Privacy and Security Guidance Cloud Computing in the MUSH Sector

Operational Privacy Risks and Opportunities in Cloud Computing: A Focus on Municipalities, Universities, School Boards, and Hospitals (MUSHSector)
Table of Contents:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of this Guidance Document and How to Apply</td>
<td>3</td>
</tr>
<tr>
<td>Why Focus on the MUSH Sector?</td>
<td>3</td>
</tr>
<tr>
<td>What is Cloud Computing?</td>
<td>5</td>
</tr>
<tr>
<td>Why Use the Cloud?</td>
<td>7</td>
</tr>
<tr>
<td>Due Diligence on the Cloud</td>
<td>8</td>
</tr>
<tr>
<td>ISO/IEC 27018 Standard for Privacy on the Cloud</td>
<td>9</td>
</tr>
<tr>
<td>Frequently Asked Questions</td>
<td>10</td>
</tr>
</tbody>
</table>
Purpose of this Guidance Document and How to Apply

This document is intended to be used by decision makers in the MUSH Sector when considering using cloud services. The document compiles observations and recommendations from a roundtable discussion held June 16, 2015.

Why Focus on the MUSH Sector?

Cloud computing is attractive to any organization holding personal information with limited means to secure it. Ensuring privacy and security is a particular challenge for organizations in the MUSH Sector: in order to provide essential services, they must collect and hold highly sensitive data, yet they have limited resources to protect it. Not surprisingly, these organizations appear to be increasingly vulnerable to information security breaches.

---

### Examples of Identified Operational Cloud Risks and Benefits in Health Care Institutions

#### Benefits
- Simplification of information management;
- Reducing costs in IT staff;
- Scalable infrastructure;
- Tiered data storage;
- Remote disaster recovery and business continuity;
- Facilitated collaboration;
- Continuity of patient care;
- Easy and rapid access;
- Comprehensive report generation;
- Harmonization of information standards, enhanced control and security measures;
- Increased patient care quality.

#### Risks
- Breaches through information sharing;
- Data leakage in multiple tenancy clouds; and
- Loss of control on data through de-localisation and remoteness.

### Examples of Identified Operational Cloud Risks and Benefits in Educational Institutions

#### Benefits
- Reducing costs in IT staff, software and infrastructure;
- Increasing data security;
- Meeting students’ expectations with increased access to new technologies;
- Facilitating content sharing and collaboration;
- Offering world-wide access.

#### Risks
- Security weaknesses (e.g. passwords in clear text, non-encryption) in relation to e-Books, Massive Open Online Courses (MOOC), student or parent-teacher email exchanges;
- Data analytics and Online Behavioural Advertising based on sensitive information from databases (identifiers, marks, comments) and individualized teaching;
- Cyber-bullying, unwanted contacts, ID theft;
- Excessive collection and retention of sensitive data;
- Inadequate safeguards in relation to vulnerability and life experience of users.
What is Cloud Computing?

The National Institute of Standards and Technology of the United States Department of Commerce ("NIST") defines cloud computing as ubiquitous access to a shared pool of configurable computing resources.² These resources could be networks, servers, storage, applications, or services. Five characteristics of cloud computing include:

### Characteristics of Cloud Computing

- **On-demand self-service**: A consumer can access the computing capabilities whenever and wherever they wish.
- **Broad network access**: Computing capabilities are delivered over a private network or the internet.
- **Resource pooling**: The provider’s computing resources are pooled to serve many consumers.
- **Rapid elasticity**: Computing capabilities can be scaled according to consumer demand.
- **Measured Service**: Consumers can pay for service on a pay-per-use or pay-as-you-go basis.

---

## Services Models

<table>
<thead>
<tr>
<th>Software as a Service (SaaS)</th>
<th>Platform as a Service (PaaS)</th>
<th>Infrastructure as a Service (IaaS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumers may use the provider’s applications running on cloud infrastructure (for example, web-based email or customer relationship management software).</td>
<td>Consumers may write or run applications on a cloud-provided platform (for example, a social networking service may offer a platform for software developers to create applications which may utilize data and provide functionality for users of the social networking service).</td>
<td>Consumers may access raw computing resources of a cloud service according to the capacity required (for example, a software developer may test an application in a simulated environment on a cloud service before transferring the software to a live environment).</td>
</tr>
</tbody>
</table>

## Deployment Models

**Public Cloud**

In the public cloud, the cloud services are available to the general public over the internet, while the infrastructure, platform, or software is managed by the cloud provider.

**Private Cloud**

In the private cloud, the consumer is the exclusive user of the service.

**Community Cloud**

In the community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

**Hybrid Cloud**

In the hybrid cloud, the cloud infrastructure is a composition of two or more cloud infrastructures that remain unique.
Why Use the Cloud?

The Office of the Privacy Commissioner of Canada identifies the main benefits of cloud computing as:

- Scalability, by offering unlimited storage and processing capacity;
- Reliability, since it eliminates the risk of losing paper, laptops, or hard drives and allows access to documents and applications via the Internet worldwide;
- Cost savings, since resources are pooled for optimal safeguards thus eliminating the need for investment in infrastructure;
- Efficiency, as the freeing up of resources through the pooling of expertise allows focus on other priorities; and
- Access to new technology as the cloud providers, being more resourceful and specialized in the area, are in a position to offer a much wider choice.³

The Québec Commission d’accès à l’information adds: increased storage capacity and opportunity to base expenses on actual use. Experts underline the low cost of cloud computing and world wide availability.⁴

A survey conducted by SafeGov indicated why many organizations are ‘going cloud’:

<table>
<thead>
<tr>
<th>Why are they going cloud?</th>
<th>0%</th>
<th>25%</th>
<th>50%</th>
<th>75%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save Money</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>61%</td>
</tr>
<tr>
<td>No More Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>52%</td>
</tr>
<tr>
<td>Dynamic Provisioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>39%</td>
</tr>
<tr>
<td>Replace Old Apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>34%</td>
</tr>
<tr>
<td>New Features</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>33%</td>
</tr>
<tr>
<td>Easier for End Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>19%</td>
</tr>
<tr>
<td>More Secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16%</td>
</tr>
<tr>
<td>Better Tech Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15%</td>
</tr>
<tr>
<td>Utility-Based Pricing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5%</td>
</tr>
<tr>
<td>Political Mandate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5%</td>
</tr>
</tbody>
</table>

---


Due Diligence on the Cloud

When considering whether to move to cloud computing, MUSH organizations should exercise due diligence commensurate to the sensitivity of the personal information they hold by:

1. assessing organizational needs and available cloud computing services;
2. examining legal obligations in relation to privacy protection;
3. performing a risk/benefit analysis of cloud computing in relation to their particular mandate; and
4. negotiating with the cloud provider,
   - Appropriate authentication/access controls that correspond with the sensitivity of the data;
   - Business continuity measures to prevent data loss in case of an outage, particularly if essential services are provided;
   - Capacity to integrate existing directory services, considering the number of files on one individual as well as the fact that some files may go on cloud and others not
   - Financial stability, technological security, track record and corporate responsibility, to ensure long term service, considering the essential, long-term mandates of MUSH organizations;

   • Clear policies for cookies, data collection minimization, use, retention and disclosure, and individual access rights;
   • Protocol for managing encryption;
   • Termination clauses to recover or delete all personal information held in the cloud;
   • Plan for data breach response;
   • Breach insurance or indemnification.
   • Transparent policies about purposes of cloud outsourcing and in obtaining consent, considering the sensitivity of data collected in the MUSH Sector.
   • Describing each party’s obligations;
   • Providing for periodic audits.

The clauses are essential and yet may be difficult to secure. Many MUSH institutions find themselves in front of “take it or leave it” cloud computing contracts. A solution is to go with a cloud provider compliant with ISO/IEC 27018 Code of Practice for Personally Identifiably Information (“PII”) Protection in Public Clouds Acting as PII Processors which requires all these guarantees as a matter of certification.6

---


ISO/IEC 27018 Standard for Privacy on the Cloud

ISO/IEC 27018 is the International Code of Practice for Personally Identifiable Information (“PII”) Protection in Public Clouds Acting as PII Processors. The Office of the Privacy Commissioner of Canada – with input from representatives of the Government of Canada, other states and Data Protection Authorities – has significantly contributed to the development of the standard. It is not the only standard for data protection in the cloud, but it has unique value in that it:

- offers a single, standardized, international set of privacy controls that align closely with existing privacy requirements;
- integrates directly into a data security framework; and
- has the highest compliance mechanisms through a certification process issued by an independent auditor and annual audits to ensure ongoing compliance.

This new standard holds certified cloud service providers to the following main obligations:

- Customer control: Store and use personal information exclusively in accordance with the instructions of the cloud customer and do not require the customer to consent to the use of their data for advertising and marketing purposes as a condition of their use of the service;
- Data retention: Establish a retention period after which customer data will be permanently returned or deleted;
- Accountability:
  - Disclose sub-processors of personal data, notify the cloud customer of any changes in sub-processors, and provide the customer the opportunity to terminate their agreement if they object to a change;

- Promptly notify the cloud customer of any breach, unauthorized access to personal information or unauthorized access to processing equipment or facilities resulting in law, disclosure or alternation of personal information;
- Disclose the countries in which a cloud customer’s personal information might be stored;
- Undergo an annual audit by the cloud customer or by an independent auditor.
- Non-disclosure: Reject any requests for personal information disclosure that are not legally binding and consult with the relevant cloud customer unless notification is prohibited (for example if it compromises an investigation); and
- Safeguards: Implement technical and organizational measures to safeguards to protect personal information.

The main advantages of ISO/IEC 27018 for the MUSH sector are as follows:

- Selecting a cloud service provider that is ISO/IEC 27018 compliant supports the cloud customer’s due diligence efforts;
- The annual independent audit required by ISO/IEC 27018 provides the cloud customer ongoing assurance that the cloud service provider remains in compliance with the standard’s requirements; and
- Because ISO/IEC 27018 is built on ISO/IEC 27001 and 27002 (INSERT NAME), the cloud service customer benefits from the enhanced security of a cloud service that adheres to international security standards.
Frequently Asked Questions

• Question: Are data centers in the United States subject to the USA PATRIOT Act?
  • Answer: Yes, and the sharing of data between Canadian and US law enforcement agencies occurs whether or not information is stored in the cloud. However, ISO/IEC 27018 requires cloud service providers to deny any request for personal information from law enforcement authorities without consent unless there is a legally binding authority, and even then the cloud provider will consult the cloud customer, unless prohibited by law. Customers should negotiate this requirement with their non-certified cloud provider.

• Question: Is the encryption up to the customer?
  • Answer: The customer may encrypt its own data. Certain cloud service providers may also encrypt the data ‘in transit’ between its customers and its service, between its data centres, and ‘at rest’.

• Question: Can personal data be mined in the cloud for advertising/marketing purposes?
  • Answer: Yes, with the customer’s consent. However, ISO/IEC 27018 prohibits a cloud service provider from making such consent a mandatory condition for using the service. The cloud provider holds the information on behalf of the customer much like a bank holds deposits in a safety deposit box on behalf of its customers.

• Question: How effective are contractual obligations to protect data?
  • Answer: A cloud provider that has made the significant investment to bring its operations in line with ISO/IEC 27018 to obtain certification, and whose business rests on that certification, will treat ISO/IEC 27018 obligations with the utmost seriousness. Breach of those obligations could result in the cloud provider failing an audit and losing its certification. If a cloud customer relies solely on contractual terms, it may not know if the cloud service provider is complying with those obligations absent a private audit (which the customer may not have the contractual right to demand, and if it does, may be too costly to be practical).

• Question: Which laws apply to cloud service providers?
  • Answer: In Canada, the cloud customer is responsible for ensuring that the cloud provider that receives the data for processing provides a “comparable level of protection [to which the cloud customer is obligated under Canadian law] while the information is being processed” by the cloud provider. This is ensured by contractual or other means.

  The cloud provider is bound by contract to respect the data protection obligations of the cloud customer. ISO27018 certified cloud providers also undertake to offer “support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed (between) the public cloud processor and its clients (cloud service customers)”. However, the cloud provider is also bound by the law applicable in the territory where it is located. For that reason, requests from government authorities of the territory of the cloud provider apply to disclosure of that data. It is with that in mind that ISO 27018 requires certified cloud providers to disclose to the cloud customers the location of their servers as well as the countries of origin of their sub-contractors.

As of July 10, 2015, we are aware of only two significant cloud service providers who have achieved compliance with ISO/IEC 27018: Microsoft and Dropbox.