

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the Privacy Officer to determine internal policies for review and sign-off of the PIA. If you have any questions about this PIA template or FOIPPA generally, please contact Shelley McKenzie (Privacy Officer) at [shelley.mckenzie@unbc.ca](mailto:shelley.mckenzie@unbc.ca) or (250) 960-6310 or visit <http://www.unbc.ca/foippa>.

### What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

## Part 1 - General

Name of Department:	Information Technology Services		
PIA Drafter:	Kevin Stewart		
Email:	<a href="mailto:Kevin.stewart@unbc.ca">Kevin.stewart@unbc.ca</a>	Phone:	250-960-5636
Program Manager:	Greg Condon		
Email:	<a href="mailto:Greg.condon@unbc.ca">Greg.condon@unbc.ca</a>	Phone:	250-960-5289

***In the following questions, delete the descriptive text and replace it with your own.***

### 1. Description of the Initiative

*UNBC currently uses two methods of access for students and employees depending on the services they need to access. One method makes use of the student/employee ID and an associated 6 digit PIN. The other uses a UNBC supplied username and a user defined password. 6 digit PIN's are relatively easy to crack making them not the best choice for security and having two sets of credentials causes endless confusion for first year students. In an effort to make it easier for students and employees while improving our security we are moving to using Active Directory credentials for accessing online services at UNBC. Students will get information on their account and how to activate it on admission and employees will be given this information on their first day of work.*

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### 2. Scope of this PIA

. This PIA covers the implementation of a single credential for Banner Self-Service- commonly referred to as SSO for Banner Self-Service.

### 3. Related Privacy Impact Assessments

NA

### 4. All Elements of Information or Data

On admission or on initial hire, a student or employee is informed of their UNBC supplied username, their student/employee ID and a unique Identifier to enable them to activate their account. Activation of their account requires them to provide a non-UNBC email address that can be used in the case of a lost or forgotten password. Once the account is activated it will allow the student or employee access onto UNBC network and computers and Banner Self-Service.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### Part 2 – Protection of Personal Information

*In the following questions, delete the descriptive text and replace it with your own.*

**5. Storage or Access outside Canada**

*Data for this initiative is stored in secured databases in UNBC's own secured data center. Only UNBC authorized IT personnel have access to the data center.*

**6. Data-linking Initiative\***

<p><b>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.</b></p>	
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;	no
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.	no
<p><b>If you have answered "yes" to all three questions, please contact the Privacy Officer to discuss the requirements of a data-linking initiative.</b></p>	

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### 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;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	NA
<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>	

**\* Please note: If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC) as well. Contact the Privacy Officer to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.**

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

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Based on information in our ERP an email or paper letter is sent to student or employee notifying them of the their user account and giving directions on how to activate their account		

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

2.	Student/Employee goes to a UNBC website to activate their account. Information needed is their student/employee number, their username and a UNBC provided unique identifier.		
3.	Student/employee provides a non-UNBC email address for potential use in case of a lost or forgotten password, sets their password and gains access to a subset of UNBC online services.		

### 9. Risk Mitigation Table

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

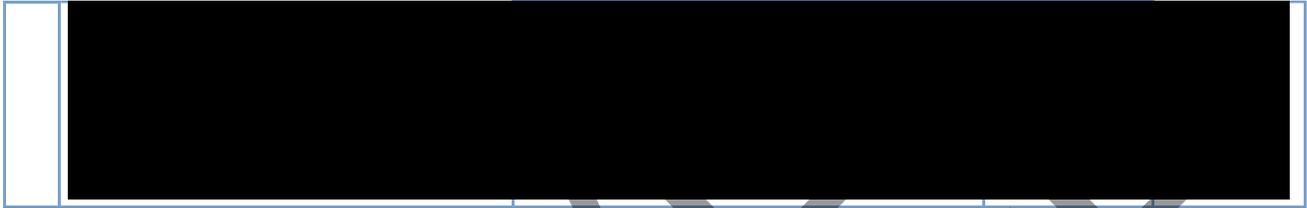
Risk Mitigation Table			
	Risk	Mitigation Strategy	Likelihood    Impact
1.			
2.			

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)



### 10. Collection Notice

#### Sample of notice going out to users:

Dear Sample User,

**Username: sampleu**

**User ID: 230029991**

**Activation PIN: 95941500**

UNBC is changing the process by which you'll recover your username or password if you forget either of them. We are providing a new Password Self Service tool which will allow you to manage and recover your account information without needing to visit the Service Desk. This will require you, this one time, to add a recovery email address to your account.

To confirm your password and set your recovery information, go to the UNBC Login Centre and click the Password Self Service link. Once there, you have two options:

1. If you know your password, simply sign in with the Username listed above.
2. If you do not know your password, click the Activate Account link and follow the instructions after signing in with your Username, User ID (employee number), and Activation PIN listed above.

**In both cases, you must follow the process all the way through to ensure we have a recovery email address on file for you.**

After this one-time activation you'll be able to use your Username and Password to access the Password Self Service tool, and can easily recover your Password if you forget it.

If you have any concerns, or believe you've received this message in error, please contact the Service Desk at 250-960-5321 or [support@unbc.ca](mailto:support@unbc.ca).

Thank you,

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### Part 3 – Security of Personal Information

*If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with the Privacy Officer, CIO or IT Security Officer when filling out this section.*

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

██  
██

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

██  
██

13. Does your department rely on any security policies? If so, indicate here:

██

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.

██

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

██

### 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?

*Recovery email information can be corrected or updated by the user logging into UNBC's password management tool. Corrections to email or physical addresses that are stored in our ERP need to be done through the appropriate channels of either the Registrar's office, Human Resources office or Alumni Relations office.*

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

**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.**

*For example: check to see that the information was obtained from a reputable source*

**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?**

*If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please describe retention schedules that apply where retention exceeds the one year requirement of FOIPPA. Please contact the Privacy Officer and/or records coordinator if you require assistance.*

### **Part 5 – Further Information**

**20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

No

***Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact the Privacy Officer.***

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

No.

***Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact the Privacy Officer, the UNBC Research Office or UNBC Archives.***

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

**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**

*A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.*

Please ensure Parts 6 and 7 are attached to your submitted PIA.

ACTIVELY INITIATED

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### **Part 6 – Privacy Officer Comments**

*This PIA is based on a review of the material provided to the Privacy Officer as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Officer.*

*These comments also reflect the discussions of a representative group including: ITS, HR (and faculty HR), Office of the Registrar and Development (Alumni Relations).*

ITS has determined, and there seems to be general understanding that, SSO represents a needed and positive improvement in security and service.

SSO does not involve the collection, by UNBC, of new or different personal information. It is instead, intended to be an improved and more secure method of accessing information currently collected and stored - in part by eliminating the d-o-b PIN reset, and also by reducing the number of passwords and login options to one username and password – (with improved complexity requirements?)

The main concern identified, is the way in which the information needed to make the transition, or to set up an account, will be delivered to employees and students: All information needed will be delivered in a single email (generated automatically when a new student or employee is “created” in banner), and the information provided will allow an individual to set up or access an account without an additional verification step. If this information is delivered to the wrong person, and if that person chooses to do something with the information, they would quite easily have full access to whatever information is available in the account linked to that login information.

The concern is minimized for existing students and existing employees as we have an existing email connection with these individuals. For new employees the concern is still minimal, in part because the volume is reasonable, and also because email communication would in all likelihood be established with an individual through the hiring process.

The risk with respect to Alumni (where again, we will likely have an established email communication) is more a relationship risk than a security risk. That is, an interruption or new barrier to access presented by a change in process. Coordination between the Help Desk, Alumni Relations and ITS to ensure smooth transition and ease of access for Alumni is to be discussed at a separate meeting.

\_\_\_\_\_  
\_\_\_\_\_

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

[REDACTED]

# Privacy Impact Assessment

## [Single Sign on for Banner Self-Service]

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# \_\_\_\_\_ (Privacy Officer to complete)

### Part 7 - Program Area Signatures

_____ Program/Department Manager	_____ Signature	_____ Date
_____ Privacy Officer/Privacy Office Representative	_____ Signature	_____ Date
_____ Head of Public Body, or designate (at UNBC, this is the Privacy Officer)	_____ Signature	_____ Date

Please send a copy of this PIA with the respective signatures to Shelley McKenzie for comment, review, approval & filing.  
A final copy of this PIA (with all signatures) will be kept on record with the Privacy Office.