Tableau for A&D Privacy Impact Assessment

Project Code	PC0917-Tableau for Alumni and Development
Submission Date	June 15, 2020
Administrative Authority	Jane Potentier, Associate Vice President Alumni and Development
Author and Contact Information	Gregory Churchill, Associate Director Alumni and Development Information Systems, Project Manager for this project.
Reviewed By	Nav Bassi, Chief Information Security Officer
Review Date	June 15, 2020

Purpose: The purpose of the Privacy Impact Assessment (PIA) is to assess risks associated with how a project plans to handle personal information. There are policy and legislative requirements and the purpose of the PIA is to ensure the project approach will be compliant with these requirements, and that any risks to privacy are mitigated or, if they cannot be completely mitigated, understood and accepted by the appropriate Administrative Authority as defined in section 2.00 of Policy IM7800:

> *Administrative Authority means individuals with administrative responsibility for units (e.g., Vice-Presidents, Chief Information Officer, Executive Directors, Deans, Chairs, Directors and other unit heads) and individuals with functional stewardship of university Information Resources.*

Roles:

The role of University Systems is to complete this document and provide guidance regarding security policy compliance and risks to the Administrative Authority.

The role of the Privacy Office is to review this document and provide guidance regarding privacy policy and legislative compliance and risks to the Administrative Authority.

The Administrative Authority is accountable for ensuring the Information Resource being implemented or changed as a result of this project is compliant with privacy and security policies and legislation and accepting risks associated with non-compliance on behalf of the institution.

1.0 Privacy Context

1.1 Description

[[Describe the project, the systems being implemented or changed as a result of this project, and what implications there are in terms of FIPPA.]]

This project will implement a new Tableau client and server software system for the Alumni and Development unit. The entire system and all related data is Sec. 15 (this is not a Cloud implementation.)

Tableau (https://www.tableau.com) is business intelligence software used by clients to build and publish dashboards (charts, graphs, and tabular data) that guide planning processes and measure performance.

This project will implement a system with the following components:

1. Tableau desktop software.
    - 5 A&D staff users in the "Creator" and "Explorer" security groups will have desktop access.
    - Desktop users create dashboards with Tableau desktop software.
    - Desktop users publish dashboards to the Tableau server.
2. Tableau web browser.
    - Approximately 50 A&D staff users in the "Viewer" security group will have web browser access.
    - Web browser users view and interact with Tableau dashboards (charts, graphs, and tabular data).
3. Tableau Server instances.
    - Tableau Server is a hosting platform that stores dashboard content and database connections.
    - Tableau users connect to the server to create, publish and view dashboards.
4. Database connections to reporting stack.
    - The Tableau servers connect to the Alumni and Development reporting stack (SQL database servers).
    - Data from the reporting stack is used to build Tableau dashboards and to create new data and information.
5. Active Directory User Authentication.
    - Clients sign in to the system using their UVic staff user accounts (primary Netlink ID).
    - University Systems will manage security groups.

There are implications in terms of **FIPPA**, with special attention to **sections 30, 30.1, 32(a)**. See the following sections for more details.

1.2 Privacy Issues Related to this Project

[[Describe the privacy issues and how they are being addressed in the project approach.]]

The information classification level of Alumni and Development data is "Highly Confidential" as defined in University Policy IM7800. The project approach is to ensure adequate information privacy and security training and documentation is in place when transitioning the system to operations. Additionally, the project will develop a risk management plan.

1.3 Privacy Impact Assessment Scope

[[Describe what records will be under the possession or use of the institution or system and how the records will be managed to address FIPPA.]]

Project Scope	Privacy-Related Activities and Processes
The Tableau servers connect to the Alumni and Development reporting stack (SQL database servers).	• University Systems will make security arrangements to ensure the protection of personal information (**FIPPA section 30**). • All data and information used by or created by the system will be stored Sec. 15 Sec. 15 in Canada (**FIPPA section 30.1**).
Data from the reporting stack is used to build Tableau dashboards and to create new data and information.	• A&D staff will only use data and information for planning and reporting purposes necessary to fulfill the objectives of the University Strategic Framework as it relates to the Alumni and Development unit (**FIPPA section 32(a)**).
Tableau users connect to the server to create and view dashboards.	• University Systems will manage Active Directory security groups and A&D will assign users to these groups (**FIPPA section 30**). • A&D documents and tracks the provisioning and de-provisioning of all users. (**FIPPA section 30**). • Access removed immediately when the University or the unit no longer employs a user (**FIPPA section 30**).

1.4 Related Privacy Impact Assessments

[[List any related privacy impact assessments that have been completed and where to find them.]]

PIA for Project PC0746 RE NXT Upgrade:

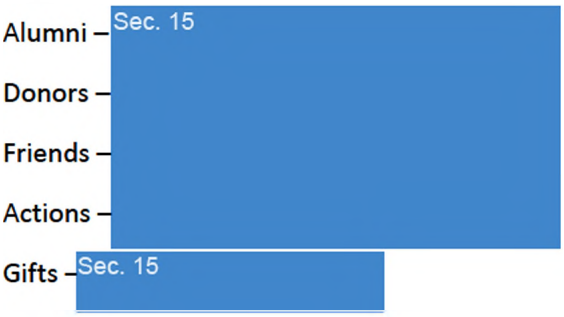
https://connect.uvic.ca/sites/systems/PMO/projects/PC0746/ProjectDocuments/RE%20NXT%20Privacy%20Impact%20Assessment%20-%20version%202-3.DOCX?Web=1

1.5 Elements of Information or Data

[[Describe the information or data and how it is used.]]

Data	Description	Usage
• Full name • Home address • Email address • Phone number • Personal web address • UVic constituent ID • Date of birth • Ethnicity • Gender • Relationships to family • Academic history • Employer and job position • Volunteer activity • Event attendance • Awards • Sec. 15 • Philanthropic interests • Interactions with UVic fundraisers	• Biographic • Demographic • Behavioural • Sec. 15	• Alumni engagement planning and reporting. • Fundraising and capital campaign planning and reporting. • Donor prospect research. • Financial reporting. • UVic Board of Governor reporting.

Record counts:



2.0 Protection of Personal Information

2.1 Storage or Access outside of Canada

[[Describe any storage or access outside of Canada.]]

There is no storage outside of Canada. Authorized UVic staff can access the system from outside of Canada using a secure VPN connection provided by University Systems.

2.2 Personal Information Flow Diagram and/or Personal Information Flow Table

[[Describe the personal information flows]]

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	Tableau users view dashboards.	Pull	32(a)
2.	Tableau users create new dashboards.	Publish	32(a)
3.	Tableau administrative users perform application tasks, such as configuring accounts and dashboard settings.	Event handling	30, 32(a)
4.	Reports exported from the system and shared with external stakeholders such as the UVic Board of Governors.	Communication, Pull	32(a)

2.3 Risk Mitigation Table

[[Identify any privacy risks associated with the initiative and the mitigation strategy for each privacy risk. Consult the University Risk Likelihood and Impact scales to complete the Likelihood and Impact ratings for each risk.]]

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Personal information breached.	University Systems will implement necessary security controls for Highly Confidential data as described in the Information Security Classification Procedures in UVic Policy IM7800. Ensure all staff aware of university policy IM7800 responsibilities when aware of an Information Security Incident.	Unlikely	Major
2.	Function creep. When information collected for one purpose is used for another, unrelated purpose.	Ensure adequate information privacy and security training and documentation is in place when transitioning the system to operations. Ensure Chief Privacy Officer is consulted prior to disclosing any personal information to other UVic departments.	Possible	Minor
3.	Over-retention of personal information.	Ensure adequate information privacy and security training and documentation is in place when transitioning the system to operations. Review and ensure compliance with UVic Directory of Records. [AD165-20 Fundraising – Donors]	Possible	Minor

4.	Software vendor change resulting in invalidation of this assessment.	Develop contingency plan for migrating data and services to an alternate vendor, such as Microsoft. Trigger new PIA/Security arrangements with new software provider.	Possible	Minor

3.0 Security of Personal Information

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

All servers are hosted in Sec. 15 For more information click here: https://www.uvic.ca/systems/support/informationsecurity/security-standards/index.php All client machines are provisioned by UVic Desktop support.

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

University Systems will implement necessary security controls for Highly Confidential data as described in the Information Security Classification Procedures in UVic Policy IM7800 and Information Security Standards.[1]

3.3 Does your department rely on security policies other than the Information Security Policy?

No

3.4 Please describe any access control and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

The software system implemented by this project does not permit any changes to personal information. Changes to personal information are only permitted within the database of record (RE NXT), which is outside of the scope of this project (there are separate access controls in place for the database of record.)

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

A&D staff maintains a chart of who has access to the system and the level of access granted to each user.

4.0 Accuracy/Correction/Retention of Personal Information

4.1 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 university notify them of the update, correction or annotation?

The software system implemented by this project does not permit any changes to personal information. Changes to personal information are only permitted within the database of record (RE NXT), which is outside of the scope of this project (there are separate access controls in place for the database of record.)

The software system implemented by this project is used to create new data and information about individuals. This new information is derived from personal data elements using a mathematical, logical, or other type of transformation, e.g. arithmetic formula, composition, aggregation.

[1] https://www.uvic.ca/systems/support/informationsecurity/security-standards/index.php

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

Yes, personal information is used to guide alumni and donor engagement programs, services, and relationship management. Examples include invitations to events, solicitations for donations, communications, delivery of programs and services, etc.

4.3 If you answered "yes" to question 4.2, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

The Data Quality Officer in Advancement Services oversees the Data Governance framework for the Alumni and Development unit. The Data Governance framework encompasses the people, processes, and information technology required to ensure consistent and proper handling of highly confidential alumni and donor data. This framework ensures a high level of data availability, usability, consistency, integrity and security.

4.4 If you answered "yes" to question 4.2, do you have approved records retention and 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?

Yes.

5.0 Further Information

5.1 Does this initiative involve systematic disclosures of personal information? If yes, please explain.

No

Information Sharing Agreement – Required Information	
Description	
Primary department involved	
All other departments involved	
Business contact title	
Business contact telephone number	
Indication of whether or not personal information is involved	
Start date	
End date (if applicable)	

5.2 Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

Not for research but for statistical purposes of program evaluation.

5.3 Will a personal information bank (PIB) result from this initiative?

No.

5.0 Comments and Signatures

Chief Information Security Officer: Nav Bassi

Comments:	**No Concerns**
Date:	June 11, 2020
Sign-Off:	Via email

Administrative Authority: Jane Potentier, Associate Vice President Alumni and Development

Comments:	**No concerns**
Date:	June 15 2020
Sign-Off:	Via Email Sec. 22

Portfolio Manager: Stephanie Rowe, Director of Advancement Services

Project Comments:	**Tableau is a key tool for the Alumni and Development program. It will provide dynamic visual representations of our data for our data driven decision-making. It will help us identify opportunities and gaps, and inform our decision on where to deploy our resources. Essentially, it will assist us in maximizing our goals of raising funds for the university and engaging alumni.**
Date:	May 15, 2020
Sign-Off:	Via Email

Consultation Checklist

IT Projects

The following leaders in each functional area can refer you to an appropriate subject matter expert to help develop the technical elements of your project plan and ensure it is complete.

Service Area	Impact? (Y/N)	Leader	Expert Consulted	Date of Consultation
Senior Management				
Associate Vice-President University Systems and Chief Information Officer	Y	Wency Lum	Nav Bassi	June 11, 2020
Director, Academic & Admin Services, and Chief Information Security Officer	Y	Nav Bassi	Nav Bassi	June 11, 2020
Director, Infrastructure Services		Ron Kozsan		
Director, UVic Online Services		Garry Sagert		
Academic & Administrative Services and Information Security Office				
Client Technologies		Lance Grant		
Computer Help Desk		Marcus Greenshields		
Desktop Support Services	Y	David Street	David Street	June 2, 2020
Information Security Office	Y	Eric van Wiltenburg	Mario Ivanov	June 8, 2020
Infrastructure Services				
Data Centre Services		Kim Lewall		
Network Services		Jane Godfrey		
Research Computing Services		Ryan Enge		
UVic Online Services				
Development Services		Ivan Petrovic		
Production and Technical Support	Y	Rizwan Bashir	Matthew Bacon	May 26, 2020
Project Management Process and Budget				
Administrative Officer		Trish Kearley		
Project Management Office	Y	Scott Thompson	Scott Thompson	May 20, 2020
Other Consultations				
Privacy Office	Y	Brad Weldon, Chief Privacy Officer	Brad Weldon	May 13, 2020
Alumni and Development Alumni and Development	Y Y	Atsuko Umeki, Data Analytics Officer Chris Coey, Software Developer		May 1, 2020

Revision History

Version	Date	Author	Comments
1.0	01-MAY-2020	Greg Churchill	Initial draft to be reviewed by project team and then submitted to Brad Weldon,

			Chief Privacy Officer for comments.
2.0	15-MAY-2020	Greg Churchill	Added reference to UVic Directory of Records and Sec. 15 as advised by CPO Brad Weldon.
3.0	9-JUNE-2020	Anna Karpova	Eric van Wiltenburg confirmed that Risk 1 mitigation strategy is fine. Matthew Bacon did not report any technical limitations to implementing security controls. Encryption at rest is an option. Therefore, we are confident University Systems can implement necessary security controls for Highly Confidential data.