



Privacy Impact Assessment

Microsoft Azure PIA#

Part 1 – General

Name of Organization	BCNET		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd.		
Email:	bev@hooperconsulting.ca	Phone:	250 896-4272
Program Manager:	Dean Crawford		
Email:	Dean.crawford@bc.net	Phone:	250 721-8477

1. Description of the Initiative

BCNET is taking the lead on the development of this Privacy Impact Assessment (PIA) of Microsoft Azure (Azure) on behalf of its members and affiliations.

BCNET is a federally incorporated not-for profit, services information technology organization that represents the interests of 43 member (to include 25 publicly funded) institutions made up of universities, colleges, institutes, and research institutes 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 and 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.

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 Azure, to serve citizens more effectively, achieve scientific breakthroughs, and educate students etc.



Privacy Impact Assessment

Microsoft Azure PIA#

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 that effective immediately, applications that were previously hosted locally by service providers may now be moving to Azure.

BCNET is committed to ensuring that the use of Azure 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 utilize applications hosted by Azure 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).

Azure is a growing collection of integrated cloud services that developers and IT professionals use to build, deploy, and manage applications through a global network of data centres. Azure is available in 140 countries divided into 42 regions. Azure has two regions in Canada with data centres in Canada Central (Toronto) and Canada East (Quebec City).

Azure is a public cloud service operating at a Hyperscale level. Hyperscale cloud computing is a concept that involves computing resources capable of increasing size rapidly, efficiently and indefinitely with a high degree of automation.

Members can choose from a series of services to develop new, or run existing applications while using features and computing resources associated with cloud-based services. The various offerings under the Azure umbrella allow members to operate in their own 'space' on the cloud but at the same time, interact with other on-premises or cloud applications.

Azure provides both Platform-as-a-Service ("PaaS") and Infrastructure-as-a-service ("IaaS") as well as support for a variety of programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems. When a PaaS offering is used by a member it allows control of applications (and possibly configuration settings), but not management or control of the network, servers, operating systems or storage. When an IaaS offering is used, it allows the member to control and deploy the operating system, storage and applications. It also allows limited control of some network components (eg. Host Firewalls).

IaaS has three components: Compute, Storage and Networking. PaaS has seven components: Compute, Web & Mobile, Developer Services, Data, Analytics & IoT, Storage and Networking.



Privacy Impact Assessment

Microsoft Azure PIA#

Additional information regarding the Microsoft Azure platform and its services may be found at:

<https://azure.microsoft.com/en-ca/>.

<https://azure.microsoft.com/en-ca/regions/services/>

2. Scope of this PIA

This PIA has been developed with a focus on the privacy protection and security measures deployed by Microsoft Azure in the Canadian Cloud environment to identify and assess potential vulnerabilities to BCNET members and the community at large. This PIA focuses on the information BCNET members provide to enable their subscriptions to Azure IaaS and PaaS services. As Members have full control of the data and applications that they host within their Azure subscriptions, those uses are outside of the scope of this PIA. Azure Active Directory contains subscription information (business contact) for the members only.

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 Microsoft Azure.

3. Related Privacy Impact Assessments

A comprehensive Foundational PIA (December 2016) has also been completed on this initiative which focuses on the project in detail from a nationwide perspective by Microsoft.

4. Elements of Information or Data

Administration data (business contact information only) will only be provided by the members to Microsoft Azure.

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. The management, collection and control of all personal information from the individual will continue to be the responsibility of the BCNET member (the provincial or public-sector organization managing the application /operating system). Examples of personal information include: name, address, date of birth, phone no., gender etc.

Microsoft has no access to member's virtual machines and/or data at anytime in Azure.



Privacy Impact Assessment

Microsoft Azure PIA#

5. Storage or Access outside Canada

Section 21, Section 15(1)(I)



Privacy Impact Assessment

Microsoft Azure PIA#

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;	NA
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.	NA
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



Privacy Impact Assessment

Microsoft Azure PIA#

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

See <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios>.

9. Risk Mitigation Table

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 the Azure environment)	Employee Code of conduct and non-disclosure agreements; password-protected access, user access based on need to know, permission restrictions, role based access controls, Just In time administration, time bound administration and monitoring.	Low	High
2.	BCNET member personal information data is compromised during transmission from the member to Azure	Microsoft employs breach strategies and remediation protocols.	Low	High
3.	Azure Cloud security breach			

Section 15(1)(I)



Privacy Impact Assessment

Microsoft Azure PIA#

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 Azure.

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 data at rest and in transit) and must meet all the applicable physical security standards required by their organization.

Azure:

Section 21, Section 15(1)(I)

<https://aka.ms/MCSCE>

**Microsoft notes that security is a shared responsibility. “Who is responsible for what (in terms of security) depends on the cloud service model you use. With IaaS, the cloud service provider is responsible for the core infrastructure security, which includes storage, networking and compute (at least at the fabric level – the physical level).”*



Privacy Impact Assessment

Microsoft Azure PIA#

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 data at rest and in transit) and must meet all the applicable physical security standards required by their organization.

Azure:

Section 21, Section 15(1)(I)

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.

Azure:

<https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx>

<https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx>



Privacy Impact Assessment

Microsoft Azure PIA#

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 need to know including the maintenance and enforcement.

Azure:

Section 21, Section 15(1)(I)

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.

Azure:

Section 21, Section 15(1)(I)



Privacy Impact Assessment

Microsoft Azure PIA#

Section 21, Section 15(1)(I)

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?

BCNET members are responsible for providing personal information updates to Azure via data transfer (Microsoft has a formal process to allow a member to correct/amend inaccurate personal information as appropriate in compliance with ISO 27018).

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 17, 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 a 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



Privacy Impact Assessment

Microsoft Azure PIA#

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.



Privacy Impact Assessment

Microsoft Azure PIA#

Signed on Behalf of BCNET:

A handwritten signature in blue ink that reads 'Bala'.

Digitally signed by Bala Kathiresan
DN: cn=Bala Kathiresan, o=BCNET,
ou=President & CEO,
email=bala.kathiresan@bc.net, c=CA
Date: 2018.03.28 16:57:45 -07'00'

Bala Kathiresan
President and Chief Executive
Officer
BCNET

Signature