MOUNT ROYAL UNIVERSITY
1910

Cloud Computing Contract – Checklist

*"The public body's **contract** with the outsource provider becomes the primary vehicle through which information risks are managed. In an outsource agreement, the public body **defines control over information**, but the outsource provider implements control over information. A proper contract sets boundaries and expectations for the outsource provider in terms of its allowable actions in the collection, use, and disclosure of personal information."*[1]

***Important:** The following provides a **checklist** used by the MRU FOIP Office and Legal Services and should be used by other departments for reference purposes only. **MRU's Signing Authority Policy (810/819)** states that agreements that do not use legal services approved templates must be reviewed by Legal Services prior to execution.*

Outsourcing Contracts "must" outline the following to protect personal information [FOIP Act][2]…….

- ☐ ***Ownership (Confidentiality)***: The University is the owner of all data loaded into the system and data that belongs to the University is to be kept confidential.
- ☐ ***Collection, Use, and Disclosure***: Compliance with the **Alberta FOIP Act** in that the vendor cannot collect, use, or disclose data beyond the purposes of those purposes authorized by the University (within the University's core mandate). Disclosure by the vendor must be limited to those vendor employees who "need to know" the information for the purpose of providing the services to the University under the contract. Notably, the use of personal information for vendor marketing does not qualify as a mandate under the University and contravenes the FOIP Act.
- ☐ ***Notification of Compelled Disclosure***: The vendor must provide prompt notice to the University, in the event of a compelled disclosure, to allow the University to seek a protective order or other remedy to prevent/contest the disclosure.
- ☐ ***Notification of Security Breach***: The vendor must notify the University in the event of a privacy breach so that the University can notify affected parties of the breach under the FOIP Act. The vendor must provide additional information such as, a cause, date/time, and remedy concerning the breach to the University.
- ☐ ***Security Practices (Data Integrity)***: The vendor must ensure the security and integrity of all data in its possession. For example, data must be maintained in a physically secure location (such as, the facility is monitored 24/7). Security may also include administrative security such as limited employee access to systems ("need to know") and privacy training. Vendor should use the same security standards to store University information as it uses to store its own information of a similar type.
- ☐ ***Termination and Destruction (Confirmation)***: The contract must state that the vendor must **return all** of the University confidential data to the University before the end of the term of the contract with no copy or portion kept by the vendor. Another option is for the vendor to **destroy all** confidential data and **provide a certification (confirmation)** of the data destruction before or shortly after termination.
- ☐ ***Sub-contracting and Solvency***: The Office of the Information and Privacy Commissioner of Alberta recommends that vendors are required to obtain permission from the University prior to engaging sub-contractors or that vendors notify the University of company takeovers. The vendor may also contractually agree to ensure that their subcontractors agree to the same confidentiality clauses outlined in the signed agreement.

---

[1] Public-Sector Outsourcing and Risks to Privacy (February 2006): Office of the Information and Privacy Commissioner of Alberta. http://www.oipc.ab.ca/Content_Files/Files/Publications/Outsource_Feb_2006_corr.pdf

[2] Reviewing the Licensing Automation System of the Ministry of Natural Resources: Privacy Investigation Report (2012) PC12-39: Information and Privacy Commissioner of Ontario. http://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf

MRU Legal Services "musts" in the Contract…….

- ***Parties Involved****:* The contract must be clear in regards to naming the official parties responsible and contact information of those signing the contract. If it is not clear as to what company is responsible for providing a service and upholding their contractual obligations then there is no legal way for the University to hold the vendor accountable to what was signed in the contract.
- ***Governing Law****:* The contract should strive to make the **Laws of Alberta** the governing law over the contract. If doing so is not possible, the parameters above will integrate the FOIP principles on collection, use, and disclosure into the contract (as above).

MRU Information Technology Services "musts" in the Contract…….

- ***Audits (Security)***: The current best practice is for vendors to be **SSAE 16 Type II (SOC's Compliant)** certified. This certification is completed by a Third Party (Auditor) on a regular basis that looks at the vendor's systems including, Logical Security, Privacy Protection, Data Center Security, Incident Management, Communication on Security Initiatives, and Change Management. Further, the contract must have the vendor provide the University **evidence of certification** when requested by the University.
  [**There are many IT security certifications vendors may rely on – Contact ITS or the MRU FOIP Office*]

Other "Possible" Recommendations in the Contract…….

- ***Catastrophic Disruption (Redundancies)***: The vendor must have appropriate **back-up protocols** in case of system-wide failure (physical, technological, and administrative). Several vendors have Emergency Response Plans prepared in the event of a catastrophic event such as, fire, earthquake, tornado, or terrorist attack.
- ***Encryption***: The vendor must use encryption **(SSL, https, and fire walls)** to protect data from interception when being accessed through the internet (hacking). **Passwords** need to be stored in an encrypted format to prevent Third party access and data manipulation.
- ***University System Administrator***: Most contracts provide that key University employees are System Administrator(s) for the software system being implemented, which gives the University more control over the data being uploaded and accessed through the new system. Administrator functionality includes, User and/or Password Administration, Data Quality Control, Monitoring Audit Logs to check who is accessing data, and the ability to ensure that data is actually deleted from the system.

Procedural Best Practices (Internal risk mitigation business processes beyond the Contract)…….

- ***Limiting Data****:* Loading only the data that is necessary to fulfill the purpose of the collection.
- ***Records Retention and Destruction***: The routine/impartial/legal deletion of electronic data based on the Mount Royal University Records Retention Schedule and any applicable University Policies.
- ***Auditing (University System Administrator)***: The ability to audit logins and view who has accessed system data in the event of a privacy breach.
- ***Granular level access (Username/Password)***: The functionality to assign unique usernames/passwords that give granular level access to system data such as "read only" or "administrator".
- ***Privacy Breach Notification Process***: Processes are in place for the Department in the event of a Privacy Breach.
- ***FOIP Notification Statement [Webpage Notice]***: The University Department has notified individuals of the purpose of the collection, the legal authority for the collection under section 33(c), and Dept Contact Information in case there are questions about the collection. In addition, the Department has informed individuals that the University has contracted a Third Party Vendor to provide such services whereby collected information may be housed on servers residing outside of Canada and, therefore, may be subject to the laws of a foreign jurisdiction. Although the University has made reasonable efforts to protect the privacy of users, the University cannot guarantee protection against possible disclosure of data residing in another country.