MOUNT ROYAL
UNIVERSITY
1910

Cloud Computing – Service Level Agreements (SLAs) – Checklist

General Principles – Protecting Privacy and FOIP

○ *The FOIP Act states that the University **must protect** identifiable personal information by making **reasonable security arrangements** against such risks as unauthorized access, collection, use, disclosure or destruction.*

○ *The Office of the Information and Privacy Commissioner (Alberta) resources also highlight that the Service Level Agreement with the Third-Party Service Provider is a **key measure** to mitigate associated privacy risks concerning the management of identifiable personal information within the software.*

○ *Below is a **list of considerations** in contractual provisions that should be reviewed in any Service Level Agreement where the services engage with personal information.*

○ *The steps taken to address privacy risks should correspond with the **sensitivity of the personal information** contained in the system. Increased security measures and processes will be engaged as the sensitivity of the personal information used within the software increases.*

○ *These contractual considerations (below) are **only part of the approach** for mitigating privacy risks - it is also important to ensure there is a review of technical security aspects of the software (Security Questionnaire performed through ITS) and to also weigh practical considerations in the event sensitive personal information is used, or integrated with Banner, in the operation of the software (often through a documented Privacy Impact Assessment or Privacy Review processes) completed by the MRU FOIP Office.*

Service Level Agreement Reviews - basic privacy terms - to protect general personal information

☐ ***Ownership of Personal Information (Confidentiality)***:

The University is the owner of all identifiable personal information loaded into the system and that the information belongs to the University (as between the vendor and the University) is to be kept confidential.

☐ ***Limits on Collection, Use and Disclosure***:

The Service Provider cannot collect, use or disclose MRU's data (or at minimum the personal information) beyond the purposes of providing the services or otherwise authorized by the University.

Disclosure by the Service Provider must be limited to only their employees or contractors who "need to know" the information for the purpose of providing the services to the University under the agreement.

The use of personal information for Service Provider's marketing purposes should be limited.

☐ ***Security Measures***:

The Service Provider must…

Implement reasonable security measures (arrangements) to protect MRU's personal information against such risks as unauthorized access, collection, use, disclosure or destruction.

Use the same security standards to store University information as it uses to store its own information of a similar type. (Optional additional language)

The vendor must ensure the security and integrity of all MRU personal information in its possession. (Optional additional language)

☐ ***Notification of Security Breach or Potential Breach***:

The Service Provider must…

Notify the University in the event of a privacy breach, or potential breach, so that MRU can then notify affected parties of the breach under the FOIP Act.

Provide additional information such as, a cause, date/time and remedy concerning the breach to the University to help with appropriate breach response. (Optional additional language)

☐ ***Termination and Destruction (Confirmation)***:

*The agreement must state that the Service Provider must **return all** of the University confidential personal information to the University before the end of the term of the contract with no copy or portion kept by the vendor.*

*The Service Provider will **destroy all** confidential personal information and either (i) **provide a certification (confirmation)** of the data destruction before or shortly after termination and/or (ii) will destroy data in accordance with their organization's retention bylaws. (Optional additional language)*

Service Level Agreement Reviews - further privacy terms when engaging sensitive personal information

- □ ***Notification of Compelled Disclosure***:

  The Service Provider must provide prompt notice to the University, in the event of a compelled disclosure under legislation. This contractual obligation allows the University to seek a protective order or other remedy to prevent/contest the disclosure.

- □ ***Sub-contracting and Solvency***:

  Government resources recommend that Service Providers are required to obtain permission from the University prior to engaging sub-contractors or that Service Providers notify the University of company takeovers.

  The company providing the service may also contractually agree to ensure that their sub-contractors agree to the same confidentiality clauses outlined in the signed agreement.

- □ ***Audits (IT Security Certifications)***:

  Where sensitive personal information is being stored in software, it is considered best practice to place contractual obligations within the agreement that allows the University to ask for the Service Provider's proof of security certification.

  Alternatively, some vendors provide their proof of certification by providing the publicly available website (url).

  *A **security certification** provides evidence that the Service Provider has taken steps to have their security protocols reviewed by an impartial Third-Party auditor.*

  Examples of security certifications may include:
  (ISO 23081, 27001, 27002, 27018, 29101 - preferred), (ISO 15489, 15801, 16175 - alternatively) or (SOC 2), (SSAE 16 Type II) or (PSI DSS)

Procedural Best Practices - Risk Mitigation business processes beyond the Agreement

Service Provider (External Processes) - ITS Considerations

ITS Security Questionnaire Completed:

ITS has completed the Security Questionnaire to review IT security measures implemented by the Vendor.

Catastrophic Disruption (Redundancies):
*The Service Provider has appropriate back-up protocols in case of system-wide failure (physical, technological and administrative). Servers may also be located strategically across geographic locations to create system redundancies. (Recommend contract, or alternatively supporting doc's, outline an **SLA level of 99.5 - 99.9%** Uptime)*

Incident Management Response Plan:
The Service Provider has an established Incident Management Response Plan based on level of risk.

Encryption (in transit) and (at rest):
*The Service Provider uses encryption protocols **(e.g. SSL, TLS, https)** to protect data from interception when being accessed through the internet in transit (hacking). Data is stored encrypted at rest **(e.g. AES-256)** (including Passwords).*

Confidentiality Training for Employees:
The Service Provider has implemented a training program to remind employees of their obligations concerning protecting the confidentiality of received MRU data.

Data Center Security (24/7/365):
The Service Provider monitors access to their server facilities (24/7/365).

The University (Internal Processes) - FOIP Considerations

Privacy Impact Assessment (PIA) or Privacy Review (PR) Completed:

Based on the data sensitivity, or system-wide integrations, a PIA/PR may be further completed by the MRU FOIP Office.

FOIP Notices (provided via privacy web-page, form, etc):
Ensure FOIP Notices are provided (a "must") when collecting personal information directly from individuals.

Limiting Data and Review of Flow of Personal Information
Review whether there is demonstrable need to collect/use/disclose the personal information for the intended purposes or activity. Also check if the new software will be integrated with the Banner Enterprise System.

University System Administrator:
The software is designed to allow key University employees as an Administrator functionality that includes User and/or Password Administration, Data Quality Control, Monitoring Audit Logs and Data Deletion Functionality.

Auditing (University System Administrator):
The software has user audit logins and to view who has accessed system data in the event of a privacy breach.

Granular level access (Username/Password):
The software has granular level access functionality to system data for University business unit employees such as "read-only", "make edits" or be the system "administrator"?

Records Retention and Destruction:
*Ensure the routine/impartial/legal deletion of electronic data based on the Mount Royal University **Records Retention Schedule** or Transitory Rules and/or any other applicable University Policies.*