Here are the steps you need to follow when procuring a Cloud Service for your faculty, department or unit.

As a Fund Manager, you are responsible for understanding the McGill Cloud Data Directive and ensuring the Cloud Service in your procurement is compliant with requirements to protect personal information and intellectual property.

The following illustrates a typical process for procuring a Cloud Service. Note that the length of the evaluation will depend on what kind of personal information and intellectual property are stored in the Cloud Service.

1. **Fund Manager**
   - Review McGill Cloud Data Directive and available cloud services to identify one that meets your needs and complies with requirements to protect personal information and intellectual property.
   - If none meet your needs, go to the next step.

2. **McGill Procurement Services**
   - Contact McGill Procurement Services to proceed with an assessment of your Cloud Service.
   - Vendors will need to sign Quebec privacy and the educational technology addendums.

3. **IT Assessment**
   - McGill IT Services will evaluate your request with regards to data protection (See Appendix A).
   - Vendors will provide IT assessment information.

4. **IT integrations (if needed)**
   - If your request needs IT integration with central IT solutions, vendors have to provide integration information.

5. **Decision on availability**
   - McGill Procurement Services will inform you when the solution is available.
Appendix A: Highlights of the McGill Cloud Data Directive

Cloud Services

- McGill-provisioned Cloud Service (Azure)
- Self-provisioned Cloud Service

~ selected Cloud Service has been validated 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.

~ cloud provisioned resources or services acquired directly by end users without the involvement of IT Services.

McGill Institutional Data

- Confidential
- Regulated institutional data
  Data protection is mandated by law, regulation, or industry requirement (e.g. personal Information, personal health information, and payment card data)

- Confidential
- Protected institutional data
  Data protection is governed by contract, or any McGill regulation, policy or directive (e.g. proprietary information, documents critical to the University’s operation, and financial records)

- Not confidential
- Public institutional data
  Information that is open to the public and is not confidential (e.g. press release)

Which confidential data can be stored in the Cloud Services?

These 3 charts display a simplified view of which McGill institutional data is allowed or not to be stored on the McGill-provisioned Cloud Service, self-provisioned Cloud Service and Microsoft Office 365 applications.

Microsoft Office 365 (Exchange, OneDrive for Business, Video @ McGill, Yammer Enterprise)

- Yes
  - Regulated inst. data (Personal info not otherwise regulated)
  - Protected inst. data
  - Public inst. data
- Yes with consent
  - Regulated inst. data (Personal health information)
- No
  - Regulated inst. data (Payment card data, other)

Self-provisioned Cloud Service

- Yes
  - Public inst. data
  - Non-research protected inst. data
- Yes with due diligence
  - Research protected inst. data
- No
  - Regulated inst. data

McGill-provisioned Cloud Service (Azure)

- Yes
  - Public inst. data
  - Protected inst. data
- Yes with consent
  - Regulated inst. data (Personal health information)
- Depends on contract
  - Regulated inst. data

Additional information:

- OLC 902: Cloud Computing online video (*KB 6199)
- McGill Cloud Data Directive (*KB 5721)

* KB= IT Knowledge Base found @ kb.mcgill.ca