CONTENTS

1. Background ......................................................................................................................... 2
2. Legislative and Policy Requirements ..................................................................................... 3
3. Out of Country Considerations ............................................................................................ 4
4. End User Notification ........................................................................................................... 5
5. Safeguards ............................................................................................................................ 5
6. Contract Considerations ....................................................................................................... 6
1. **Background**

Providing Algonquin College's data to a third-party cloud service provider has important security considerations. Increasingly, the College is handling more sensitive information, whether it be staff or student PII, student health data, financial data, applied research data, or sensitive business planning information. Also increasing is the hacktivists' and criminal organizations’ desire to steal College electronic identities and information for purposes of selling it on the black market. Without clearly understanding the service provider’s security architecture, practices, and without stipulating the minimum set of security safeguards and clauses required in contract, the College and its data may be subjected to unacceptable vulnerabilities, threats and risks, and may be non-compliant with legislative requirements and College policy.

Clouds deliver scalable services that provide networking, computing and applications services for multiple ‘tenants’, which often provides for a compelling business case. However, shared infrastructure including CPUs, GPUs, disk partitions, memory, and other components—weren’t originally designed for strong compartmentalization, and thus separation and protection of client data. Even with newer virtualization technologies, and the use of hypervisors to mediate access between operating systems and physical resources, there is risk that attackers can gain unauthorized access and control of the underlying platforms. Compromise of the hypervisor layer can lead to a potential compromise of all the shared physical resources of the server that it controls, including memory and data as well as other virtual machines (VMs) on a given server. There are also additional risks associated with the data as it is transmitted to and from the cloud service provider, and with system account management, which must be properly addressed.

Generally speaking, it is possible to adequately secure cloud service provider environments. However, this requires careful planning and deployment, along with overall due diligence. The best way to approach cloud security is to integrate it with overall cloud services planning, beginning early in the process. In this way, a proactive, measured and risk based approach can assist with designing the cloud delivery model, architecture, processes and related cloud security requirements.

The College can outsource service and provide sensitive data in the process, however it can’t outsource overall accountability and responsibility. Ultimately, the College remains legally responsible for the safeguarding personal information even if it is outsourced and thus it remains with the College to make sure that any cloud service provider implements adequate safeguards.

Questions or suggestions regarding this guide should be forwarded to:

Manager, Information Security  
Information Technology Services (ITS)  
infosec@algonquincollege.com  
X6491
2. **Legislative and Policy Requirements**

Algonquin College is subject to three primary Acts that drive information security and personally identifiable information (PII) requirements:

1. **PIPEDA (Personal Information and Protection of Electronic Documents Act) - Federal**
2. **FIPPA (Freedom of Information and Protection of Privacy Act) - Provincial**
3. **PHIPA (Personal Health Information Protection Act) - Provincial**

While these acts generally state that PII should be protected, they do not prescribe specific security practices that should be adopted when using cloud computing. As an example, PIPEDA only states that safeguards must be adopted that are commensurate with the sensitivity of the information. The more sensitive the information, the greater the precautions that should be taken. The generally accepted view is that industry best practices (e.g. ISO 27001 safeguards) should be used. The Cloud Security Alliance (CSA) (www.cloudsecurityalliance.org) provides good information on proper cloud security safeguards. CSA also administers the Security, Trust & Assurance Registry (STAR) program (https://cloudsecurityalliance.org/star/registry/), a publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud service providers they currently use or are considering contracting with.

It is important to note that PHIPA has mandatory breach notification provisions. That means that if health data is compromised the College would be obligated to notify affected individuals without delay. The Federal Privacy Commissioner and Ontario Privacy Commissioner are currently pushing for similar notification provisions within PIPEDA and PHIPA.

Algonquin College has three (3) primary Directives and a Data Privacy Statement that include outsourcing security requirements, namely:

1. **Academic Affairs AA-35 (Confidentiality of Student Records)**
   
   1.5 **All online or web accessible student information will reside on secure College owned and operated servers or on approved external third party operated servers, and be readily accessible to College employees responsible for the administration of such information.**

   1.6 **The use of an external Application Service Provider (ASP) to house Algonquin student information must include an agreement with clear indications on security, privacy, retention, deletion and backup procedures, signed by the Director, Information, Institutional Research and Technology Services (IIrts), the Registrar, the VP Administration (Freedom of Information Coordinator) and the Vice President, Academic.**

2. **Administration AD-02 (Freedom of Information and Protection of Privacy)**

   3.4 **The College remains accountable for personal information under its control, including personal information which is disclosed to third parties for processing. The College will use contractual or other means to protect personal information that has been transferred to service providers for processing.**
3. Information Technology IT-05 (Information Sensitivity and Security)

6.2 All employees and third parties who have access to sensitive information will be asked to sign a written acknowledgement of having read this policy, and agreeing to comply with its provisions.

7.2 All online or web accessible Student Information will reside on secure College owned and operated servers or on approved external third party operated servers, and be readily accessible only to College employees responsible for the administration of such information.

7.3 The use of an external ASP other than the College owned and operated servers to house Algonquin student information must include an agreement with clear indications on security, privacy and backup procedures, signed by the Director, IIRTS, the Vice President, Administration and the Vice President, Academic.

Algonquin College Data Privacy Statement

"The College will take all reasonable measures to safeguard personal information in its control, including but not limited to physical, technical, and operational measures. The College will require, by contract or otherwise, that any third party service provider to whom personal information is transferred has adequate policies and safeguards in place to protect that information."

3. Out of Country Considerations

There are very few laws that prevent Canadian public sector organizations from 'exporting' PII. Currently, only B.C. and Nova Scotia have legislation that restricts the PII export. With all other provinces - Ontario included - export is allowed, however the public organization must ensure a similar level of security for PII whether it is managed by a Canadian or a non-Canadian company.

There exists considerable organizational concern relative to outsourcing applications and PII to cloud services located outside of Canada, with the most common concern being the potential application of the USA Patriot Act. The reality is that it doesn’t matter where the information resides, it will most always be subject to access by law enforcement and national security organizations through various informal and formal means. This includes the US and Canadian sharing agreements. European countries typically permit even broader access.

In the US, the Foreign Intelligence Surveillance Act (FISA), as amended by the Patriot Act, permits secret court orders for the production of “any tangible thing” in connection with terrorism investigations. Unfortunately, these orders are often inclusive of a gag order that prevents the company from notifying its customer that the government is accessing its data. The Act also permits the US government to intercept foreign communications and international communications without a warrant.

In Canada, lawful access includes search warrants under the Criminal Code of Canada and the Canadian Security Intelligence Service Act, and administrative subpoenas such as those issued under the Income Tax Act. As well, Canada’s National Defence Act has similar intercept powers as US FISA.
It is important to note that keeping data within Canada does not guarantee protection from US lawful access. Canada and the US, along with most other western democracies, have long cooperated (even before the Patriot Act) with mutual legal assistance treaties and ad hoc information sharing. US law enforcement agencies, such as the FBI, can make a formal request of the RCMP or CSIS to obtain the relevant PII on their behalf, through laws aforementioned. Most Canadian privacy laws actually permit this sort of information sharing.

There has been considerable recent public debate concerning a recently discovered covert US "Prism" data gathering program. A surveillance system launched in 2007, Prism allows the US National Security Agency (NSA) to "receive" emails, video clips, photos, voice and video calls, social networking details, logins and other data, held by a range of US internet firms including Microsoft and its Skype division; Google and its YouTube division; Yahoo; Facebook, AOL, and Apple. Obviously, If there is concern with this, the obvious solution(s) are (a) not use these organizations to store sensitive College data, and/or (b) encrypt the data with strong security ciphers (e.g. AES 128) for which only the College holds the encryption key(s). This latter safeguard often proves to be unworkable, due to the fact that Cloud service providers often require access to the data to administer systems, or in some cases, it forms part of their business model (e.g. Facebook).

4. **End User Notification**

The Privacy Commissioner of Canada believes that organizations processing PII outside of Canada should give notice to its end users. It is important to note that 'notice' does not mean 'request for consent', allowing an 'opt out' situation.

Algonquin College's Data Privacy Statement, often associated with College websites (some of which may be located in the Cloud, outside of Canada), contains the following: "On occasions, personal information may be collected, used and/or disclosed in jurisdictions outside of Ontario."

5. **Safeguards**

As with any new IT solution that involves the handling of PII, a privacy impact assessment (PIA) should be undertaken. PIAs are a systematic way of identifying and documenting all of the privacy concerns inherent in an IT solution so that they can be properly managed. It also documents the recommended safeguards required to address any areas of unacceptable risk. The Manager, Information Security, ITS, maintains an Algonquin College PIA template and can assist with the process.

For any IT solution that involves the handling of sensitive data other than PII (e.g. sensitive business information or third-party information of which the College is obligated to protect) a statement of sensitivity (SoS) should be documented. An SoS systematically identifies the confidentiality, integrity, and availability requirements so that they can be properly managed. The Manager, Information Security, ITS, maintains an Algonquin College SoS template and can assist with the process.

In addition, and depending on the situation, a threat and risk assessment (TRA) should be undertaken.
In all circumstances in which cloud computing is being considered, a consultation with the ITS Information Security unit should be undertaken to help identify the right mix of security safeguards for the particular situation.

6. Contract Considerations

When Algonquin College acquires the services of a cloud service provider, such as in a Software as a Service (SaaS) or Infrastructure as a Service (IaaS) situation, it is important to include the following security related clauses in a legal agreement. These clauses will help protect the data, and avoid an unauthorized breach. There are additional, more stringent contractual requirements that need to be considered when personal health data is under consideration, due to PHIPA mandatory breach notification provisions.

1. Information Ownership
   The contract should state that Algonquin College is the sole owner of all College information. College information should be defined as that created or modified by service/system, including all data created, modified, collected and stored in databases, including legacy data.

2. Information to Be Held in Trust
   The contract should stipulate that Algonquin College's data is "held in trust". This ensures that the College retains ownership, and the service provider's role with respect to the data is to process, store and manage it on the College's behalf.

3. Limiting Secondary Use
   The contract should limit the purposes for which the service provider can use Algonquin College data. Some service providers may wish to gather analytics about users and/or their data for service improvement purposes, however secondary uses should be strictly limited, identified and pre-authorized in writing.

4. Obligation to Resist Legal Process
   If the service provider receives legal notice that requires the handover of College data, yet the service provider is not allowed to inform the College, it would be mandatory that the service provider resists the handover to the extent possible. For example, if the service provider receives a subpoena or a production order under US FISA, then it should apply to the court to have the subpoena quashed, even if not successful in the end. Some orders such as search warrants, and depending on the jurisdiction, cannot be resisted at the time; however, an application can be made to have the warrant set aside and the data returned.

5. Obligation to Cooperate with Regulators' Investigations
   In the event of an investigation by a Privacy Commissioner or some other government regulator, the service provider should be obliged to assist the College with the investigation.
6. **No Direct Regulator Participation**  
In the event of an investigation by a Privacy Commissioner or other government regulator, the service provider should not be allowed to deal directly with the regulator. Since the data is owned by the College (and held in trust) the job of addressing any complaints will be the College’s alone.

7. **Security Safeguards – Set Minimums and Shift Responsibility**  
Cloud agreements are complicated, technologies are subject to constant change and security standards shift over time, thus it is better to have the service provider agree to abide by well-known information security standards or subsets thereof (e.g. ISO 27001, ISO 22301) or approaches, instead of dictating specific technologies to use. Set minimums, ensure third-party audits are being conducted on a minimum annual basis, and ensure that the College has the right to obtain copies of the audit reports. Ensure physical and environment security of the data center is covered, in addition to logical security controls.

8. **No Limitations of Liability Related to Data Privacy and Security (Full Indemnity)**  
One primary reason for choosing a cloud service provider is because of their expertise in securing College owned data. The agreement should not limit liability to a nominal amount if the service provider fails to safeguard College data and a breach occurs as a result. Warranty and indemnity should cover all costs, mitigations and remedies to limit damage as a result of a security breach. The service provider should have adequate insurance for incidents, should be obliged to keep the insurance in force, and should provide the College insurance certificates, when requested.

This is not as important in situations where the data is encrypted.

9. **No Retention of Information after Contract Completion**  
The service provider should be obliged to return or destroy (according to industry security standards) all copies of College data (including any backups) within a set period of time (e.g. one week) if the contract ends or is terminated.

*Information Security is everybody’s business*