Carleton University

Policy Name:	**Cloud Computing Security Policy**
Originating/Responsible Department:	**Information Technology Services (ITS)**
Approval Authority:	**Senior Management Committee**
Date of Original Policy:	**May 2015**
Last Updated:	**May 2022**
Mandatory Revision Date:	**May 2023**
Contact:	**AVP (ITS) & Chief Information Officer**

Policy Statement:

The confidentiality, integrity and availability of the University's information must be preserved when stored, processed, or transmitted by a third-party cloud computing provider. Any risk to the University must also be evaluated to determine if the risk can be avoided, accepted, or transferred.

Purpose:

This Policy defines the security requirements on the use of cloud computing to protect internal, confidential, and sensitive information being processed, stored, or transmitted by cloud computing services, by ensuring risks to the University are identified and appropriately managed.

Scope:

This policy applies to all faculty and staff utilizing external cloud computing services for the storage and/or processing of Carleton University internal, confidential, or sensitive data or data which the University has a contractual or regulatory obligation to secure.

Procedure:

Cloud computing is the provisioning of services and applications through shared infrastructure, typically accessed over the Internet. These can be:

- Internal, with the infrastructure owned and operated by the University (private);
- External to the University (public, remotely hosted i.e., third party); and/or
- A combination of both public and private clouds (hybrid).

The use of external cloud computing resources presents risks that must be understood and considered in the selection of cloud computing providers. Risks include but are not limited to the:

- Loss of information confidentiality and potential reputational damage to the University; e.g., data breaches;
- Non-compliance with federal and provincial privacy legislation, regulation and guidelines;
- Cloud computing providers' unilateral change of their terms of service;
- Loss of information; e.g. disappearance of cloud provider, with no adequate backup of service or data;

- Loss of information ownership;
- Unavailability of information; e.g. Denial of Service;
- Loss of control over information; e.g. information stored using non-University cloud accounts;
- Inability to investigate the change in integrity, confidentiality or availability of the service or information;
- Inability to satisfy timely information requests for legal, investigatory or compliance purposes;
- Hijacking of cloud computing account or service; and
- Inability of the University to control information access controls.

Examples of external cloud computing services that incur these risks include, but are not limited to:

- Free versions of cloud storage services such as OneDrive, Google Drive, Dropbox, Box, Amazon Cloud Drive, Amazon S3, CloudMe, etc.
- Free email services such as Hotmail, Gmail, Outlook, GMX, Yahoo, etc.
- Software as a Service (SaaS) providers that don’t ensure the confidentiality, integrity, or availability of information.

To address these and other risks, formal agreements are required with external service providers.

Agreements with External Providers

Formal agreements with third parties where internal, confidential, or sensitive information are involved are required to ensure these services are provided in compliance with University policies and privacy legislation. This applies also to the personal information exchanged with third parties for the purposes of service provisioning.

These agreements must include the following requirements on the use of cloud computing for the storage, processing, or transmission of University data assets:

- Clear confidentiality, integrity and availability requirements including the treatment of internal, confidential and sensitive information;
- Employee security awareness and training;
- Limitations on information collection, use and disclosure;
- Information ownership must remain solely with the University;
- Vulnerability management requirements including periodic vulnerability assessments and penetration testing;
- Suitability requirements on the third party, including the provision of independent audits and audit attestations on information security controls;
- Provisions governing the return and destruction of information in the third party’s possession in compliance with the university Corporate Records and Archives Policy;

- Provisions on the protection of information in accordance with the Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) and Personal Health Information Protection Act (PHIPA) and their associated formal request for information requirements;
- Provisions on the protection of information in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA);
- If necessary, provisions on the limitation of use of contact information in accordance with Canada's Anti-Spam Legislation and Carleton's Anti-Spam Compliance Policy.
- Information Security incident response, management and notification requirements;
- Limits and requirements on subcontracting; and
- When credit card data is involved, the requirement to demonstrate ongoing compliance as a service provider to the Payment Card Industry Data Security Standard (PCI DSS).

Where internal, confidential, or sensitive information is involved, Data Protection Risk Assessments must be performed prior to the exchange of information and awarding of a contract. Assessments are conducted by the ITS Security Governance team and the University's Privacy Office.

Standards, Compliance, and Reliability

Service providers housing data considered internal, confidential, or sensitive under Carleton's Data and Information Classification and Protection policy are required to provide evidence of data center certification against acceptable industry standards (i.e., NIST, HECVAT, SAS 70 Type II, SSAE 16, SOC 1, SOC 2, SOC 3, or ISO) which are appropriate in the circumstances. Likewise, if a service provider's role is deemed critical to University operations, its data center must be at least Tier 3 according to the industry recognized Data Center Tier Classification Standard which categorize Data Center reliability.

Roles and Responsibilities:

Department Chairs, Directors and Management are responsible for:

- Ensuring that University policies are adhered to during the procurement and use of external cloud computing,
- All engaged by the University are responsible to consider security and privacy requirements when evaluating and selecting potential vendors for services;
- Ensure that, prior to signing any binding agreement or contract, the University's Signing Authorities Policy and Procurement Policy have been complied with and, if necessary, that Procurement Services has been consulted to provide guidance on purchasing requirements;
- Ensure that, prior to signing any binding agreement or contract, ITS Security has been consulted to provide guidance on security requirements;
- Ensure that, prior to signing any binding agreement or contract, the Carleton University Privacy Office has been consulted to provide guidance on the privacy impact to the university;
- Ensure that, prior to signing any binding agreement or contract, a formal agreement has been reviewed by the Office of the General Counsel, and, Risk and Insurance Services, to comply with the university's Signing Authorities Policy;

- Ensure that, prior to singing any binding agreement or contract, the Business Office has been consulted where Credit Card payments are being processed or managed by the Cloud Service Provider;
- Ensure that, prior to singing any binding agreement or contract, the Corporate Archives and Records Office has been consulted where records are being processed or stored by the Cloud Service Provider;
- Ensure the University receives a current copy of a third party's Attestation of Compliance or Report on Compliance if processing of credit cards is a component of the external vendor's service offering;
- Ensure that the confidentiality of sensitive and personal information is protected by only using approved features and functionality from approved cloud computing service providers;
- Obtain permission from data asset owners prior to using cloud computing to process, store or transmit University data assets;
- Ensure that new cloud services or applications procured are used in compliance with University policy as well as privacy legislation (FIPPA, PIPEDA);
- Supporting the completion of Data Protection Risk Assessments; and
- Ensuring that all agreements that are renewed are re-evaluated under this policy for cases where the services consumed or the agreements have changed, or where a Data Protection Risk Assessment has not been previously completed.

ITS Security Governance is responsible for:

- Providing security guidance on security requirements for external vendor contracts; and
- Completing the Data Protection Risk Assessment process in collaboration with the Carleton University Privacy Office.

Carleton University Privacy Office is responsible for:

- Providing guidance on external vendor agreements including applicable laws governing the protection of personal information; e.g., FIPPA, PIPEDA, CASL and GDPR
- Completing the Data Protection Risk Assessment process in collaboration with ITS Security Governance and reporting findings to internal stakeholders.

Office of the General Counsel is responsible for:

- Review of any agreement, prior to signing.

Risk & Insurance Services is responsible for:

- Providing guidance on insurance and broader risk issues to the university prior to signing agreements.

Contacts:
Assistant Vice-President (ITS) & chief Information Officer

Links to Related Policies:

- Information Security

- Information Technology (IT) Security
- Data and Information Classification and Protection
- Information Security Incident Response
- Signing Authorities
- Procurement
- Risk Management
- Anti-Spam Compliance
- Access to Information and Privacy
- Corporate Records and Archives
- Personal Health Information Processing