BRITISH
COLUMBIA

Privacy Impact Assessment for Non-Ministry Public Bodies

Thoughtexchange

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 office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

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/Branch:			
PIA Drafter:	Wes Skulmoski, Manager, Institutional Research & Planning		
Email:	Wes.skulmoski@nic.bc.ca	Phone:	**250-334-5245**
Program Manager:			
Email:		Phone:	

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

1. Description of the Initiative

Implementation and use of Thoughtexchange. Thoughtexchange is comprised of software services and professional services provided by Fulcrum Management Solutions. Software services are those provided by the software platform that creates online conversations between leaders and their participants and provides analytics and data visualization. Professional services include email and phone support, coaching for leaders, and online access to help and resources.

2. Scope of this PIA

Thoughtexchange will be used to create online conversations with NIC employees, students, and external stakeholder groups and to generate reports and data visualizations.

3. Related Privacy Impact Assessments

N/A

4. Elements of Information or Data

Respondents will provide answers to open-ended questions. Demographic data may be collected from respondents by Thoughtexchange. Participants' identity (email address, name and telephone number) may be shared between NIC and Thoughtexchange. This information (Name, email and phone number) are collected from exchange leaders by Thoughtexchange when Thoughtexchange accounts are created. Information provided by participants as part of an exchange is not collected or stored by North Island College.

Part 7 – Program Area Signatures

Wes Skulmoski

Program/Department Manager | Signature | January 30, 2019 Date

Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.) | Signature | Date

John Bowman

Head of Public Body, or designate President | Signature | January 30/19 Date

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

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

Part 6 – Privacy Office(r) Comments

See attached data security document submitted by Thoughtexchange titled Thoughtexchange and Security.

Lisa Richard.
Privacy Officer/Privacy Office Representative

Lisa Richard.
Signature

Jan. 30 / 2019
Date

Thoughtexchange and Security

Introduction

Section 21

Personnel security

Section 21

Physical Security

Section 21

Secure by design

Section 21

Section 21, Section 15(1)(l)

Protecting customer data

Data encryption

Section 21, Section 15(1)(l)

Backups

Section 21, Section 15(1)(l)

Penetration testing

Section 21, Section 15(1)(l)

Network security

Section 21, Section 15(1)(l)

File sharing

Section 21, Section 15(1)(l)

Authentication

Section 21, Section 15(1)(l)

System monitoring, logging and alerting

Section 21, Section 15(1)(l)

Virus scanning

Section 21, Section 15(1)(l)

Endpoint monitoring and computer security

Section 21, Section 15(1)(l)

Mobile device management

Section 21, Section 15(1)(l)

Data confidentiality

Section 21

Participant Privacy and Terms of Use

Section 21

Section 21

Data removal

Section 21

Information security incident management

Section 21

Breach notification

Section 21

3rd party suppliers

Section 21