Carleton UNIVERSITY
Canada's Capital University

Policy Name:	**Cloud Computing Security**
Originating/Responsible Department:	**Information Technology Services (ITS)**
Approval Authority:	**Senior Management Committee**
Date of Original Policy:	**May 2015**
Last Updated:	**May 2020**
Mandatory Revision Date:	**May 2021**
Contact:	**AVP (ITS) & Chief Information Officer**

Policy:
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 in order 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 faculty and staff utilizing 3rd party cloud computing services for the storage and/or processing of Carleton University internal, confidential or sensitive data or data which Carleton has a contractual or regulatory obligation to secure.

Procedures:
Cloud computing is the provisioning of services and applications through shared services or resources. 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)
- A combination of both public and private clouds

The use of3rd-party cloud computing and applications introduces risks that must be considered in the selection of cloud computing providers. Risks include but are not limited to the:

- Loss of information confidentiality and potential brand damage to Carleton; 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;
- Availability 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 3rd-party 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 third party service providers.

Third Party Agreements

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 confidential or personal information:

- 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;
- Provisions on the protection of information in accordance with the Ontario Freedom of Information and Protection of Privacy Act (FIPPA) as well as Access to Information requirements;
- Provisions on the protection of information in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA);
- 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.

Where internal, confidential or sensitive information is involved, Information Security and Privacy Impact Assessments must be performed prior to the exchange of information and awarding of a contract.

Standards, Compliance, and Reliability

Service providers housing data considered sensitive or confidential 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. 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 Carleton operations, its data center must be at least Tier 3 according to the industry recognized Data Center Tier classification standards 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 third-party 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 ITS Security has been consulted to provide guidance on security requirements for third party contracts;
- Ensure the Carleton University Privacy Office has been consulted to provide guidance on the privacy impact to the university;
- Ensure that a formal agreement has been reviewed by Carleton University's General Counsel office and to comply with the university's Signing Authorities Policy prior to signing the agreement;
- Ensure the Business Office has been consulted where Credit Card payments are being processed or managed by the Cloud Service Provider prior to the signing and acceptance of the agreement;
- Ensure the University receives a current copy of a third party's Attestation of Compliance or Report on Compliance if processing of credit cards are a component of the third party 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 information owners prior to using cloud computing to process, store or transmit University information;
- 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 required Security and Privacy Impact 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 Security Assessment and/or a Privacy Impact Assessment has not been previously completed.

ITS is responsible for:

- Providing security guidance on security requirements for third party contracts; and
- Conducting Information Security Assessments.

Carleton University's Privacy Office is responsible for:

- Providing guidance on third party agreements including applicable laws governing the protection of personal information; e.g.; FIPPA, PIPEDA; and
- Conducting Privacy Impact Assessments.

Carleton University's General Counsel Office is responsible for:

Review of the agreement, prior to signing;

Compliance
Non-compliance to this Policy may result in disciplinary action.

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

Links to Related Policies:
http://carleton.ca/secretariat/policies/

- Information Security Policy
- Information Technology (IT) Security Policy
- Data and Information Classification and Protection
- Information Security Incident Response
- Signing Authorities Policy

http://www.carleton.ca/privacy/policies/

- Carleton's Privacy Policies

http://carleton.ca/ITS/about-ITS/policies/

- Guidelines for the Use of Cloud Computing