BCNET

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 bev@hooperconsulting.ca	Phone:	250-920-6331 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) *is an Information Technology & Services company headquartered in Seattle, WA, USA. AWS offers a broad set of global compute, storage, database, analytics, application, and deployment services, all of which are listed at http://aws.amazon.com/products/. All of these services are hosted within their global data center footprint that allows customers to consume services without having to build or manage facilities or equipment. Using AWS, customers can requisition compute power, storage, and other services in minutes. Tens of thousands of government agencies, education institutions, and nonprofit organizations around the world use AWS. Customers pay only for what they use, with no upfront expenses or long-term commitments, making AWS a cost-effective way to deliver applications.*

* **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

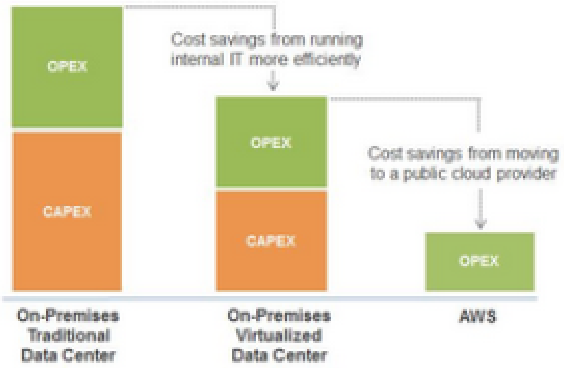
Cloud computing allows customers to focus on projects that differentiate their organization, free from the burden of data center investments and IT infrastructure operations. Below are some of the key benefits of AWS's cloud platform over on-premises IT solutions.

Trade Capital Expense for Variable Expense. *Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can use cloud computing and only pay for the resources you consume.*

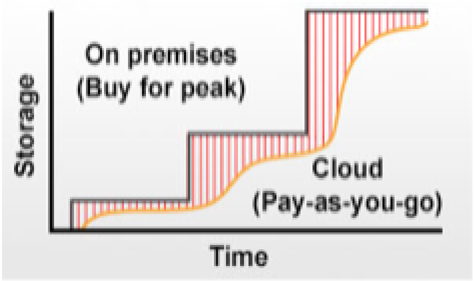
Benefit from Massive Economies of Scale. *By using cloud computing, you can achieve a low variable cost. Because usage from millions of active customers every month is aggregated in the cloud, cloud computing providers such as AWS can achieve higher economies of scale, which translates into lower, pay-as-you-go prices.*

Increase Speed and Agility. *In a cloud computing environment, new IT resources are only ever a click away, reducing the time it takes to make those resources available to customers from weeks to just minutes. This results in an increase in agility for the organization, since the cost and time it takes to experiment and develop is likely to be significantly lower.*

Stop Spending Money on Running and Maintaining Data Centers. *Focus on projects that are core to an organization, not the infrastructure. As shown in **Figure 4**, cloud computing lets you move from a CapEx model to an OpEx model, letting you focus resources on customers rather than on the heavy lifting of racking, stacking, and powering servers.*



Stop Guessing at Capacity. *Eliminate guessing at your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. As illustrated in **Figure 5**, with cloud computing these problems are minimized. You can access as much or as little as you need and scale up and down as required within minutes.*



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.

AWS treats all Customer content and associated assets as Critical information. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used, archived and protected from disclosure.

AWS does not access customer data, and customers are given the choice as to how they store, manage, and protect their data. There are four important basics regarding data ownership and management in the shared responsibility model:

1) *Customers continue to own their data.*
2) *Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.*
3) *Customers can download or delete their data whenever they like.*
4) *Customers should consider the sensitivity of their data and decide if and how to encrypt the data while it is in transit and at rest.*

AWS does not access or use member content for any purpose other than as legally required and for maintaining the AWS services and providing them to members and their end users. AWS does not use member content or derive information from it for marketing or advertising.

AWS classifies customer data into two categories: customer content and account information.

Customer Content

Defined as software (including machine images), data, text, audio, video, or images that a customer or any end user transfers to us for processing, storage, or hosting by AWS services in connection with that customer's account and any computational results that a customer or any end user derives from the foregoing through their use of AWS services. For example, customer content includes content that a customer or any end user stores in Amazon Simple Storage Service. Customer content does not include account information, which they describe below. The terms of the AWS Customer Agreement or other agreement with them governing the use of AWS services apply to your customer content.

Account Information

Defined as information about a customer that a customer provides to AWS in connection with the creation or administration of a customer account.

For example, account information includes names, usernames, phone numbers, email addresses, and billing information associated with a customer account. The information practices described in the AWS Privacy Notice (https://aws.amazon.com/privacy/) apply to account information.

Customers maintain ownership of their customer content and select which AWS services process, store, and host their customer content. AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to their customers and their end users. They never use customer content or derive information from it for marketing or advertising.

AWS customers:

Determine where their customer content will be stored, including the type of storage and geographic region of that storage.

Choose the secured state of their customer content. AWS offer customers strong encryption for customer content in transit or at rest, and they provide customers with the option to manage their own encryption keys.

Manage access to their customer content and AWS services and resources through users, groups, permissions and credentials that customers control.

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.

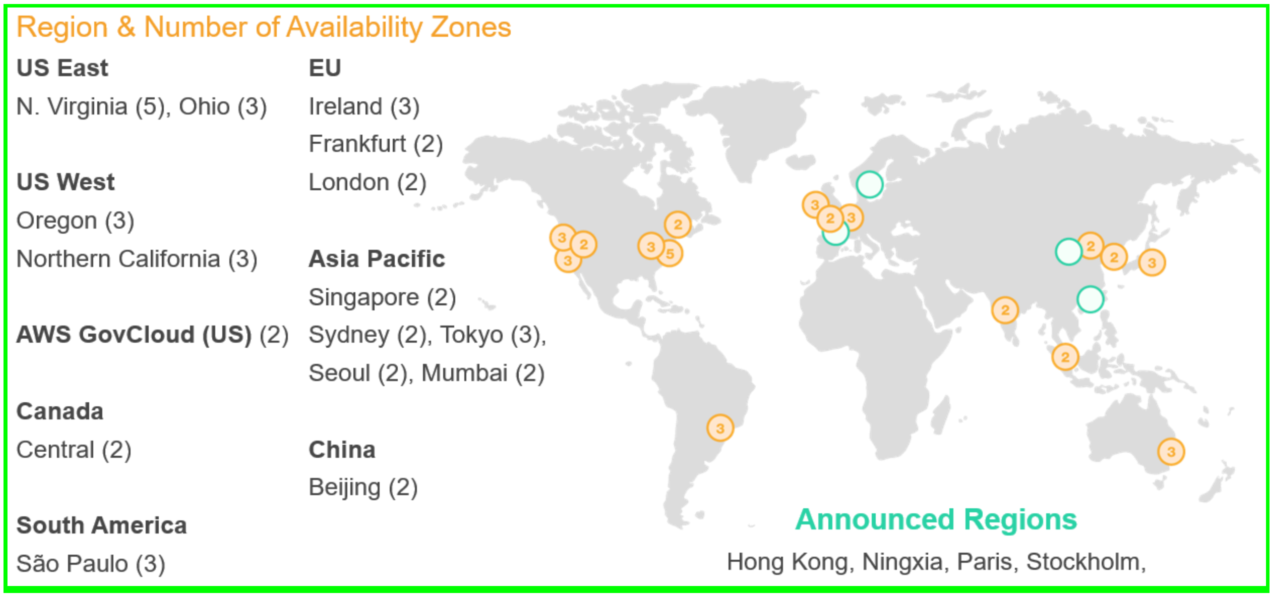
<u>Part 2 – Protection of Personal Information</u>

5. **Storage or Access outside Canada**

The AWS Cloud infrastructure is built around regions and Availability Zones. A region is a physical location in the world where they have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer members the ability to operate *production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.*

AWS currently has 16 regions and 43 Availability Zones throughout the world. Information on each region can be found at the [AWS Global Infrastructure](#) webpage.

***Figure 2** depicts the current AWS Regions and Availability Zones, along with four new regions that are coming online throughout the next year.*



Region & Number of Availability Zones

US East
N. Virginia (5), Ohio (3)

US West
Oregon (3)
Northern California (3)

AWS GovCloud (US) (2)

Canada
Central (2)

South America
São Paulo (3)

EU
Ireland (3)
Frankfurt (2)
London (2)

Asia Pacific
Singapore (2)
Sydney (2), Tokyo (3),
Seoul (2), Mumbai (2)

China
Beijing (2)

Announced Regions
Hong Kong, Ningxia, Paris, Stockholm,

Figure 2 – Global Map of AWS Regions and Availability Zones

***Figure 3** illustrates the relationship between regions and Availability Zones.*

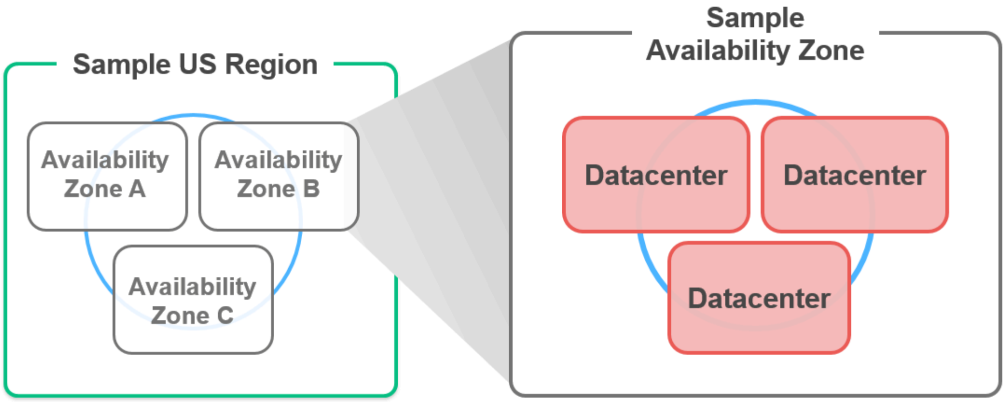


Figure 3 – Regions and Availability Zones

AWS Canada

Customers can run their applications and workloads in the Canada (Central) Region with 2 availability zones. As of July 2017, there are tens of thousands of active Canadian AWS customers.

Customers choose the region(s) in which their customer content will be stored, allowing them to deploy AWS services in the location(s) of their choice, in accordance with their specific geographic requirements. For example, an AWS customer in Canada can choose to deploy its AWS services exclusively in the Canada (Central) region and store its content onshore in Canada. If the customer makes this choice, its customer content will be located in Canada. AWS customers retain control and ownership of their content and it is the customer's responsibility to manage their data backup plans.

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)

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. With Direct Connect, you bypass Internet service providers in your network path. The new Canada Region is currently available for multiple services, including AWS Direct Connect.

The APN Technology and Consulting Partners (formerly called AWS Direct Connect Solution Providers) listed on this page (https://aws.amazon.com/directconnect/partners/#americas) can assist you in using the AWS Direct Connect service by helping you establish network circuits between an AWS Direct Connect location and your datacenter, office, or colocation environment, or assist you in constructing a hybrid environment

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:

The Central Canada Region is not a single data centre, but multiple data centres organized in what AWS calls Availability Zones (AZ's). Each AZ has an isolated grid power, fibre connectivity and is on a different floodplain and within 20K radius of on another. Each AZ can contain more than one data centre, Montreal has 2. Best practice supports using multiple zones within a region in your deployment.

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*

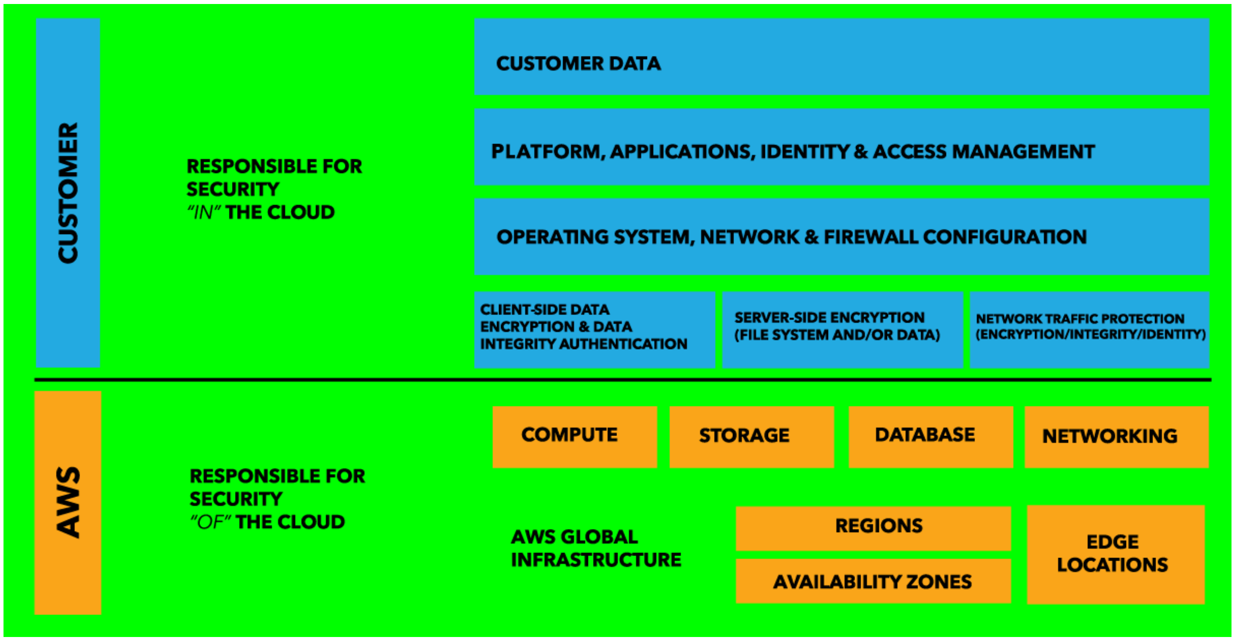
In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must 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: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (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

As cloud computing customers are building systems on top of cloud infrastructure, the security and compliance responsibilities are shared between the Cloud Service Provider (CSP) and cloud customers. In an Infrastructure as a Service (IaaS) model, customers control how they architect and secure their applications and data put on the infrastructure, while CSPs are responsible for providing services on a highly secure and controlled platform and providing a wide array of additional security features. The level of CSP and customer responsibilities in this shared responsibility model depends on the cloud deployment model (see the NIST Definition of Cloud Computing models). Customers should be clear as to their responsibilities in each model. AWS's shared responsibility/security model is depicted in the figure below.


CUSTOMER
RESPONSIBLE FOR SECURITY "IN" THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

- **AWS Responsibility**: *AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.*
- **Customer/Partner Responsibility**: *Customers/partners assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, configuration of the AWS-provided security group firewalls, and other security, change management, and logging features.*

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	Transmission is encrypted with 256 bit AES encryption and over a secure line. Encryption keys managed by BCNET members.	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.

<u>Part 3 – Security of Personal Information</u>

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

AWS's data centers are state of the art, using innovative architectural and engineering approaches. AWS has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities.

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges.

When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

AWS does not disclose the exact location of data centers and does not allow data center access to customers as this exposes a wide range of customers to physical access of a third party. Instead of allowing customers to perform physical audits, AWS has an independent third party perform audits of its data centers. These audits are conducted in accordance with the Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. The auditors produce a Service Organization Controls 1 (SOC 1), Type 2 report in connection with the audit. Independent reviews of data center physical security are also part of an ISO 27001 audit, a Payment Card Industry (PCI) Data Security Standard (DSS) assessment, and an International Traffic in Arms Regulations (ITAR) audit.

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning

As part of AWS's storage decommissioning process, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

AWS will provide the SOC 1 report to customers under NDA. The AWS Security Center provides up-to-date information on AWS audits by independent third-party auditors.

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:

With the AWS Cloud, not only are infrastructure headaches removed, but so are many of the security issues that come with them. AWS's highly secure data centers use state-of-the-art electronic surveillance and multi-factor access control systems and maintain strict, least-privileged-based access authorizations. Our environmental systems are designed to minimize the impact of disruptions to operations, and our multiple geographic regions and Availability Zones allow customers to remain resilient in the face of most failure modes, including natural disasters or system failures. AWS manages over 1,800 security controls to provide an optimally secure environment for all of our customers.

In addition, network traffic between AWS Regions, Availability Zones, and individual data centers travels over private network segments by default. These private network segments are fully isolated from the public Internet and not routable externally. AWS resources can be configured to reside only on isolated AWS network segments and to avoid utilizing any public IP addresses or routing over the public Internet.

AWS security engineers and solution architects have developed whitepapers and operational checklists to help customers select the best options for their needs and to recommend security best practices, *such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.*

Not only are applications and data protected by highly secure facilities and infrastructure, they are also protected by extensive network and security monitoring systems. AWS and its partners offer over 700 tools and features to help customers meet their security objectives concerning visibility, auditability, controllability, and agility.
These tools and features provide basic but important security measures such as Distributed Denial of Service (DDoS) protection and password brute-force detection on AWS accounts.

AWS-provided security features include:

- ***Managed DDoS Protection:*** *AWS Shield is a managed DDoS protection service that provides always-on detection and automatic inline mitigations that minimize downtime and latency. With two tiers to choose from—Standard and Advanced—customers can protect multiple layers of their web applications against DDoS attacks.*

- ***Secure Access:*** *Customer access points, also called Application Programming Interface (API) endpoints, allow secure HTTP access (HTTPS) so that customers can establish secure communication sessions with their AWS Cloud services using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).*

- ***Built-In Firewalls:*** *Customers can control how accessible their instances are by configuring built-in firewall rules—from totally public to completely private or somewhere in between. And when instances reside within an Amazon Virtual Private Cloud (Amazon VPC) subnet, customers can control egress as well as ingress.*

- ***Unique Users:*** *The AWS Identity and Access Management (IAM) tool allows AWS customers to control the level of access their own users have to AWS infrastructure services. With IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.*

- ***Multi-Factor Authentication (MFA):*** *AWS provides built-in support for MFA for use with AWS accounts as well as individual IAM user accounts.*

- ***Private Subnets:*** *The Amazon VPC service allows customers to add another layer of network security to instances by creating private subnets and even adding an Internet Protocol Security (IPsec) Virtual Private Network (VPN) tunnel between a home network and Amazon VPC.*

- ***Encrypted Data Storage:*** *Customers can have the data and objects they store in Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon Redshift, and Amazon Relational Database Service (Amazon RDS) on Oracle and SQL Server encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.*

- ***Dedicated Connection Option:*** *The AWS Direct Connect service allows customers to establish a dedicated network connection from their premises to AWS. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable access to both public and private IP environments within the AWS Cloud.*

- ***Dedicated, Hardware-Based Crypto Key Storage Option:*** *For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.*

- ***Centralized Key Management:*** *For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service (KMS) provides a convenient management option for creating and administering the keys used to encrypt data at rest.*

- ***Perfect Forward Secrecy:*** *For even greater communication privacy, several AWS Cloud services such as Elastic Load Balancing and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use perfect forward secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.*

Several of AWS's built-in cloud security features focus on providing visibility into data, performance, and resource usage. The tools listed below help customers gain more insight into their cloud operations, giving them the means to better control their security and providing information for data-driven decisions.

- ***AWS Personal Health Dashboard:*** *AWS Personal Health Dashboard provides a personalized view into the performance and availability of the AWS services you are using, as well as alerts that are automatically triggered by changes in the health of those services. In addition to event-based alerts, Personal Health Dashboard provides proactive notifications of scheduled activities, such as any changes to the infrastructure powering your resources, enabling you to better plan for events that may affect you.*

- ***AWS Trusted Advisor:*** *Provided automatically when AWS customers sign up for AWS Support, the AWS Trusted Advisor service is a convenient way for customers to see where they could use a little more security. It monitors AWS resources and alerts customers to security configuration gaps such as overly permissive access to certain Amazon Elastic Compute Cloud (Amazon EC2) instance ports and Amazon S3 storage buckets, minimal use of role segregation using AWS IAM, and weak password policies.*

- ***Amazon CloudWatch:*** *Amazon CloudWatch enables customers to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by a customer's applications and services and any log files their applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly.*

- ***AWS CloudTrail:*** *AWS CloudTrail provides logs of all user activity within an AWS account. The recorded information includes the identity of the API caller, the time of the API call, the source IP* *address of the API caller, the request parameters, and the response elements returned by the AWS Cloud service. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.*

- ***AWS Config:*** *With the AWS Config service, customers can immediately discover all of their AWS resources and view the configuration of each. Customers can receive notifications each time a configuration changes as well as dig into the configuration history to perform incident analysis.*

- ***Amazon Inspector:*** *Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices.*

After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

AWS Organizations: *AWS Organizations allows you to create groups of AWS accounts that you can use to more easily manage security and automation settings. With AWS Organizations, you can centrally manage multiple accounts to help you scale. You can control which AWS Cloud services are available to individual accounts, automate new account creation, and simplify billing.*

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.

AWS' commitment to all AWS customers is as follows:

> *If AWS becomes aware of any unlawful or unauthorized access to any Customer Data (i.e. any personal data that is uploaded to Customer's AWS account) on AWS's equipment or in AWS's facilities and this unlawful or unauthorized access results in loss, disclosure or alteration of Customer Data, AWS will promptly notify the Customer and take reasonable steps to reduce the effects of this security incident.*
>
> *AWS defines, administers and monitors security for the underlying cloud infrastructure (i.e. the hardware, the facilities housing the hardware and the network infrastructure).*
>
> *Because AWS manages the infrastructure and the security controls that apply to it, AWS can:*

(a) Identify potential incidents affecting the infrastructure;
(b) Determine if any access to Customer Data resulted from that incident; and
(c) Determine if that access was actually unlawful or unauthorized i.e. it would be unauthorized if it was in breach of AWS' Security Policies.

If an incident happens within AWS' sphere of knowledge and control and this incident results in loss, disclosure or alteration of Customer Content, AWS will promptly notify the Customer. AWS does this regardless of whether the Customer's Content is sensitive or not, because AWS does not know what the Customer Content is and protects all Customer Content in the same robust way.

The AWS ISO 27017 16.1.1 and 16.1.2 requirements validate that AWS maintains breach notification obligations and has processes and procedures in place to notify you in the event of a breach.

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

The AWS Cloud infrastructure has been designed and is managed in alignment with regulations, standards, and best practices, including:

Federal Risk and Authorization Management Program (FedRAMP)
Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
SOC 2
SOC 3
Payment Card Industry Data Security Standard (PCI DSS)
International Organization for Standardization (ISO) 27001
ISO 27017
ISO 27018
ISO 9001
Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2 and 4
Federal Information Security Management Act (FISMA)
US Health Insurance Portability and Accountability Act (HIPAA)
FBI Criminal Justice Information Services (CJIS)
National Institute of Standards and Technology (NIST) 800-171
International Traffic in Arms Regulations (ITAR)
Federal Information Processing Standard (FIPS) 140-2
Family Educational Rights and Privacy Act (FERPA)
Information Security Registered Assessors Program (IRAP) (Australia)
IT-Grundschutz (Germany)

For information on all of the security regulations and standards with which AWS complies, visit the AWS Compliance page (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.

The AWS Identity and Access Management (IAM) tool allows AWS BCNET members to control the level of access their own users have to AWS infrastructure services. With IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.

AWS CloudTrail provides logs of all user activity within an AWS account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS Cloud service. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

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 Manager, Shared Systems & Technology BCNET	Signature	Date

Signed on behalf of Amazon Web Services

XXXXXXXXXXXX XXXXXXXXXXX Amazon Web Services	Signature	Date

Head of BCNET

Bala Kathiresan President & Chief Executive Officer BCNET	Signature	Date

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