Atlantic Canada Opportunities Agency

SUMMARY OF PRIVACY IMPACT ASSESSMENT FOR MICROSOFT OFFICE 365

1. Overview and Privacy Impact Assessment Initiation

1.1 Overview of the Atlantic Canada Opportunities Agency

The Atlantic Canada Opportunities Agency (ACOA) works in partnership with Atlantic Canadians to improve the economy of communities throughout the region and to enhance its competitiveness. Working with partners in government, the private sector, academia and other non-government sectors, ACOA seeks to advance economic opportunities and innovation in order to serve the needs of businesses, organizations, individuals and communities. This work addresses the Agency's mandate "to enhance the growth of earned income and employment opportunities in Atlantic Canada."

With its many partners in economic development, ACOA works to strengthen the Atlantic economy through:

- Enterprise development – helping improve the business climate and lending a hand for individual business start-ups, modernizations and expansions.
- Community development – working with communities to nurture economic growth, improve local infrastructure and develop opportunities in the local economy.
- Policy, advocacy and coordination – being a champion for Atlantic Canada by representing the region's interests at the national level in areas such as policy development as well as research and analysis and in work with other departments to ensure coordination of policies and programs.

ACOA is subject to the accountability regime set out in Part II of the *Financial Administration Act* (FAA) and is listed under Schedules IV and VI of the FAA.

1.2 Government of Canada Policy Alignment

The Treasury Board *Directive on Privacy Impact Assessment* (PIA) provides direction to government institutions on how to assess the privacy impacts of new or substantially modified programs or activities involving the creation, collection and handling of personal information. It also ensures that privacy implications will be appropriately identified, assessed and resolved before a new or substantially modified program or activity involving personal information is implemented.

Government of Canada Policy Hierarchy

- *Privacy Act*
  - Policy on Privacy Protection
    - Directive on Privacy Impact Assessments
    - Directive on Privacy Practices
    - Directive on Social Insurance Number

1.3 Description of the Initiative

M365 is the Government of Canada's (GC) new digital platform to improve the way federal government employees communicate and collaborate with their colleagues and deliver services to Canadians.

Microsoft Canada Inc. commissioned independent PIAs on its Microsoft Office 365 cloud computing platform as well as its Azure Infrastructure as a Service and Platform as a Service. Those documents are available on Microsoft's Compliance Resources for Canada page.

ACOA was 1 of 5 departments chosen by Shared Services Canada (SSC) as pathfinders to roll out Microsoft 365 (M365) to all employees. This suite of software includes updated and multi-platform versions of Outlook, Word, PowerPoint, Excel and Teams, among other applications. SSC recommended that each department planning to onboard to M365 complete its own PIA to identify risks and mitigation measures by taking into account its own infrastructure, data elements, workloads and tenant configuration. The SSC Enterprise DCC PIA will serve as a foundational piece in this task.

M365 is a powerful suite of applications that will help ACOA improve its collaboration and speed of communications across the organization and help it meet its growth and business objectives. It has many features and capabilities that will facilitate the Agency's transition to a digital organization that operates virtually anywhere anytime. This initiative focuses on transitioning ACOA's current Microsoft Office suite of products (Outlook, PowerPoint, Word and Excel) and its personal network drive from on-premise storage to cloud storage. The solutions ACOA is leveraging are Office 365 and One Drive for Business, both of which are Microsoft (MS) products. The solution will leverage a Software as a Service (SaaS) model. ACOA information will be stored and processed on data centres located in Canada.

MS Teams

- MS Teams becomes the heart of your interactions in M365 by providing chat, audio and video conference functions.
- A Teams virtual workspace means there is always a boardroom available for employees to meet, no matter where they are physically located.
- The chat function in Teams allows employees to quickly interact with others when an email is not required.

Exchange Online

- Cloud-based M365 synchronizes emails, calendars, tasks and contact information in Exchange Online across devices in real time, so it is up to date no matter what device is used. Scheduling is easy and hassle-free.
- Exchange Online helps employees collaborate on critical documents and gives them a focused inbox that prioritizes important messages and adapts to their work style so they can get more done – faster.

OneDrive

- OneDrive is M365's personal cloud storage platform, providing quick and easy access to files from any GC mobile or computing device.
- OneDrive makes email attachment size limitations obsolete. Through Teams or Outlook, employees can share a link to their document in OneDrive that allows colleagues to read or work on it while keeping it all saved in their personal drive.

Cloud / Security / Mobility

- M365's cloud-based tools allow employees to easily transition between GC mobile and computing devices and still access their documents and messages even when on the go.
- Cloud-based M365 provides world-class secure access from any GC mobile or computing device, which means employees can work on Protected B documents no matter where they are.

1.4 Assessment Objective

The objective of this PIA is to determine how ACOA's adoption of Microsoft Office 365 could affect the privacy of an individual. The PIA is a way for the Agency to state its commitment to protecting the privacy of individuals as it promotes transparency and accountability, and contributes to continued confidence in the way the Agency manages personal information.

1.5 Legal Authorities

Atlantic Canada Opportunities Agency Act

In accordance with the act, the object of the Agency is to support and promote opportunity for economic development in Atlantic Canada, with particular emphasis on small and medium-sized enterprises, through policy, program and project development and implementation and through advocacy of the interests of Atlantic Canada in national economic policy, program and project development and implementation. Its purpose is to increase opportunity for economic development in Atlantic Canada and, more particularly, to enhance the growth of earned incomes and employment opportunities in that region.

Financial Administration Act

The Agency is subject to the accountability regime set out in the FAA. ACOA is listed under Schedules I.1 and IV of the FAA.

1.6 Elements of Personal Information

Personal information banks (PIBs) are descriptions of personal information under the control of a government institution that is organized and retrievable by an individual's name or by a number, symbol or other element that identifies that individual. The personal information described in a PIB has been used, is being used or is available for an administrative purpose. The PIB describes how personal information is collected, used, disclosed, retained and/or disposed of in the administration of a government institution's program or activity. Standard PIBs describe information about members of the public as well as current and former federal employees contained in records created, collected and maintained by most government institutions in support of common internal services. This includes personal information relating to human resources management, travel, corporate communications and other administrative services. Standard PIBs are created by the Treasury Board of Canada Secretariat. A description of the following ACOA Standard PIBs is available in the Treasury Board Secretariat Info Source.

ACOA Standard PIBs Titles	Bank No.
Access to Information and Privacy	PSU 901
Accounts Payable	PSU 931
Accounts Receivable	PSU 932
Acquisition Cards	PSU 940
Applications for Employment	PSU 911
Attendance and Leave	PSE 903
Business Continuity Planning	PSU 903
Canadian Human Rights Act - Complaints	PSU 933
Discipline	PSE 911
Disclosure of Wrongdoing in the Workplace	PSU 906
Disclosure to Investigative Bodies	PSU 913
Electronic Network Monitoring Logs	PSU 905
Employee Assistance	PSE 916
Employee Performance Management Program	PSE 912
Employee Personnel Record	PSE 901
Employment Equity and Diversity	PSE 918
Executive Correspondence	PSU 902
Evaluation	PSU 942
EX Talent Management	PSU 934
Governor In Council Appointments	PSU 918
Grievances	PSE 910
Harassment	PSE 919
Hospitality	PSU 908
Human Resources Planning	PSE 935
Identification Cards and Access Badges	PSU 917
Internal Audit	PSU 941
Internal Communications	PSU 915
Library Services	PSU 936
Lobbying Act Requirements	PSU 937
Members of Boards, Committees and Councils	PSU 919
Occupational Health and Safety	PSE 907
Official Languages	PSE 906
Outreach Activities	PSU 938
Pay and Benefits	PSE 904

Personnel Security Screening	PSU 917
Professional Services Contracts	PSU 912
Public Communications	PSU 914
Real Property Management	PSU 948
Recognition Program	PSE 920
Relocation	PSU 910
Security Incidents and Privacy Breaches	PSU 939
Security Video Surveillance and Temporary Visitor Access Control Logs and Access Badges	PSU 907
Staffing	PSE 902
Training and Development	PSE 905
Travel	PSU 909
Values and Ethics Codes for the Public Sector and Organizational Code(s) of Conduct	PSE 915
Vehicle, Ship, Boat and Aircraft Accidents	PSE 908

Titles of ACOA-specific PIBs	**Bank No.**	**TBS Reg. No.**
• **Grants and Contributions**	**ACOA PPU 005**	**007070**

Description: This bank describes information collected in support of requests for grants and contributions from individuals, federal or provincial governments, organizations, corporations and municipalities and in records required to confirm that the recipient has respected the requirements of the contribution agreement. The personal information may include name, contact information, language preferences, biographical information, professional references, signature, financial information, date of birth, Social Insurance Number and photographs.

Class of individuals: Individuals, sole proprietors, partners in a business, government employees, employees of an organization, a corporation or a municipality.

Purpose: Personal information is collected to assess and process requests for funding in accordance with the *Atlantic Canada Opportunities Act* (ACOA Act) and the FAA. The Social Insurance Number (SIN) is collected in accordance with the *Income Tax Act.*

Consistent Uses: The names of successful applicants and selected relevant information are included in public records and published on the Agency's website in accordance with the Government of Canada's proactive disclosure practices. With consent, some personal information is published in ACOA success stories. Information may be used for internal audit, evaluation and reporting purposes.

Titles of ACOA-specific PIBs	Bank No.	TBS Reg. No.
• Peer Reviewers	ACOA PPU 111	20090345

***Description*:** This bank describes information collected from peer reviewers in support of scientific reviews of a proponent's project proposals for funding under the AIF. The personal information may include name, contact information, financial or contract information, language preference, biographical information, education, employment history, professional references, signature and SIN.

Class of Individuals: Individuals in specific scientific and innovative fields who perform peer reviews of scientific project proponents.

Purpose: The personal information is used to evaluate the credentials of peer reviewers required to review AIF proposals for project funding, to pay for their services when required and to maintain an inventory of such reviewers. The SIN is used for income tax purposes under the authority of the *Income Tax Act.*

***Consistent Uses*:** A list of peer reviewers is maintained for call-back purposes. Information may be shared with the Canada Revenue Agency (CRA); refer to CRA PPU 150 - Information Returns (Infodec) Databank. Information may also be used for evaluation and reporting to senior management.

1.7 Privacy Compliance Analysis (10 Privacy Principles)

While there are no changes to the 10 privacy principles, the location of storage and means to access has changed with the move to the cloud. It is important to note that Microsoft does not collect personal information other than employee data for user registration – information that ACOA will provide to them.

Principle 1: Accountability

ACOA is responsible for all personal information collected and used under the authority of the ACOA Act. The following internal policy instruments were developed to inform all employees of their responsibilities.

- **ACOA's Effective Privacy Practices** are to be followed by all ACOA employees involved in activities related to the creation, collection, retention, accuracy, use, disclosure or disposition of personal information under the control of ACOA, including the personal information of employees of the Agency.
- **ACOA's Privacy Protocol** serves to ensure that the collection, use or disclosure of personal information for *non-administrative purposes* is carried out in compliance with the *Privacy Act*, the Privacy Regulations and related privacy policy requirements of the Treasury Board Secretariat.
- **ACOA's Procedures to Address Privacy Breaches** outline the roles and responsibilities of Agency employees on the management of privacy breaches and the internal procedures and communications (including timing) for notifying the Office of the Privacy Commissioner, the Treasury Board Secretariat and other parties affected by the privacy breaches. It also deals with general requirements under sections 4 to 6 of the *Privacy Act* with respect to the collection, retention, use, disclosure and disposition of personal information.
- The Agency's **Managing Information – A Handbook for ACOA employees** lists the employees' role and responsibilities as it relates to the collection, use and management of information.

- Agency officials are required to complete a **Standard Government of Canada Briefing**. During a security briefing, individuals are informed of their security responsibilities under the *Policy on Government Security* and of the access permissions attached to their screening level. Security briefings provide an opportunity for people to ask questions and to develop a better understanding of these responsibilities. A security briefing formalizes the granting of the security status or clearance, as well as the individual's acceptance of and agreement to abide by the security responsibilities. Security briefings are conducted at various times: before an individual takes up his or her duties, when required based on the update cycle, and whenever a change occurs in screening level.

For the purpose of this initiative, the Chief Information Officer and the Director of Access to Information and Privacy are accountable for the organization's compliance with the following principles. Employees are accountable for following these policies and procedures to ensure that the organization remains compliant with the following principles.

Principle 2: Purpose

The Agency only collects personal information that is required to fulfill its mandate, as defined by the *ACOA Act,* and that it is legally authorized to collect.

Principle 3: Consent

The Agency uses privacy statements and Info Source to advise individuals of the information it collects, why it is collected, what the individual's rights are with regards to accessing and correcting this information, and to whom the information may be disclosed.

The Agency will inform employees by email regarding M365 and the move to cloud services. Externally, the Agency will post a notification on its website indicating that it is using cloud services to store some of its information.

Principle 4: Limiting Collection

ACOA's specific authority to collect information falls under the *ACOA Act*. Details on the collection of personal information are included in ACOA's standard and specific PIBs, which are listed below (after the 10 privacy principles).

Principle 5: Limiting Use, Disclosure and Retention

ACOA's **Network Access Policy and Directive** serves to ensure that authorized users will recognize the appropriate use of ACOA's electronic network.

- **Use**: Access to information is controlled through security clearances and a need to know, and the use is based on an employee's duties and the policies, protocols and standard operating procedures in place.
- **Disclosure**: ACOA will not disclose personal information without the consent of the individual unless it is legally authorized to do so in accordance with the *Privacy Act*.
- **Retention**: ACOA's retention and disposition schedules are mainly for its common administrative records. The retention rules for common administrative records are in line with the Generic Valuation Tools produced by Library and Archives Canada. Personal information held by the Agency will be retained for a minimum of 2 years after an administrative action has been completed.

Principle 6: Accuracy

ACOA's operational areas that handle personal information are responsible for ensuring the information is accurate, complete and up to date. In addition to the policy instruments developed by the Treasury Board Secretariat, the Agency has produced documents to assist employees in the use, identification and handling of personal information. They include:

- The Handbook on Managing Information
- The Privacy Protocol
- The Privacy Impact Assessment Handbook
- ACOA's Effective Privacy Practices

Principle 7: Safeguarding Personal Information

ACOA takes the necessary steps to safeguard personal information under its control. The Agency has a framework of policies, directives and procedures in place to protect personal information against loss, theft, unauthorized access or disclosure. ACOA also has a combination of mandatory and optional training opportunities to educate employees on their role and responsibilities in protecting personal information. The Agency employs physical, operational and technological measures to safeguard personal information.

- **Physical Safeguards:**

  The Directive on Security Management requires safeguards to be implemented to ensure the confidentiality of information while stored, processed or transmitted; the integrity of information and processes; the availability of the information and related systems and services, as well as the protection of staff and assets.

  - All employees, contractors and volunteers are screened to reliability status as a minimum.
  - Employees, contractors and visitors must wear their ID cards or access badges at all times.
  - Visitors are to be accompanied at all times when entering and exiting ACOA operational and security zones.
  - Physical information is stored in a locked cabinet appropriate for its security level.
  - Only employees with a need to know and the proper security screening can gain access to the information required to complete their job.
  - Disposal of sensitive paper information is carried out using approved RCMP shredders and/or contractors with the appropriate security screening and equipment to meet RCMP guidelines.

- **Technical Safeguards:**

  - ACOA's Information Technology Security Policy was developed to ensure that the Agency effectively manages its Information Technology (IT) Security activities and contributes to effective government-wide security management.
  - The Departmental Information Technology Security Directive establishes the minimum IT security control objectives that the Agency must achieve to ensure that its mandate, operations, priorities and security requirements are met.
  - The Agency also developed **Managing Information – A Handbook for ACOA employees**, which provides the basic elements employees need to know to carry out their responsibilities for managing information.

- Microsoft uses controls that are commensurate to the Canadian Centre for Cyber Security ITSG-33 publication. That document was developed to help government departments ensure security is considered right from the start. By following the principles within this document, ACOA helps ensure not only predictability and cost-effectiveness, but also that there are no hidden surprises preventing it from obtaining authority to operate and maintain continued authorization.
- Continuous monitoring of the safeguards will help ACOA ascertain how its internal guidelines, policies, etc. may need to be modified to better suit the changing environment.

Principle 8: Openness

ACOA proactively discloses information so that Canadians and Parliament are better able to hold the Agency accountable. Various Agency publications accessible to the public can be found on ACOA's website.

Principle 9: Individual Access

The *Privacy Act* provides the right of every individual to be given access to any personal information about that individual contained in a PIB, and any other personal information about that individual under the control of a government institution. Where personal information is used for administrative purposes, the individual is entitled to request correction of any error or omission.

The collection of personal information held by ACOA falls under the standard or ACOA-specific PIBs registered with the Treasury Board Secretariat (TBS). The description of standard PIBs registered by ACOA is available in the TBS's Info Source, on its Access to information and privacy web page. The Agency has registered 2 ACOA-specific PIBs related to its programs; a description is available in its own Info Source. The publication also provides a description of ACOA's programs and information holdings.

Individuals can request access or a correction to their personal information by contacting ACOA's Access to Information and Privacy Coordinator by phone at 506-871-2806 or by email to *atip-aiprp@acoa-apeca.gc.ca*.

Principle 10: Challenging Compliance

An individual is able to address a challenge concerning ACOA's compliance with these principles. Complaints may be addressed to ACOA's Access to Information and Privacy Coordinator by phone at 506-871-2806 or by email to *atip-aiprp@acoa-apeca.gc.ca*.

In addition, under the *Privacy Act*, individuals may file a formal complaint to the Office of the Privacy Commissioner of Canada if they think their personal information has been mishandled. Additional information is available on the Office of the Privacy Commissioner's Report a concern page.

1.8 Personal Information Flow Table

INSIDE THE MICROSOFT CLOUD			OUTSIDE THE MICROSOFT CLOUD			
ACOA EMPLOYEES - AT WORK - AT HOME - IN TRANSIT	ENCRYPTED 	ENCRYPTED (Office 365)	NOT ENCRYPTED 	EXTERNAL EMAIL SERVER	NOT ENCRYPTED 	EXTERNAL EMAIL USER

Inside the cloud:

- Emails (with or without attachments) to and from ACOA employees;
- Information contained in One Drive; and
- Back-up information.

Outside the cloud:

- Emails (with or without attachments) sent by ACOA employees to non-ACOA email accounts (employees can still encrypt the information using PKI if required); and
- Emails (with or without attachments) sent to ACOA employees from external parties.

2. Risk Area Identification and Categorization

2.1 Type of Activity	Risk level
Program or activity that does NOT involve a decision about an identifiable individual	☐ 1
Administration of Programs / Activity and Services	☒ 2
Compliance / Regulatory investigations and enforcement	☐ 3

2.2 Type of Personal Information Involved and Context	Risk level
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	☐ 1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	☐ 2
Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual.	☒ 3
Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.	☐ 4

2.3 Program or Activity Partners and Private-Sector Involvement	Risk level
- Within the institution (among 1 or more programs within the same institution)	☐ 1
- With other government institutions	☐ 2
- With other institutions or a combination of federal, provincial or territorial, and municipal governments	☐ 3
- Private-sector organizations, international organizations or foreign governments	☒ 4
Details: ACOA information will be stored and processed in Microsoft data centres located in Canada.	

2.4 Duration of the Program or Activity	Risk level
- One-time program or activity	☐ 1
- Short–term program or activity	☐ 2
- Long-term program or activity	☒ 3

2.5 Program Population	Risk level
- The program's use of personal information for internal administrative purposes affects certain employees.	☐ 1
- The program's use of personal information for internal administrative purposes affects all employees.	☐ 2
- The program's use of personal information for external administrative purposes affects certain individuals.	☐ 3

- The program's use of personal information for external administrative purposes affects all individuals.	☒ 4

2.6 Technology and Privacy	Privacy Risk
Does the new or modified program or activity involve the implementation of a new electronic system, software or application program, including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	☒ YES ☐ NO
Does the new or modified program or activity require any modifications to IT legacy systems and/or services?	☒ YES ☐ NO
The new or modified program or activity involves the implementation of 1 or more of the following technologies:	
Enhanced identification methods If yes, provide details:	☒YES ☐ NO
Use of Surveillance If yes, provide details:	☒YES ☐ NO
Use of automated personal information analysis, personal information matching and knowledge discovery techniques: (if yes, provide details)	☒YES ☐ NO
Details: • 2 factor authentication • Surveillance of IP address, geo-fencing, etc. • Protected information discovery and enhanced protection (e.g., SIN)	

2.7 Personal Information Transmission	Risk level
- The personal information is used within a closed system (i.e., no connections to the internet, intranet or any other system and the circulation of hard copy documents is controlled).	☐ 1
- The personal information is used in a system that has connections to at least 1 other system.	☐ 2
- The personal information is transferred to a portable device (e.g., USB key, diskette, laptop computer), transferred to a different medium or is printed.	☐ 3
- The personal information is transmitted using wireless technologies.	☒ 4
Details: M365 applications are offered via an online internet platform with data stored in a cloud environment located in Canada and hosted by Microsoft. Employees access only the information required to fulfill their responsibilities via protected corporate Wi-Fi or VPN and using ACOA-provided equipment.	

2.8 Privacy Breach Individual Impact	Yes	No
Potential risk that, in the event of a privacy breach, there will be an impact on the individual or employee.	☒	☐
Details: In the event of a privacy breach involving routine non-sensitive personal information, the impact on the affected individual(s) may be considered minimal. However, the impact may increase depending on the sensitivity of the personal information, resulting in embarrassment for the individual. The Agency has developed procedures to address privacy breaches.		

2.9 Privacy Breach Institution Impact	Yes	No
Potential risk that, in the event of a privacy breach, there will be an impact on the institution.	☒	☐
Details: In the event of a privacy breach involving routine non-sensitive personal information, the impact to the institution may be considered minimal. However, the impact may increase depending on the sensitivity of the personal information, resulting in embarrassment for the institution. The Agency has developed procedures to address privacy breaches.		

2.10 Risk Impact to the Agency	Risk level
Managerial harm Processes must be reviewed, tools must be changed, change in provider/partner.	☐ 1
Organizational harm Changes to the organizational structure, changes to the organization's decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	☐ 2
Financial harm Lawsuit, additional moneys required reallocation of financial resources.	☐ 3
Reputational harm, embarrassment, loss of credibility Decreased confidence by the public, elected officials under the spotlight, institution's strategic outcome compromised, or government priority compromised.	☒ 4

2.11 Risk Impact to the Individual or Employee	Risk Level
Inconvenience	☐ 1
Reputational harm, embarrassment	☐ 2
Financial harm	☒ 3
Physical harm	☐ 4

2.12 Example of Personal Information and its Path Outside ACOA

Description/Purpose	Type
Email received from client requesting service, providing feedback.	Collection
Email client back requesting more information, providing resolution, acknowledging receipt.	Disclosure
Service request transferred to service provider contracted by ACOA.	Disclosure and Use

Email received from service provider contracted by ACOA.	Collection
Email to external party as per legal and/or process requirements.	Disclosure and Use

2.13 Collection Notice

ACOA already has tools in place to advise individuals providing personal information about the purpose, legal authority, use, disclosure, consequences, right of access and correction, the PIB reference and the right to file a complaint for its collection.

The Agency will include a privacy statement for the move to cloud services. This statement will be available internally to employees and externally to the public. All initial questions related to its privacy statement will be directed to the Access to Information and Privacy Office.

2.14 Security of Personal Information

This PIA revolves around a cloud-based information system. Shared Services Canada is the custodian of the largest portion of the government's IT infrastructure. SSC works with departments and agencies to help prevent cyber threats and unwarranted intrusions by protecting and securing the integrity of the Government's networks and information. The full IT security component is done through a separate assessment called a Security Assessment and Authorization (SA&A). SSC supports ACOA through its SA&A service to ensure confidentiality, integrity and availability of its systems and data.

The Agency has its own security policies, directives and guidelines in addition to the TBS Policy on Government Security.

2.15 The Physical Security Measures Related to the Initiative

Microsoft Facility Security

- Perimeter Security: data centres have on-premise security staff around the clock. Buildings are nondescript and do not advertise that Microsoft Data Centre hosting services are provided at the location.
- Surveillance: data centres are monitored using motion sensors, video surveillance and security breach alarms.
- Physical access controls: multi-factor authentication is used, including biometric scanning, badging, badges and smart cards for data centre access.
- Computer rooms: rooms are equipped with two-factor access control biometric and card readers.
- Segregation: internal data centre network is segregated from the external network.
- Power: uninterruptable power supplies and diesel generators are present in the event of a power failure.
- Additional measures: role separation, demagnetization and physical destruction of faulty hard drives and physical destruction of decommissioned hard drives.

2.16 The Technical Security Measures Related to the Initiative

- Cloud service provider utilizes data isolation (within multi-tenant environment).
- Cloud provider uses logically partitioned systems using virtual local area networks (VLANs).

- Cloud service provider utilizes firewall, Network Address Translation, and IP filtering functions.
- Cloud service provider uses Network Intrusion Detection and Prevention.
- Cloud service provider performs scheduled operating system security patching.
- Cloud service provider offers multi-factor authentication for service access.
- Cloud service provider performs vulnerability scanning on servers hosting tenant data and perimeter devices.

2.17 Mitigating Access Controls

Microsoft will limit or restrict unauthorized access to personal information, including changes such as additions or deletions. It will ensure:

- separation of duties to render the location of specific client data unintelligible to the personnel who have physical access;
- policies and procedures enforce access controls on a "least privilege" basis for operational systems and subscriber/tenant data;
- staff sign confidentiality and non-disclosure agreements; and
- it uses Azure Active Directory for account provisioning, which is based on the tenant model and separates multi-tenants into discrete logical containers.

How individuals accessing personal information without authorization will be identified:

- Microsoft (Cloud Provider) and ACOA (Tenant) have well documented Incident Response and Management practices.
- Office 365 can be configured to comply with audit policies. This permits ACOA to log specific events, including viewing, editing and deleting content (e.g., email messages, documents, task lists, issues lists, discussion groups and calendars).

Further Information

ACOA does not provide access to personally identifiable information for research or statistical purposes.

None of ACOA's current PIBs are affected by this initiative. Personal information will continue to be created and/or collected as described within the Agency's specific PIBs and its standard PIBs.

Stakeholders

Name	Role	Contact information
Louise Doucet	Director-Coordinator Access to Information and Privacy	louise.doucet@acoa-apeca.gc.ca
Marc Gagnon	Director General Chief Information Officer Directorate	marc.gagnon@acoa-apeca.gc.ca