# Privacy Impact Assessment

## *Amazon Web Services (AWS) Canada* - PIA#

**Part 1 – General**

| | | | |
|---|---|---|---|
| Name of Department/Branch: | BCNET | | |
| PIA Drafter: | Hooper Access and Privacy Consulting Ltd. (Roseann Whitton) | | |
| Email: | rwhitton@hooperconsulting.ca<br>bev@hooperconsulting.ca | Phone: | 250-920-6331<br>250-896-4272 |
| Program Manager: | Dean Crawford | | |
| Email: | dean.crawford@bc.net | | 250-721-8477 |

### 1. Description of the Initiative

**BCNET** is taking the lead on the development of this Privacy Impact Assessment (PIA) on Amazon Web Services Canada (AWSC), on behalf of its members and affiliations.

BCNET is federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions (to include 25 publicly funded) made up of universities, colleges, institutes, and research organisations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing and IT services.

This unique, collaborative shared services model provides a multitude of benefits to its members from reducing and containing costs and increasing spending power, to decreasing duplication and improving service quality and productivity. The model cultivates a strong community, where members actively engage with peers to share, explore and develop innovative ideas and solutions as they tackle a broad spectrum of common and unique research and education technology challenges and topics. BCNET strives to add value to its membership by leveraging an advanced network that provides economies of scale to maximize efficiencies and drive down collective costs, while at the same time, continuing to facilitate collaborative innovative solutions that meet the needs of their stakeholders in support of world-class research and education.

A key component of facilitating innovative information technology (IT) solutions through this advanced network is ensuring they are hosted, accessed, managed and protected within a secure environment in accordance with Provincial (*Freedom of Information and Protection of Privacy Act*, FOIPPA) privacy laws, regulations and controls. The BCNET community has recently been advised by some of its members that effective immediately, applications that were previously hosted locally by service providers are now moving to AWS.

BCNET is committed to ensuring that the use of the AWS meets provincial privacy and security legislative requirements, policies and practices, and works with its members to strive to reduce the privacy risks associated with the legislative requirements accordingly. These privacy risks are managed through a combination of technical, administrative and physical controls that mitigate the associated risk. This privacy impact assessment (PIA) is intended to allow BCNET members who wish to either utilize applications hosted in AWS or to utilize AWS directly to proceed, and to ensure that these services are offered and provided in a way that is compliant with the *Freedom of Information and Protection of Privacy Act* (FIPPA).

This PIA does not speak to the contractual requirements and responsibilities of BCNET members in meeting their privacy obligations when entering into service agreements with AWS.

This PIA has been developed with a focus on the privacy protection and security measures deployed by AWS in the Canadian Cloud environment to identify and assess potential vulnerabilities to BCNET members and the community at large.

**Please note:**

***All the italicized information contained in this PIA was provided directly by AWS legal.***

***Amazon Web Services, Inc. (AWS)*** Section 14, Section 21

*http://aws.amazon.com/products/*. Section 14, Section 21

*** Please note:** For the purposes of this PIA, Customer as described by AWS = BCNET member.

AWS Canada (Central) Region, (data centers physically located within Canada), was launched in December of 2016 in response to the growth of the cloud computing business, and a rapidly expanding customer base within the country. As government, education, and non-profit organizations (public-sector) face unique challenges to accomplish complex mandates with limited resources, they are overwhelmingly turning to the power and speed of cloud computing technology/infrastructure to include AWS, to serve citizens more effectively, achieve scientific breakthroughs, and educate students etc. AWS offers flexible, low cost infrastructure computing. It allows organizations to focus on content and design versus managing IT infrastructure.

***Cloud vs On-Premises***

Section 14, Section 21

***Trade Capital Expense for Variable Expense.*** Section 14, Section 21

***Benefit from Massive Economies of Scale.*** Section 14, Section 21

***Increase Speed and Agility.*** Section 14, Section 21

***Stop Spending Money on Running and Maintaining Data Centers.*** Section 14, Section 21

Section 14, Section 21

***Stop Guessing at Capacity.*** Section 14, Section 21

Section 14, Section 21

It is the responsibility of all BCNET members to ensure that all data containing personal information is encrypted **prior** to transmission to AWS. AWS facilitates, manages, and controls only the infrastructure components of the host operating system in which the services operate.

AWS does not access, use or disclose personal information of any kind in providing their services.

Section 14, Section 21

*Customer Content*

Section 14, Section 21

*Account Information*

Section 14, Section 21

(*https://aws.amazon.com/privacy/*) Section 14, Section 21

Section 14, Section 21

2. **Scope of this PIA**

   This PIA covers the AWS Canada platform, its services, and operational controls as it relates to Privacy, Security, and Data protection in British Columbia.

3. **Related Privacy Impact Assessments**

   No other PIA's have been completed on this initiative.

4. **Elements of Information or Data**

   In this context the personal information (PI) is the PI that is required and provided directly from individuals to the members to participate in any BCNET member's activity or program, and then provided by the members to AWS.

   The collection of all personal information from the individual will continue to be the responsibility of the BCNET member (e.g. the provincial, public sector organization managing the application/operating system). Examples of personal information include: name, address, date of birth, phone no., gender etc. and may also include highly sensitive personal information as provided by the member to AWS. The BCNET member is also responsible for the secure transmission of the data from their operating system to AWS. AWS offers members strong encryption for content in transit or at rest, including the option to manage their own encryption keys.

**Part 2 – Protection of Personal Information**

5. **Storage or Access outside Canada**

Section 14, Section 21

# Section 14, Section 21

*AWS Canada*

Section 14, Section 21

AWS does provide backup services, but the customer has the option of arranging independent back-up services from an alternative service provider (inside or outside of Canada) for additional protection if they so choose.

BCNET members should deploy and store AWS services exclusively in the Canada (Central) region. The data will reside in discrete data centers on servers in Montreal, and at no time is it stored or accessed outside of Canada. Under these circumstances, all data transmitted between the BCNET advanced research network and AWS is within Canada only.

Data Residency (for data in transit)

Section 14, Section 21

Section 14, Section 21

(https://aws.amazon.com/directconnect/partners/#americas) Section 14, Section 21

AWS "Direct Connect" will allow BCNET members to establish a dedicated network connection between their network and one of the AWS Direct Connect locations solely within Canada. AWS Direct Connect locations provide access to AWS in the region the member chooses. You can establish connections in multiple regions, but a connection in one region does not provide connectivity to other regions. Selecting an AWS access point partner operating in the Canada Region ensures all data is transmitted exclusively within Canada and not routed through the U.S.

See appendix A for a list of Canadian APN Technology Partners available to assist in using the AWS Direct Connect service to establish network circuits between an AWS Direct Connect location and datacenters.

AWS does not move or replicate member content outside of the members chosen region(s), unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. In those circumstances U.S. law enforcement agencies requesting the release of information stored in Canada, under the Stored Communications Act must use recognized international processes, such as the Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters or through other similar cross-border assistance arrangements between these countries, to obtain valid and binding orders. Unless they are legally prevented from doing so, AWS practice is to notify members where practical before disclosing their content, so that they can seek protection from disclosure.

Disaster Recovery:

Section 21, Section 15(1)(l)

BCNET member support:

Basic, Developer, Business and Enterprise support plans are available to members based on their needs. Enterprise level members have direct access to a dedicated Technical Account manager (TAM) based inside or outside of Canada. BCNET members, who establish an AWS account, would automatically receive access to a "Basic Support" plan that provides 24x7x365 access to a highly personalized level of service from experienced technical support engineers from both within and outside of Canada. BCNET members have sole control and responsibility of what information they share with technical engineers when they contact them at that time as permitted under Section 33.1 of the Act.

Members can contact AWS Support via the Support Center. All Developer-level support members can open a case online with "Web Support" using a web browser. Business and Enterprise-level members may also "Click to Call" to have AWS contact them at any convenient phone number of strike up a conversation with and engineer via Chat.

## 6. Data-linking Initiative*

| | |
|---|---|
| **In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.** | |
| 1. Personal information from one database is linked or combined with personal information from another database; | No |
| 2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled; | N/A |
| 3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies. | N/A |
| **If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.** | |

## 7. Common or Integrated Program or Activity*

| | |
|---|---|
| **In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.** | |
| 1. This initiative involves a program or activity that provides a service (or services); | No |
| 2. Those services are provided through:<br>(a) a public body and at least one other public body or agency working collaboratively to provide that service; or<br>(b) one public body working on behalf of one or more other public bodies or agencies; | No |
| 3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation. | N/A |
| **Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.** | |

**8. Personal Information Flow Diagram and/or Personal Information Flow Table**

# Section 14, Section 21

- **AWS Responsibility***:* Section 14, Section 21
- **Customer/Partner Responsibility***:* Section 14, Section 21

## 9. Risk Mitigation Table

**NOTE:**

It should be noted that primary responsibility for the management and administration of any physical and/or technical security risks is born by any BCNET member choosing to deploy and utilize AWS. These privacy risks are managed through a combination of technical, administrative and physical controls that are designed and in place to mitigate each associated risk.

| Risk Mitigation Table | | | | |
|---|---|---|---|---|
| | **Risk** | **Mitigation Strategy** | **Likelihood** | **Impact** |
| 1. | Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes (within AWS) | Employee Code of conduct and Non-disclosure agreements; Use of Information & Technology Policies), password protected access, user access to system, based on need to know basis, permission restrictions, controls, and monitoring. | Low | High |
| 2. | BCNET member personal information data is compromised during transmission from the member to AWS | Section 15(1)(l) | Low | High |
| 3. | AWS Cloud Security Breach | AWS breach protocols are in place to reduce risks to client data in the event of a security breach | Low | High |

## 10. Collection Notice

The BCNET member is responsible for ensuring the appropriate collection notification (for the specific application/program) is in place prior to the collection of personal information and before transmission to AWS.

## Part 3 – Security of Personal Information

### 11. Please describe the physical security measures related to the initiative (if applicable).

BCNET members and their service providers are responsible at all times for ensuring the physical security of all data while in their custody and/or control (including all data at rest or in transit) and must meet all applicable physical security standards required by their organization.

**AWS:**

***Physical and Environmental Security***

Section 14, Section 21, Section 15(1)(l)

Section 21, Section 15(1)(l)

***Fire Detection and Suppression***

Section 14, Section 21, Section 15(1)(l)

***Power***

Section 14, Section 21, Section 15(1)(l)

***Climate and Temperature***

Section 14, Section 21, Section 15(1)(l)

***Management***

Section 14, Section 21

***Storage Device Decommissioning***

Section 14, Section 21, Section 15(1)(l)

**12. Please describe the technical security measures related to the initiative (if applicable).**

BCNET members and their service providers are responsible at all times for ensuring the technical security of all data while in their custody and/or control (including all data at rest or in transit) and must meet all applicable technical security standards required by their organization.

***AWS:***

Section 14, Section 21, Section 15(1)(l)

# Section 14, Section 21, Section 15(1)(l)

- ***Managed DDoS Protection:*** Section 14, Section 21, Section 15(1)(l)
- ***Secure Access:*** Section 14, Section 21, Section 15(1)(l)
- ***Built-In Firewalls:*** Section 14, Section 21, Section 15(1)(l)
- ***Unique Users:*** Section 14, Section 21, Section 15(1)(l)
- ***Multi-Factor Authentication (MFA):*** Section 14, Section 21, Section 15(1)(l)
- ***Private Subnets:*** Section 14, Section 21, Section 15(1)(l)
- ***Encrypted Data Storage:*** Section 14, Section 21, Section 15(1)(l)

- ***Dedicated Connection Option:*** Section 14, Section 21, Section 15(1)(l)

- ***Dedicated, Hardware-Based Crypto Key Storage Option:*** Section 14, Section 21, Section 15(1)(l)

- ***Centralized Key Management:*** Section 14, Section 21, Section 15(1)(l)

- ***Perfect Forward Secrecy:*** Section 14, Section 21, Section 15(1)(l)

# Section 14, Section 21, Section 15(1)(l)

- ***AWS Personal Health Dashboard:*** Section 14, Section 21, Section 15(1)(l)

- ***AWS Trusted Advisor:*** Section 14, Section 21, Section 15(1)(l)

- ***Amazon CloudWatch:*** Section 14, Section 21, Section 15(1)(l)

- ***AWS CloudTrail:*** Section 14, Section 21, Section 15(1)(l)

- ***AWS Config:*** Section 14, Section 21, Section 15(1)(l)

- ***Amazon Inspector*** Section 14, Section 21, Section 15(1)(l)

***AWS Organizations:*** Section 14, Section 21, Section 15(1)(l)

AWS has implemented various methods of external communication to support BCNET members, their services providers and community. Mechanisms are in place to allow the BCNET member support team to be notified of operational issues that impact the BCNET member experience such as a security incident or security breach. The "Service Health Dashboard" note above is available and would be maintained by the AWS BCNET member support team to alert them of any issues. AWS would notify BCNET members of a security breach in accordance with the specific terms outlined in their service agreement with AWS. BCNET members are responsible for updating their AWS accounts with their correct Security Team contact information. AWS works with the BCNET member and the Security Team identified in their AWS accounts.

In addition, AWS maintains the AWS security bulletin webpage to notify BCNET members of security and privacy events affecting services. Members can subscribe to the Security Bulletin RSS Feed to keep abreast of security announcements on the Security Bulletin webpage. The BCNET member support team maintains a Service Health Dashboard webpage to alert members to any broadly impacting availability issues. The BCNET member is responsible for reporting incidents involving customer storage, virtual machines, and applications, unless the incident is caused by AWS.

Section 14, Section 21

Section 14, Section 21

**13. Does your branch/department rely on any security policies?**

BCNET members and their service providers are responsible for the deployment, dissemination and administration of all organizational security policies etc. as it relates to the handling and management of personal information in their custody and/or control.

**AWS Compliance**

Section 14, Section 21, Section 15(1)(l)

Section 14, Section 21, Section 15(1)(l)

Section 14, Section 21

(https://aws.amazon.com/compliance/).

**14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.**

BCNET members and their service providers are responsible for the strict management and administration of user access based on a "need to know" basis only including maintenance and enforcement.

**AWS** - cannot access or alter personal information in any way.

**15. Please describe how you track who has access to the personal information.**

BCNET members and their service providers are responsible for ensuring that access to all personal information in their custody and/or control is controlled, monitored, and reviewed/audited on a regular basis.

**AWS**

AWS does not have access to BCNET member personal data unless required under section 33.1 of the Act.

Section 14, Section 21, Section 15(1)(l)

**Part 4 – Accuracy/Correction/Retention of Personal Information**

**16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**

**AWS** - cannot alter personal information in any way.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    **No**

18. **If you answered "yes" to question 18, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    **N/A**

19. **If you answered "yes" to question 17, do you have records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

    **N/A**

**Part 5 – Further Information**

20. **Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

    **No**

21. **Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.**

    **No**

22. **Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.**

    **No**

## Part 6 – Sign Off

**BCNET Program Manager**

| | | |
|---|---|---|
| Dean Crawford<br>Manager, Shared Systems & Technology<br>BCNET | Signature | Date |

**Signed on behalf of Amazon Web Services**

| | | |
|---|---|---|
| XXXXXXXXXXX<br>XXXXXXXXXXX<br>Amazon Web Services | Signature | Date |

**Head of BCNET**

| | | |
|---|---|---|
| Bala Kathiresan<br>President & Chief Executive Officer<br>BCNET | Signature | Date |

A final copy of this PIA (with all signatures) must be kept on record.