CLOUD COMPUTING *Best Practices*

at Mount Royal University

MOUNT ROYAL UNIVERSITY 1910

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

General Overview – *Cloud Computing*

Implementing cloud computing services (through a third party vendor) should strive to not only gain efficiencies with technology, but must also make every effort to protect the personal information in the **custody** and/or **control** of Mount Royal University under the FOIP Act.

What is Cloud Computing?

Refers to the delivery of scalable IT resources over the internet as opposed to hosting/operating those resources internally through the organization.

What is Personal Information?

Any recorded information about an identifiable individual.

- Name
- Home address, phone number, or personal e-mail
- Race, color, religion, national or ethnic origin
- Political beliefs or associations
- Age or gender
- Marital or family status
- Identifying numbers
- Fingerprints or blood type
- Health care information
- Opinions about the individual
- Personal financial information

GETTING STARTED

1. Determine what personal information and how much will be retained in the cloud

Before implementing any cloud computing technology generally assume that the personal information stored in the cloud will be stored in a foreign country.

Always limit the risk by questioning how much personal information (if any), and what personal information, absolutely needs to be stored in the cloud to fulfill your operations.

Expect that the more personal information that is disclosed to the vendor will translate into more risk that needs to be mitigated for your department. Assess internal solutions if it is deemed sensitive information such as financial information.

Remember: *Mount Royal University (a public body) may only collect personal information if it has the legal authority to do so under section 33(c) of the Alberta FOIP Act, therefore, the University can only collect personal information if that information relates directly to and is necessary for an operating program or activity of the public body*

2. Determine the vitality of the electronic records being managed

Assess the vitality of the University information that may be stored with another company (possibly in a foreign jurisdiction).

Records that are vital, paramount, or sensitive to daily University operations may not be good candidates for cloud computing services if a break in service occurs.

3. Determine the mechanisms that will obtain the notification/consent necessary from the effected individuals

Be open and transparent with individuals on storing their personal information in the cloud.

According to section **34(2)** of the FOIP Act, a public body **directly** collecting personal information **must** inform individuals the information is about regarding:

(a) The purpose of the collection

(b) The specific legal authority for the collection **[33(c)]**, and

(c) The Title, Business Address, Business Number, Business E-mail of a public body employee who can answer questions about the collection.

The Information and Privacy Commissioner of Alberta also recommends **notifying** individuals that their personal information will be stored in the cloud and whether their information will be stored in another country where a foreign jurisdiction applies.

Additional information on notification/consent is available on **mtroyal.ca/foip/PoliciesGuidelines**

Additional Cloud Computing Resources

Office of the Privacy Commissioner of Canada
Outsourcing of Canada.com e-mail services to US based firm raises question for subscribers **www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp**

Office of the Information and Privacy Commissioner of Alberta
Cloud Computing for Small and Medium Sized Enterprises **www.oipc.ab.ca/Content_Files/Files/Publications/Cloud_for_SME_June_2012.pdf**

What is custody?

Refers to the physical possession of a record by a public body.

What is control?

Refers to the authority of a public body to manage (even partially) what is done with a record.

For example, custody includes the right to demand possession of a record or forbid access to a record.

Cloud computing contracts should address a public body's **custody** over the digital records before being stored with another party.

Who needs to be involved?

Any cloud computing services project must involve:

INFORMATION TECHNOLOGY SERVICES (ext.7260)

- **Initial IT Consultation**

  Evaluates the vendor's IT security policies/procedures *(IT audit standards, encryption protocols, server security)*

  Investigates other possible IT solutions as required *(ie. internal solution available)*

LEGAL SERVICES (ext.6318)

- **Vendor Service Contract**

  Controls how the vendor handles University personal information *(Limitations on Collection, Use, Disclosure)*

  Ensures that the service contract protects the University *(Privacy, Legal, Financial, Terms)*

PRIVACY (FOIP) OFFICE (ext.7288)

- **Privacy Impact Assessment (PIA)**

  Outlines how your department protects privacy

  Documents your department's mitigation strategy

  Determines the legal authority for your project

  Posts your PIA file number completion online

mtroyal.ca/foip/PoliciesGuidelines

Contacts

Mount Royal University Information Management/ Privacy Office

t: 403.440.7288
w: mtroyal.ca/foip

For the Employee FOIP Toolkit on MYMRU: *Click on Employee Resources Tab under Quick Links for Employees*

Provincial Information and Privacy Commissioner

#410, 9925 - 109 Street
Edmonton, AB T5K 2J8
t: 780.422.6860
w: www.oipc.ab.ca

revised Feb 2013

4. Determine the security arrangements that need to be in place by the vendor

Mount Royal University must **protect** personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction under the FOIP Act.

Signed **legal contracts** should include reasonable steps to prevent against unauthorized collection, use, and disclosure by the company providing the cloud computing services including financial practices and notification by the vendor of either when a security breach occurs or when the vendor is legally obligated to disclose to a third party.

Establish **records destruction** processes. Assign a University system administrator to ensure records are routinely destroyed and use the Mount Royal Records Retention Schedule. If the vendor is responsible for the destruction routinely obtain a record of the destruction and establish an audit process as outlined in the contract.

Discuss with the vendor on what **security measures** they have in place to protect the University's personal information. Do they audit their security?

Document the security protocols in your **Privacy Impact Assessment (PIA)** to assess and demonstrate that privacy was considered prior to implementation.

5. Involve Mount Royal ITS, Legal Services and the Privacy Office (FOIP)

The contract is the first step and the best way to ensure that personal information will be protected by the vendor. Always assess the contract before signing as it should include the following:

Official name and business address of the vendor

Guidelines (limitations) on how the vendor collects, uses, discloses, and actually protects personal information it will store on behalf of Mount Royal University

Audit and Security protocol obligations for the vendor

- **Physical Security**: Locked facility, camera surveillance
- **Administrative Security**: Limited staff access, privacy policies
- **Technical Security**: Routine audit certification, encryption, password-authentication access, fail-safe redundancy, on-ongoing security assessments

Parameters on data ownership and notification concerning:

- Bankruptcy and company takeovers
- Hiring sub-contractors
- Termination of service
- Privacy breaches
- Legal *(foreign)* obligation for disclosure

Location of the cloud data and the applicable law in the event of a contract dispute

Notification requirements in the event the vendor is legally requested to disclose records in a foreign jurisdiction and/or the event of a catastrophic disruption.

Destruction processes regarding who/what/where/when the personal information is destroyed. *(Example: University system administrator)*

6. Complete a Privacy Impact Assessment (PIA) for your project

A Privacy Impact Assessment (PIA) form:

- Helps determine privacy implications
- Informs the public that a PIA was completed
- Can also be reviewed by the Information and Privacy Commissioner

FORM available on **L:Drive/foip**

7. Determine when and how the data will be systematically destroyed in the cloud

Put processes in place regarding how the information will be systematically destroyed in the digital cloud environment.

Electronic records should be assigned a records retention code based on the MRU Records Retention Schedule and routinely destroyed.

- Designate a University system administrator
- Assign a University Records Retention Code
- Have the vendor supply proof of destruction *(if vendor destroys)*

MOUNT ROYAL UNIVERSITY 1910

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY