Privacy Impact Assessment

TeamDynamix PIA#

Name of Organization	BCNET		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd. (Tracy Jo Reid)		
Email:	bev@hooperconsulting.ca tjreid@hooperconsulting.ca	Phone:	250 896-4272 250 388-0145
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 TeamDynamix (TD) 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 members (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 public-sector organizations face unique challenges to accomplish complex mandates with limited resources, they are overwhelmingly turning to the power and speed of cloud computing technology and infrastructure to serve citizens more effectively, achieve scientific breakthroughs, and educate students.

BCNET

Privacy Impact Assessment

TeamDynamix PIA#

BCNET is proactively leading the implementation of the Team Dynamix platform internally, and for its members. The platform provides a suite of services including workflow tracking, reporting, project management, issues resolution, task coordination, self-service portals and process synchronization. This functionality simplifies and streamlines business practices which supports internal organizational alignment in the following areas:

IT	Project Portfolio	Enterprise Svces
Incident Management	Dashboards & Reporting	Facilities Mgmt
Self-Service Portal	Project Intake	Human Resources
Automation & Workflow	Project Mgmt	Marketing/Promotion
Change & Release Mgmt	Resource Mgmt	Event Mgmt
Dashboards & Reporting	Budget Mgmt	Student Portal

While the above services may require the collection of personal information, it is recommended that users do not include personal information outside of the employee login credentials and mandatory personal information fields unless the inclusion is necessary to administer the functionality of the system.

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 use of TeamDynamix 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 and its members who wish to utilize applications hosted by TD 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).

TeamDynamix is a provider of cloud-based service and project management software, with a focus on serving the higher education space. The core product is used by students, faculty and staff to request, fulfill and receive service across a wide variety of departments including IT, facilities and marketing.

2. Scope of this PIA

This PIA has been developed with a focus on the privacy protection and security measures deployed by TeamDynamix in the Canadian cloud environment. This includes use of TeamDynamix by BCNET, its services and operational controls as it relates to Privacy, Security and Data Protection in British Columbia.

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

3. Related Privacy Impact Assessments

No other PIA's have been completed on this initiative to date. A PIA has been completed on the Microsoft Azure platform by BCNET.

4. Elements of Information or Data

Mandatory Fields containing PI:

- User Name (only if single sign on is not implemented)
- Password (only if single sign on is not implemented)
- FirstName
- Last Name
- Primary Email
- Alert Email
- Is Employee
- Is Active

Discretionary Fields containing PI:

- Middle Name
- Birthday
- Salutation
- Nickname
- Gender
- Alternate Email
- Home Phone
- Primary Phone
- Pager

- Other Phone
- Mobile Phone
- About Me (open text field to provide information about the individual)
- Home Address
- Home City
- Home Province
- Home Postal Code
- Home Country

5. Storage or Access outside Canada

All data will be stored within Canada.

TeamDynamix is hosted in Microsoft Azure. BCNET customer data will be hosted in a TD environment that is hosted in Central Canada (Azure Region). All user information is stored in a Microsoft SQL Server database. All database files are stored on encrypted disk using 256-bit AES encryption block cipher. Database backups are encrypted as part of the backup process using 256-bit AES encryption block cipher. Database backups for BCNET customers will be stored in a geo-replicated Microsoft Azure Blob Storage Account with the primary location being in the Azure Central Canada region and the backup in the Azure East Canada region.

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;	Yes
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);	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;	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

See *Appendix A* – attached.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Users login to TeamDynamix with credentials using Single Sign On, LDAP authentication or TeamDynamix Authentication.	Collection	*26(c)*
2.	'People Profiles' are created manually by users with the appropriate assigned permissions via the TDAdmin & TDNext applications or imported via the TDWebApi application.	Use	*32(a)*

3.	Users are given permissions to the TD applications (e.g. IT, Project Management, Assets, etc.) as appropriate by an IT administrator. Users login using secure credentials & work in the modules for which they have been assigned permission (e.g. Open a 'HelpDesk' IT ticket & assign to a technician to resolve an incident).	Use	*32(a)*
4.	Discontinued user data is exported, transferred to the client and deleted from the TD system upon termination of contract between TD and client.	Use	*32(a)* *33.1* *33.2*

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 TD environment – Microsoft Azure)	Employee Code of conduct and non-disclosure agreements; password-protected access, user access based on need to know, permission restrictions, role based access controls, multi-factor authentication, privacy training, just in time user provisioning via SAML and audit/monitoring.	Low	High
2.	BCNET/member personal information data is compromised during transmission from the BCNET/member to TD	Encrypted by TD during transfer of data (HTTPS TLS 1.2, AES 128/256 cipher suites).	Low	High
3.	TeamDynamix Cloud (Microsoft Azure) security breach	TD employs breach strategies and remediation protocols. See also Microsoft Azure protocols detailed below.	Low	High

10. Collection Notice

BCNET and its members are 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 TD.

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

BCNET:

BCNET, its 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.

TD:

https://docs.microsoft.com/en-us/azure/security/azure-physical-security

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

BCNET:

BCNET, its 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.

TD:

Data in transit: All web traffic between the web server and the user's browser or API client is encrypted via HTTPs using TLS 1.2 with AES 128/256 cipher suites.

Data at rest: BCNET and member data is hosted by Microsoft Azure. All user information is stored in a Microsoft SQL Server database. All database files are stored on encrypted disks using 256-bit AES encryption block cipher. Database backups are encrypted as part of the backup process using 256-bit AES encryption block cipher.

Multi-factor authentication. Environments (production, non-production, etc) are on segregated networks and have separate database servers, web servers, load balancers, etc. This ensures that deployments to a lower environment cannot target production systems.

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

BCNET:

BCNET, its 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.

TD:

https://docs.microsoft.com/en-us/azure/security/azure-physical-security

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:

BCNET, its members and their service providers are solely responsible for the strict management and administration of user access based on need to know including the maintenance and enforcement.

TD:

TD will not be making any changes to the personal information that resides within the system.

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

BCNET:

BCNET, its 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.

TD:

Access to the TeamDynamix hosted environments follows a least privilege approach. This includes role based access rules managed in a centralized directory. All logins to the Azure Portal have two factor authentication enabled. Account information is tracked in a password vault that has access limited to the infrastructure team and also requires two factor authentication. Login attempts at the operating system and database levels are recorded in a centralized logging solution.
Login attempts to the TD application are stored within the application's database, are read-only in the application's interface, and are only accessible by TD employees who are delegated as application administrators.

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 and its members are responsible for providing personal information updates to TD via data transfer (formal process to allow a BCNET/member to correct/amend inaccurate personal information as appropriate in compliance with ISO 27018). Responsibility for ensuring all personal information is up to date and accurate lies with BCNET and its members.

TeamDynamix does not make any updates or corrections to the data on behalf of BCNET or its members.

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

BCNET and its members may use personal information to make a decision that directly affects an individual in the course of using the system when administering programs and services. Responsibility for ensuring all personal information is up to date and accurate lies with BCNET and its members.

TeamDynamix does not use personal information to make a decision that directly affects an individual.

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.

Responsibility for ensuring all personal information is up to date and accurate lies with BCNET and its members. BCNET and its members are responsible for providing personal information updates to TD via data transfer (formal process to allow BCNET and its members to correct/amend inaccurate personal information as appropriate in compliance with ISO 27018).

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?

Responsibility for records retention and/or disposition schedules lies with BCNET and its members.

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.

Yes.

a. Team Dynamix platform/system.
b. Registration for TD includes all personal information as outlined in point 4. above.
c. Section 26(c)
d. Obtained, compiled and used for the implementation and deployment of the Team Dynamix platform/system.
e. Used by authorized BCNET, its members, students and TD staff in support of implementation and deployment of the Team Dynamix platform/system.

Privacy Impact Assessment

TeamDynamix PIA#

Signed on Behalf of BCNET:

Dean Crawford Director, Shared Systems and Technology BCNET	Date
Bala Kathiresan President and Chief Executive Officer BCNET	Date