and held accountable and responsible for related costs in addition to all costs of migrating the **Regulated Institutional Data** or **Protected Institutional Data** to a McGill compliant Cloud Service.

7.3. 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 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.

7.4. If data falls within more than one of the data categories described above, the level of protection required of such data shall be the one that corresponds to the higher level of protection.

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

8. Reviews:

8.1. This is a living document that will be updated with new McGill-provisioned Cloud services and new requirements as security and privacy risks change over time.