Cloud 101

Contents

Cloud services: Definition .......................................................................................................................... 1
Benefits ............................................................................................................................................... 1
Disadvantages/risks .............................................................................................................................. 1
McGill’s Cloud Directive: what it is, and why we need it................................................................. 2
What is expected from you? ................................................................................................................... 2
Where to go for help............................................................................................................................... 2
McGill Institutional Data types and where they can be hosted ....................................................... 3
Highlights of the Cloud Directive ....................................................................................................... 4

Cloud services: Definition

Instead of running a software application and storing/accessing your data on your desktop or on McGill’s network, this functionality is provided to you remotely as a service (by an external service provider) and accessed over the Internet.

Benefits

With cloud services, we:

- Reduce the cost of maintaining our systems
- Implement software more quickly
- Connect to the University anytime, from anywhere
- Access our data more easily

Disadvantages/risks

- Since our data is no longer kept within the walls of our organization, we don’t have the knowledge or control of who has access to our data without performing due diligence
- Syncing between devices may leave sensitive data on an unsecured device.
- Vulnerabilities of the cloud service to cyber attacks can expose data to unauthorized access.

For more information, see the IT Knowledge Base article Security checklist for using cloud services.
McGill’s Cloud Directive: what it is, and why we need it
McGill’s Cloud Directive governs the use of cloud services at McGill. The purpose of the directive is to protect confidential information stored in the cloud, in compliance with Quebec and Canadian law. McGill Institutional Data types and where they can be hosted for more information.

The Cloud Directive aims to:

• Protect personal information
• Comply with applicable laws and regulations
• Support other University policies and directives
• Raise awareness of the suitability and risks of hosting specific data in the cloud.

McGill’s Cloud Directive: Who should follow it?
This directive applies to all members of the McGill University community that acquire or use Cloud services for Institutional Data. Research Data is subject to the same provisions as Institutional Data.

What is expected from you?
Everyone should make informed decisions when acquiring or using a cloud service.

To be able to do so, you are expected to:

• Ask yourself the right questions in order to understand the implications of your choice - see Checklist of Considerations on the Cloud Service Directive & Guidance page of the ITS website.
• Consult Procurement Services, IT Services, others if needed (see Who to contact on the Cloud Service Directive & Guidance page on the ITS website)
• Follow the cloud acquisition process
• Raise awareness: Explain the process to others and encourage them to do the same.
• Report any suspected breach of the Cloud Directive to the Chief Information Officer (CIO) of McGill.

Remember: As a McGill employee, you as an individual as well as your unit take full accountability for any resulting data breaches and security incidents related to this data (ex. data breach notification).

Where to go for help
See “Who to Contact” on the Cloud Service Directive & Guidance page on the ITS website.

13-June-2019
McGill Institutional Data types and where they can be hosted

<table>
<thead>
<tr>
<th>Cloud Services</th>
<th>Institutional Data</th>
<th>Non-Institutional Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Regulated</td>
<td>Protected</td>
</tr>
<tr>
<td>Self-Provisioned</td>
<td>no</td>
<td>yes, with due diligence</td>
</tr>
<tr>
<td>McGill-provisioned</td>
<td>depends on contract</td>
<td>yes</td>
</tr>
</tbody>
</table>

Definitions of terms

This table contains a subset of the terms defined in the Cloud Directive. See the Cloud Directive for the complete list of terms and definitions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition &amp; examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institutional Data</td>
<td>Any Regulated Institutional Data, Protected Institutional Data or Public Institutional Data.</td>
</tr>
<tr>
<td>McGill-provisioned Cloud Services</td>
<td>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).</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry. It consists of all merchant organizations, which store, process and transmit payment cardholder data. Examples: credit cards, bank cards</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Information concerning a natural person that allows the person to be identified as provided for in applicable Canadian and Quebec privacy legislation. Examples: student records, human resource records, donor information, and personal health information.</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal health information</td>
</tr>
<tr>
<td>Examples: medical, and pharmaceutical records</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Protected Institutional Data</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Information whose protection and use is governed by contract, or any McGill regulation, policy or directive because of its confidential nature.  
Examples: proprietary information, data critical to the University’s operation, and financial data |
| **Public Institutional Data**                  |
| Information that is deemed accessible to the public and is not confidential  
Examples: information publicly accessible via websites, journals |
| **Regulated Institutional Data**               |
| Information whose protection and use is mandated by law, regulation, or industry requirement.  
Examples: Personal Information, PHI, and payment card data, as well as tender bids and their evaluation |
| **Research Data**                              |
| The factual 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.  
Research data include all information or records of any sort related to the application for, performance of, or results obtained from the research in question. |
| **Self-provisioned Cloud Services**            |
| 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). |

**Highlights of the Cloud Directive**

Be aware of the following key points in McGill’s Cloud Directive:

**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.

**2.5.** 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.

**2.8.** 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.

**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.

**3.6.** Only public institutional data may be stored on self-provisioned cloud services – these are free or paid cloud services that McGill community members acquire independently of McGill’s formal acquisition process.

**3.8.** If you acquire/use a Cloud service provider, the use of a McGill purchase order is mandatory. In particular, payment by PCard is not allowed, unless written approval is received from Procurement Services.

**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.

**6.2.** 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.

**6.3.** 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.