Privacy Impact Assessment

EduCloud

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 EduCloud Server (EduCloud), 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.

BCNET is committed to ensuring that the ongoing deployment of EduCloud Server continues to meet 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 support the ongoing use of EduCloud Server by its members, and to ensure that this cloud-based service is offered and provided in a way that allows BCNET users to continue to be 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 and BCNET members that are addressed within the EduCloud Service Addendum.

Government, education, and non-profit organizations (public sector) continually face unique challenges to accomplish complex mandates with limited resources, as a result they are overwhelmingly turning to the power and speed of cloud computing technology/infrastructure. EduCloud offers flexible, low cost infrastructure computing that enables the BC higher education community of practice to focus on content and design versus managing IT infrastructure.

EduCloud Server is an infrastructure as a service (IaaS) cloud-based platform that was established based on the concept of supporting the entire "higher education of BC community of practice". It sits on top of the BCNET network and is the foundational service linked to the delivery of all BCNET member programs and services activities. Its tied to everything they do. Designed and developed by the University of British Columbia (UBC), and, in partnership with BCNET, EduCloud was launched in May of 2015 in response to:

- the growth in cloud computing business;
- the increase in size of the BCNET community at large;
- the prohibitive cost of other major cloud service providers.

EduCloud is a software solution that allows higher education IT organizations to build secure, multi-tenant private clouds by pooling infrastructure resources into virtual datacentres. These virtual data centres are provided through web-based portals and programmatic interfaces as fully automated, catalogue-based services.

EduCloud is built on the technology of VMware, the industry-leading server virtualization vendor. By building secure and cost-effective private clouds utilizing EduCloud's VMware technology, the organization can simplify the delivery of services, innovate and improve agility, increase IT efficiency and enhance security. EduCloud provides the ability to leverage existing investments and the flexibility to extend capacity between clouds.

EduCloud Server (IaaS) delivers resources to internal users as virtual datacentres. By pooling storage and networking capacity into virtual datacentres, EduCloud supports managing existing resources more efficiently with complete abstraction between consumption and delivery of services. EduCloud delivers isolated virtual datacentres that draw resources from a common physical infrastructure (BCNET network). By pooling these physical resources on the back end, hardware utilization and consolidation increases. Similarly, underlying infrastructure can be pooled into tiers and offered to end users at distinct service levels and prices.

EduCloud Server changes the way end users consume IT services. The EduCloud self-service web portal enables simplified, self-managed access allowing members to manage their own virtual datacentres. Members can maintain control with permissions, quotas and leases governed by role-based access controls that use the existing AD and LDAP directory services.

EduCloud Dashboards are also part of the service. It is a web application that provides EduCloud administrators visibility into health and consumption of their virtual data center environments. Various dashboards and metrics are available to assist in monitoring, troubleshooting, and capacity planning.

BCNET member IT administrators completely manage the service to include:

- Requesting resources assigned to their organization;
- Networking and security configuration (networks, firewalls, load balancing, NAT, VPN);
- Users and groups – who will access the service and the privileges they have;
- Deployment of virtual servers and the resources assigned to them;
- Quotas and leases to control the amount and length of time resources are consumed;
- Catalogs – pre-built images of operating systems or applications that can be self-deployed by service users.

EduCloud provides the benefits of cloud computing without sacrificing security or control. In addition, through increased consolidation, costs are reduced, along with task automation and simplified administration. EduCloud Server integrates with existing VMware deployments and supports existing and future applications by providing flexible standard storage and networking interfaces, such as connectivity and broadcasting between existing virtual machines housed in the traditional grid environment and new virtual machines hosted on EduCloud.

Key Features/benefits:

- Low-cost, high-performance, on-demand cloud service for the Higher Education community (BCNET members)
- Member operated, highly flexible designed to meet their needs and managed through a web-based portal
- Virtual Data Centre with pools of resources for institutions to use/change without having to contact a service provider
- Efficient provisioning, sharing, and management of virtualized resources
- Standard catalog of predefined virtual machine templates with usage metering and secure multi-tenancy for applications
- Fast, easy and secure access to provisioning, managing, and using servers at a fraction of physical and/or other cloud server offerings
- Simple, self-service portal allowing quick & easy set-up and removal of servers from anywhere and (almost) any device
- Scalable infrastructure compliant with BC privacy legislation and FIPPA (Freedom of Information and Protection of Privacy Act) requirements
- Resilient & robust architecture that is fully monitored
- Secure, FIPPA compliant data storage, with pre-designed secure off-site back-ups (located on a different campus)

- All data is stored within BC/Canada
- 24x7 availability

EduCloud Server is available to all BCNET members. Connecting to the BCNET Advanced Network is preferred for the use of EduCloud, but not required. EduCloud is also available over the public Internet; however, BCNET cannot guarantee the quality of service when accessing EduCloud services over the public Internet.

2. Scope of this PIA

This PIA covers the use of EduCloud Server, its services, and the operational controls in place 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 moved in to the EduCloud platform by those members.

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 the EduCloud Platform. The BCNET member is responsible for the secure transmission of the data from their operating system to EduCloud. EduCloud offers members strong encryption for content in transit, including the option to manage their own encryption keys.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

EduCloud Server is currently hosted on secure servers in 2 geographic locations (Vancouver and Kamloops) within BC. Data backup for the Vancouver location is located in Kamloops, and data backup for the Kamloops location is located in Vancouver. The platform is restricted to authorized users and not by geographic location. All personal information stored by members will reside in Canada and will not be stored outside of Canada.

Disaster Recovery:

At present there is no Disaster Recovery (DR) plan or service option in place for member services however, the EduCloud service automatically create backups as part of the service. A full High Availabilty (HA) service using Zerto for VM replication is currently being implemented. The Kaltura service is already covered under HA DR as it resides on the UBC portion of EduCloud. does have a DR plan that is managed and tested by UBC for UBC purposes only. In the event of a disaster recover prioritization will be dependent on site/EduCloud instance and internal priorities.

BCNET member support:

BCNET and BCNET members can work with UBC to manage and resolve all incidents and issues raised and reported. BCNET and their members have 24x7 access to UBC technical support staff all of whom are located in BC. BCNET members have sole control and responsibility of what information they share with technical staff when they contact them at the time as permitted under Section 33.1 of the Act.

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

BCNET members:
As BCNET members are building systems on top of cloud infrastructure, the security and compliance responsibilities are shared between EduCloud and BCNET members. In this IaaS model, members control how they architect and secure their applications and data put on the infrastructure, while EduCloud is responsible for providing services on a highly secure and controlled platform and providing a wide array of additional security features. The level of EduCloud and member responsibilities in this shared responsibility model depends on the cloud deployment model. Members should be clear as to their responsibilities under this model.

EduCloud:
No PI is maintained by the EduCloud Operators or BCNET as part of the administration on the service.

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 EduCloud Server. 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 UBC)	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 EduCloud	Transmission is encrypted with 256-bit AES encryption and over a secure line. Encryption keys managed by BCNET members.	Low	High
3.	EduCloud Security Breach	EduCloud breach protocols are. in place to reduce risks to member 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 EduCloud Server.

Part 3 – Security of Personal Information

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

BCNET members:
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.

EduCloud:
The EduCloud service is hosted in two secure data centers protected by access controls. Access is continuously monitored both electronically and by cameras. Only authorized personnel have access to the secure data centers.

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.

EduCloud:

As EduCloud is built on VMware technology the service operator follows VMware best practices for securing the platform.

VMware vCloud Networking and Security vCloud Networking and Security provides networking and security capabilities for virtualized compute environments that are built with vCloud Suite technologies. It provides a broad range of services delivered through virtual appliances (see Figure 1), such as a virtual firewall, virtual private network (VPN), load balancing, network address translation (NAT), DHCP and VXLAN-extended networks, while also providing a comprehensive framework to integrate third-party solutions. These foundational networking and security capabilities of the vCloud Suite enhance operational efficiency, improve agility with control and enable extensibility to partner solutions. Management integration with VMware vCenter Server™ and VMware vCloud Director® reduces the cost and complexity of data center operations.

VCloud Networking and Security Features

FEATURES	VCLOUD SUITE ENTERPISE
Firewall	*
VPN	*
VXLAN	*
vCloud Ecosystem Framework	*
NAT	*
CHCP	*
High availability (HA)	*
Load balancing	*
Data Security	*
Endpoint	*

Figure 1

More detailed information on VMware vCloud security can be found at:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/products/vcns/vmware-vcloud-networking-and-security-overview-whitepaper.pdf and/or

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmw-10q3-white-paper-cloud-director-security.pdf

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 of their individual organizational security policies etc. as it relates to the handling and management of personal information in their custody and/or control.

EduCloud/VMware vCloud:

Using the VMWare NSX solution, members can configure security rules for their individual VDC. With NSX, members have the ability to lock down applications, create a logical DMZ in software, and reduce the attack surface of a virtual desktop environment, NSX Data Center enables micro-segmentation to define and enforce network security policies consistently on any workload hosted anywhere.

All features are configured and administered by the member with support provided by the EduCloud operators as required.

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.

EduCloud – 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.

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

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?

EduCloud – 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

<u>Part 5 – Further Information</u>

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 — 10 January, 2019

Dean Crawford
Director, Shared Systems & Technology
BCNET

Date

Head of BCNET

Digitally signed by Bala Kathiresan
DN: cn=Bala Kathiresan, o=BCNET, ou=President and CEO, email=bala.kathiresan@bc.net, c=CA
Date: 2019.01.11 11:08:43 -08'00'

January 11, 2019

Bala Kathiresan
President & Chief Executive Officer
BCNET

Date

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