

Privacy Impact Assessment: BlueJeans Video Conferencing Platform

Name of Organization	BCNET		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd. – Roseann Whitton		
Email:	bev@hooperconsulting.ca Rwhitton@hooperconsulting.ca	Tel:	250 896-4272 250 920-6331
Program Manager:	Dean Crawford - Director Shared Systems and Technology Wilson Lee – Business Analyst, Shared Systems and Technology		
Email:	dean.crawford@bc.net wilson.lee@bc.net	Tel:	250 721-8477 250 472-5791

1. Description of the Initiative

BCNET is taking the lead on the development of this Privacy Impact Assessment (PIA) for the BlueJeans Network video conferencing platform (BJN) on behalf of its members and affiliations.

BCNET is a 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 organizations 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.

BCNET has licensed 2560 user accounts on behalf of its members to facilitate online video conferencing services to support remote learning enrichment, improve collaboration for faculty and students, and improve efficiency for administrative staff. BCNET and its members have access to

BJN service which supports the continuation of essential communications and interactions between faculty, students and employees that would typically take place on site and face to face. BJN is highly flexible and can facilitate remote on demand cloud-based meetings and large interactive multimodal meetings and learning and training events over a large geographical expanse from any device. (i.e. desktop, mobile app etc.). Once an individual has been approved as a user (by BCNET or their member institution) they are assigned an account, they set up their security credentials, activate their account and can access the BJN service.

A key component of facilitating innovative information technology (IT) solutions through BCNET is ensuring they are hosted, accessed, managed, and protected within a secure environment in accordance with Provincial FIPPA privacy laws, regulations, and controls.

The BJN solution provides hosted high definition video conferencing services across multiple enterprise level platforms using current scheduling, messaging and productivity tools (i.e. Microsoft Outlook & Google email and calendars etc) through its secure online website (browser) and/or its direct website portal (desktop) located at <http://www.bluejeans.com>. It brings audio, web, and video together in one place. This service offers a simple and easy-to-use video conferencing bridge that improves meeting participation, eliminates travel time and the associated costs, and improves the ability to communicate effectively with faculty, students and staff across multiple locations, institutions, and technologies. This increases productivity, promotes member collaboration, supports student learning, and creates significant costs savings to the BCNET community at large.

Primary benefits of deploying BJN:

- Conduct online course delivery
- Integrates with Microsoft Teams
- Conduct thesis dissertation and defense
- Host remote guest lectures
- Improve research collaboration
- Collaborate with faculty committees
- Conducts admissions interviews
- Connects with colleagues
- Conducts company interviews
- Recruits students and staff
- Sets up co-op student interviews
- Augment global career services to connect recruiters and students
- Low-cost, alternate solution to expensive room-based systems
- Easy access to meetings from any device for students, faculty and staff
- Improves meeting participation
- Reduce travel costs

BlueJeans' service and client products are built with security and privacy in mind. BlueJeans follows Operating System vendors' best practices for installation and uninstallation on end user machines. The products uninstall cleanly. BlueJeans has taken precautions to make sure that the meeting Uniform Resource Locators (URLs) cannot be invoked from unauthorized websites. Only white-listed websites can invoke BlueJeans applications on desktops and laptops for example. These white-listed websites include bluejeans.com and a select partner sites. In addition, the BJN platform is an interoperable solution that works seamlessly with existing BCNET member institution systems hardware and supports BCNET's ongoing efforts to aid its

members' in facilitating innovative approaches to higher education. Using this platform as a service (PaaS) frees up BCNET and its members from having to design and develop internal solutions and installing the supporting in-house hardware requirements. Leveraging BJN technology enables the BC higher education community of practice to focus on the management, administration, and delivery of programs.

BJN is a product of BlueJeans Network Inc. (BJNI), a subsidiary of Verizon Business based out of San Jose, California. BJN controls and operates the website and website portal from the U.S. on behalf of BCNET and its members as users of the service. They have international offices in the United Kingdom, Australia and India and cloud-based data centres around the world including Amazon Web Services (AWS) in Canada. BJNs platform is hosted on AWS servers, a global solutions provider with a demonstrated track record in providing enterprise-grade security, scalability, administrative safeguards, and data protection protocols for industry-leading video conferencing solutions. BlueJeans utilizes various AWS regions to elastically increase meeting capacity. A comprehensive PIA has been completed by BCNET on AWS Canada Region. This PIA covers the full spectrum of AWS services and their operational controls and measures deployed in the AWS Canadian Cloud environment to identify and assess potential vulnerabilities to BCNET members.

Live BJN meetings (data in transit) are initiated and deployed by BCNET and its members are aggregated into a single video session on servers located outside of Canada. This is considered data in transit and as such is not stored under any circumstances. However, login details (username and password) are stored in the U.S. and duplicated to every global data centre currently supported by BJN. This enables a user to login from any region around the world supported by BJN. All interactions and communications (audio, video chat, web etc.) that take place and flow between authorized participants go through the non-Canadian based servers.

BlueJeans has added AWS Canada as a region for storing recordings (data at rest) for Canadian customers. This an account level setting that BJN Support has enabled based on BCNET's request to store all recorded events within Canada. As a result, all BCNET member meeting recordings are stored in AWS Canada. Only the moderator/organizer of those can activate or cancel the recording feature. At that time, event participants receive an automated system notification that the recording feature has been activated and a red flashing light icon appears on the screen. When an event is recorded, an added level of security is added, and it is stored in a secure container within the server in the cloud. **Section 15(1)(l)**

BJN does not access client content for any purpose other than as legally required and for maintaining the services and does not use BJN content or derive information from it for marketing or advertising. BJN employees who provide customer support, troubleshooting support or maintain the platform may access client personal information but only as requested by BCNET and its members and with their explicit permission. BCNET and its members have sole control and responsibility of what information they share with BJN support staff when they contact them.

BJN complies with applicable laws and regulations of the relevant jurisdiction within which BJN operates at any given time. Personal information is collected, used, and disclosed in accordance with all applicable privacy protection laws as required by each jurisdiction. BJN commits to ensuring that any and all applicable privacy legislation is reviewed annually to ensure that any change to existing jurisdictional privacy legislation is addressed and reflected within its policies and practices.

Access to the website and website portal are managed by BCNET who have negotiated a sector-wide, user-based enterprise service contract with BJN. BCNET IT administrators are responsible for the BJN dashboard security, high-level end-user accessibility and establishing and assigning member accounts. BCNET uses a decentralized model in managing and providing this service to its members and has delegated the "Administrator Privilege" to an authorized senior IT employee within each member institution. This employee oversees, manages, assigns, and administers user accounts on behalf of their institution. However, it should be noted that once a member is granted this privilege, they also have access to and the ability to make changes to other BCNET member data. BCNET is clear that members should not access or change any global account settings and manages and reinforces this both verbally and by sending a written notification to each institution. Individual institutional administrators may only create and alter user accounts for users from their own institution.

BCNET is committed to ensuring that the use of the BlueJeans application meets provincial privacy and security legislative requirements, policies, and practices, and strives 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 and expanded use of the BJN platform by BCNET and 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).

2. Scope of this PIA

This Privacy Impact Assessment (PIA) addresses the collection, use, disclosure, storage, access, and security of personal information while using the BJN service. In order to meet privacy requirements, BCNET works collaboratively with their IT department and BJN for ongoing maintenance and upgrades to the platform.

This PIA also covers the privacy and security measures deployed by the BJN video conferencing platform in the AWS Canadian cloud environment 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 however, a comprehensive PIA has been completed by BCNET on Amazon Web Services Canada (AWS). This PIA covers the full spectrum of AWS services and its operational controls and measures (to include disaster recovery) deployed in the Canadian Cloud environment to identify and assess potential vulnerabilities to BCNET members and the community at large.

This PIA reflects the current status of the BJN service and will be updated/revised to ensure that any future privacy issues identified related to the collection, use, disclosure, storage, access, and security of personal information is captured, addressed, and reflected in this document, as necessary.

4. Elements of Information or Data

First and last name, Username, password, email address, title (optional), institution, and profile picture (optional).

5. Storage or Access outside Canada

BJN owns and operates the BJN website and the website portal BCNET's behalf.

BJN meetings (data in transit) utilized by BCNET and its members are aggregated into a single video session hosted on servers located outside of Canada (audio, video, chat, web etc.). As noted previously, only the username and password are stored in the US and duplicated to every global data centre BJN has and controls. All interactions and communications (data in transit) that take place and flow between authorized participants go through the servers located outside of Canada, but it is not collected unless the option to record the event (data at rest) is activated. They use Amazon Web Services (AWS) in Canada to store recorded data only in the cloud. Section 15(1)(j)

Recordings are stored strictly in the AWS Canada region.

In deploying BJN, BCNET and its member institutions will be using the AWS servers in the Canadian cloud for data at rest for recording storage. Assessment of this platform, including disaster recovery options, is outlined in the BCNET Amazon Web Services (AWS) Canada Privacy Impact Assessment.

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*

<p>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.</p>	
1. This initiative involves a program or activity that provides a service (or services);	Yes
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;	Yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
<p>Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.</p>	

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

This table addresses the flow of personal information while using the BJN video conferencing system (e.g. BCNET members - students, instructors, employees).

Personal Information Flow Table – Users			
	Description/Purpose	Type	FOIPPA Authority
1.	"Administrator Privilege" is delegated by BCNET to authorized individual within the member institutions IT department.	Collection	26(c)
2.	Member IT department establishes and assigns accounts to users as requested and approved.	Collection	26(c)
3.	User sets up personal profile credentials under their account and enables access to BJN.	Collection	26(c)
4.	Member students, faculty and staff access BJN via a secure connection using their ID and password.	Use	32(a)
6.	Member faculty, staff and students, access BJN and invite participants to join meeting/event using both a moderator and participant passcode. (Moderator passcode: the meeting host or delegate must enter the code to start the meeting;	Use	32(a)

	<u>Participant passcode</u> : an additional layer of security to ensure that only invited attendees can join the meeting)		
7.	Moderator determines if meeting will be recorded and a notification of recording is sent to all users.	Use	32(a)
8.	Moderator can determine what portions of recordings are required and recording is stored in AWS data centre in Canada	Use	32(a)

9. Risk Mitigation Table

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 BJN. 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 BJN platform and use or disclose it for personal purposes (within BCNET and its members).	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, audit, controls, and monitoring.	Low	High
2.	BJN user account is accessed externally by another individual.	User assigns a unique password to protect their information and self manages changes.	Low	High
3.	Personal information is compromised when a user accesses BJN and enters information from their computer and/or mobile device.	Managed and maintained by user through computer and/or mobile device security controls and protocols.	Low	High
4.	Unauthorized employees/service providers could access the personal information in BJN (within BJN).	Contractual privacy protections flow downs between BCNET and BJN. BJN internal security and privacy standards, access controls, role-based authorization, and IP whitelisting in place restricting access to cloud data.	Low	High
5.	Personal information is compromised when transmitted and stored in BJN AWS servers.	Section 15(1)(l)	Low	High
6.	Third-party security breach.	BJN & AWS breach protocols are in place to reduce risks to user	Low	High

		data in the event of a security breach.		
--	--	---	--	--

BCNET

(Responsible for Security "IN" The Cloud)

ACCESS MANAGEMENT

BCNET and its members: Assume responsibility and management of the operating system (including updates and security patches), other associated platform tools, configuration of the BCNET member cloud-provided security firewalls, user access controls, and other security, change management, and logging features.

BlueJeans (BJN)

BJN PLATFORM, WEBSITE BROWSER AND PORTAL
 SERVER-SIDE ENCRYPTION NETWORK TRAFFIC PROTECTION
 ENCRYPTION & DATA (FILE SYSTEM AND/OR DATA) (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

(Responsible for Security "OF" The Cloud)

COMPUTE STORAGE DATABASE NETWORKING

AWS Infrastructure: REGIONS/AVAILABILITY ZONES/EDGE LOCATIONS

AWS Canada: 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.

10. Collection Notice

The BCNET member is responsible for ensuring the appropriate collection notification is in place prior to the collection of personal information and before transmission to the BJN server.

Notice:

The personal information that you provide in activating your BlueJeans Network (BJN) account will be used to securely communicate, engage, and interact with you and other employees, students, and faculty, within your institution as well as other members across the BCNET community. This information will be used and disclosed only for purposes directly related to and required by BCNET and (the name of institution) in the management and use of your BJN account, to include conducting meetings, events, and other communications with others remotely. Your personal information, specifically your login credentials (username, password, and profile picture [if provided]) only, will be processed and stored on a secure server in San Jose, California in the U.S.,

until your account is deactivated and deleted. All events that are recorded will be stored on a secure server within Canada.

For more information about BlueJeans privacy policies and practices please see <https://www.bluejeans.com/privacy-policy>.

By registering with BJN and activating your account you consent to the collection, use, and disclosure of your personal information as described above.

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

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

BJN

Section 15(1)(l), Section 21

AWS

Refer to the BCNET AWS PIA

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

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

BJN

Section 15(1)(l), Section 21

Summary of Comments on QUESTIONS

Page: 9

 Number: 1 Author: Roseann Date: 2020-06-01 8:03:00 PM

 Wilson

If you and Dean are okay with this language then its good to go to sign off. Thanks

 Number: 2 Author: Wilson Lee Date: 2020-06-02 2:14:00 PM

I am happy with the language. Dean?

Section 15(1)(I), Section 21

AWS

Refer to the BCNET AWS PIA

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

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

Section 15(1)(I)

AWS

Refer to the BCNET AWS 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 third-party service providers are responsible for the strict management and administration of user access based on a "need to know" principles including maintenance and enforcement.

BJN

BJN provides access permission-based roles which can be assigned to authorized users of each account. Permissions can be customized for users based on their access level. BJN implements access controls, role-based authorization and IP whitelisting to restrict unauthorized access to cloud data by both internal and external parties.

Only as requested by BCNET and its members and with their explicit permission do a limited number of authorized BJN employees have access to client personal information. Access is role based and only authorized to those employees who provide customer support, troubleshoot or maintain the platform. BJN employees cannot access client personal information except in the performance their job responsibilities and cannot alter personal information except at the written request of BCNET and its members. The access list is reviewed quarterly by VPs of Support and Operations.

AWS

Refer to the BCNET AWS PIA

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

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

BJN

Section 15(1)(I), Section 21

AWS

Refer to the BCNET AWS PIA

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

Updates to user information (e.g. students, faculty, staff) can only be made and noted by BCNET and its BCNET members. Users (faculty, students and staff) can also update their personal information at any time via the BJN website or portal via a secure login. BCNET and its members rely on users to ensure the information provided is accurate and up to date.

BJN

Personal information is provided directly from BCNET member institutions, faculty, students and staff. BJN cannot at any time update or alter the client personal information in the BJN system unless requested through a support ticket.

AWS

Refer to the BCNET AWS PIA

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

No. While students, faculty and staff may use BJN for sessions that will inform decision making, and decisions affecting individuals may be made during those sessions, the platform itself is not used specifically for direct decision making but rather to assist in the decision making process.

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.

NA

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?

NA

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.

Signed on Behalf of BCNET:

Dean Crawford
Director
Shared Systems and Technology

Date