Cloud-Computing and Protecting Privacy

Jeremy Duffin, BA, MAS, ECMs

Information Management & Privacy Advisor

Mount Royal University

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

Agenda

Step 1 ***– What is Cloud Computing?***

Step 2 ***– What are the basic FOIP Rules?***

Step 3 ***– What are the MRU Best Practices?***

- ***Contract requirements – Legal Services***
- ***IT security requirements – ITS***
- ***Privacy Impact Assessment (PIA's) – FOIP Office***

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

What is Cloud-Computing?

- *Refers to the delivery of **scalable IT resources** over the Internet as opposed to hosting and operating those resources locally through the Mount Royal network (Wikipedia)*
- *These resources can include applications and services as well as the infrastructure on which they operate.*

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

What is Cloud-Computing?

- *In "The Cloud" there are networks of computers that run applications and* ***store data****.*
- *Typically the computers are located in another country - (often leads towards privacy legal implications)*
    - *US Patriot Act (2001)*
    - *Foreign Intelligence Surveillance Act (1977)*
- *Local computers interface with the cloud network*
- *Organizations will purchase IT resources on* ***as-needed basis*** *to save costs.*

MOUNT ROYAL
UNIVERSITY
1910

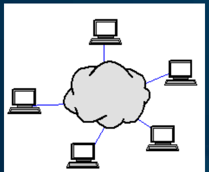
Cloud-Computing and Protecting Privacy

What is Cloud-Computing?

facebook

Gmail by Google

YAHOO!



kijiji

msn Hotmail

Linked in

SurveyMonkey.com
because knowledge is everything

Cloud-Computing and Protecting Privacy

What is Cloud-Computing?

- *BC and Nova Scotia Privacy Laws dictate that all public bodies **must** store personal information in Canada. [*Alberta FOIP Act does not specify]*

Relevant Lawsuits

- *July, 2010 – Winnipeg – Class action privacy lawsuit against Facebook. Facebook used PI for commercial purposes*
- *Sept, 2010 – California – Google (Buzz) settles lawsuit for $8.5 million. Google made PI public*
- *May, 2011 - Best Buy (Epsilon Marketing) 2,500 Clients –*

  privacy breached, personal information hacked
  (stored data not encrypted)
- *June, 2017 – BC – Women sues Facebook for its use of her name and profile photo in ad's she clicked "like" on. (Endorsing company)*

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

What are the basic FOIP Rules?

- *The FOIP Act provides the rules on how public bodies (MRU) must collect, use, disclose and protect personal information (PI).*
- ***Collection**: Public bodies may only collect PI when the info relates directly to and is necessary for an operating program or activity. **(demonstrable need)***
- ***Collection**: Public bodies must generally collect PI directly from the individual the info is about and provide them a **FOIP Notification Statement**.*

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

What are the basic FOIP Rules?

- *The FOIP Act provides the rules on how public bodies (MRU) must collect, use, disclose and protect personal information (PI).*
- ***Use/Disclose**: Public bodies may only **use/disclose** personal information for the purpose for which the PI was collected or compiled or for a use consistent with that purpose. **FOIP Notification Statement***
- ***Protection**: Public bodies **must protect** PI by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

MRU Best Practices – Contract Requirements

- *MRU (Legal Services) must ensure that vendors handling MRU's identifiable PI are contractually obligated to follow FOIP principles.*

FOIP Requirement	**Description**
Data Ownership	MRU owns the data disclosed to the vendor.
Collection/Use/Disclosure	The Vendor may only use MRU's data in order to fulfill the services outlined in the agreement. (e.g. No Marketing - CASL)
Protection	The Vendor will make reasonable security arrangements to protect MRU's data.
Breach Notification Compelled disclosure (US)	The Vendor will, as soon as practicable, notify MRU when they become aware of an unauthorized access, collection, use, disclosure or destruction of MRU's data.
Termination	Upon termination of agreement, the Vendor will provide a copy of the MRU's data and then delete MRU's data after [#] of days. The Vendor will also provide a certificate of destruction.

Cloud-Computing and Protecting Privacy

MRU Best Practices – IT Security

- *MRU (ITS) must ensure that vendors handling MRU's identifiable PI are securely stored.*

ITS Security Requirement	Description
Web transmissions (https)	Vendor website uses (https) Hypertext Transfer Protocol Secure The https ensures that transmitted data is encrypted.
Single Sign-On (SSO)	The Vendor allows granular level access to information based on username/password. Either based on @mtroyal.ca login or otherwise.
Administrator Rights	The Vendor System provides for a database Administrator role, who can manage MRU data. (Create/Delete/Edit/Manage)
Database encryption	The Vendor System (database) is encrypted (at rest).
Service Level Agreement (Catastrophic Disruption)	The Vendor is contractually obligated to ensure that their system will be running 99.9% of the time.
Security Certifications (Audits) -firewalls -24/7 monitoring -vulnerability testing -Anti-virus	The Vendor's security controls have been audited by a third party and has obtained a security certificate. (SSAE 16, ISO27001, PCI, etc) Statement on Standards for Attestation Engagements

Cloud-Computing and Protecting Privacy

MRU Best Practices – FOIP Office

- *MRU (FOIP Office) must ensure that vendors handling MRU's identifiable PI are securely stored.*

PIA Documentation	Description
Legal authorities	Check that the collection/use/disclosure of PI is allowed under the FOIP Act.
Contract Details	Document the articles contained in the contract to prove that steps were taken to control how the vendor will collect/use/disclose/protect MRU's PI.
IT security details	Document Vendor IT Security processes.
Operational processes	Make recommendations for the new business process. -Records Retention Periods -Limiting type (sensitivity) of PI being requested. -Draft FOIP Notification Statements

Cloud-Computing and Protecting Privacy

MRU Best Practices – FOIP Office

How to submit a PIA…

(1) Access PIA Template on L:\foip\FOIP Forms

(2) Fill out ***(Section A) Overview of Project and Benefits***

(3) Fill out ***(Section D) Information Flow Chart***

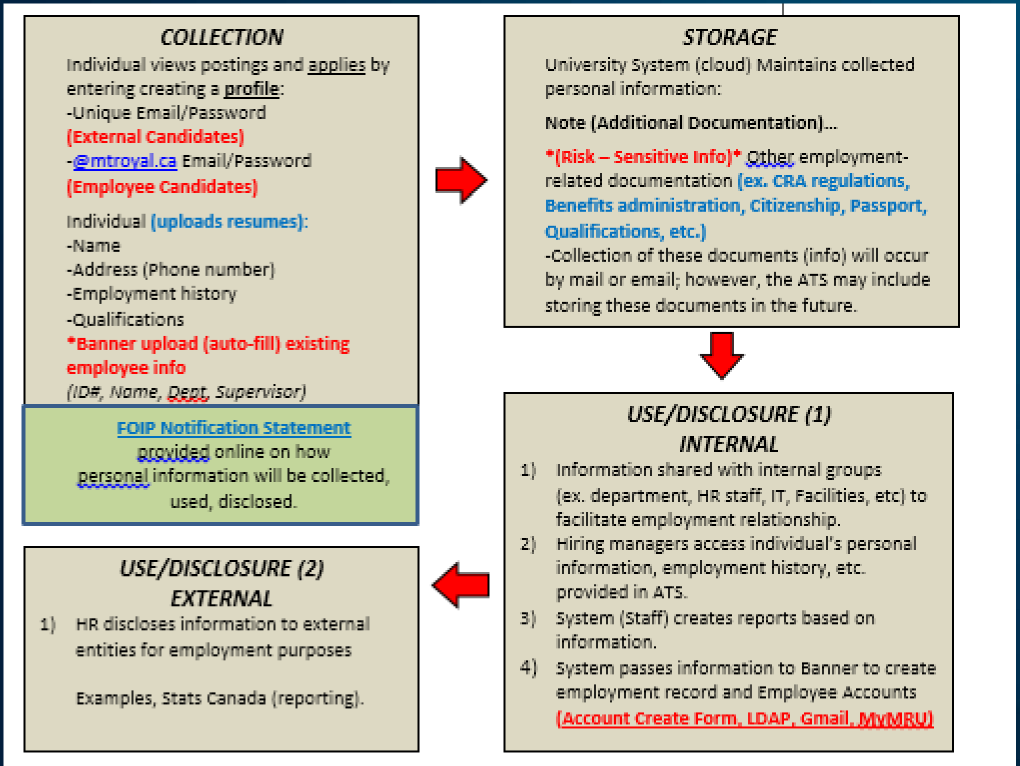
(4) Submit to jgduffin@mtroyal.ca

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

MRU Best Practices – FOIP Office

How to submit a PIA (Section D – Information Flow)…



COLLECTION

Individual views postings and applies by entering creating a profile:
-Unique Email/Password
(External Candidates)
-@mtroyal.ca Email/Password
(Employee Candidates)

Individual (uploads resumes):
-Name
-Address (Phone number)
-Employment history
-Qualifications
*Banner upload (auto-fill) existing employee info
(ID#, Name, Dept, Supervisor)

FOIP Notification Statement provided online on how personal information will be collected, used, disclosed.

STORAGE

University System (cloud) Maintains collected personal information:

Note (Additional Documentation)…

(Risk – Sensitive Info) Other employment-related documentation (ex. CRA regulations, Benefits administration, Citizenship, Passport, Qualifications, etc.)
-Collection of these documents (info) will occur by mail or email; however, the ATS may include storing these documents in the future.

USE/DISCLOSURE (1)
INTERNAL

1) Information shared with internal groups (ex. department, HR staff, IT, Facilities, etc) to facilitate employment relationship.
2) Hiring managers access individual's personal information, employment history, etc. provided in ATS.
3) System (Staff) creates reports based on information.
4) System passes information to Banner to create employment record and Employee Accounts (Account Create Form, LDAP, Gmail, MyMRU)

USE/DISCLOSURE (2)
EXTERNAL

1) HR discloses information to external entities for employment purposes

Examples, Stats Canada (reporting).

MOUNT ROYAL
UNIVERSITY
1910

Cloud-Computing and Protecting Privacy

MRU Best Practices – Tips

- ✓ *Determine what personal info (level of sensitivity) and how much will be stored in the cloud?*
- ✓ *Determine how a **FOIP Notification Statement** will be provided prior to the collection of personal information?*
- ✓ *Send the contract for legal review.*
- ✓ *Check with ITS concerning the vendor IT security.*

  **Vendors that have a security certification are preferred.*

  **A higher level of info sensitivity will require stronger security measures. (Health info, banking info)*
- ✓ *Submit your draft PIA to the FOIP Office*

MOUNT ROYAL
UNIVERSITY
1910

Cloud Computing and Protecting Privacy

Questions?

MOUNT ROYAL
UNIVERSITY
1910