Privacy Impact Assessment for Non-Ministry Public Bodies

Cloud-based RSAO Management

PIA 12-08-15

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:	Emily Carr University of Art + Design Research Department		
PIA Drafter:	Alisha Walsh		
Email:	awalsh@ecuad.ca	Phone:	604-844-3811
Program Manager:	Jerri-Lynne Cameron		
Email:	jlcameron@ecuad.ca	Phone:	604-844-3091

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

1. Description of the Initiative

Emily Carr University is planning to purchase a software service that will provide a) management of research office data (grants and proposals) and b) process and forms management for proposal tracking in (a), as well as for mandatory institutional compliance processes (Human Ethics and Animal Care). This system is used (in either a cloud or local implementation) by over 50% of Canadian universities. It is a solely Canadian-based system.

2. Scope of this PIA

The scope of this PIA covers the use of a cloud based software service by a) Research Department staff to establish accounts and data records, store and maintain such records, and process transactions, and by b) faculty, administration, and occasionally staff, establishing accounts, entering data into forms and initiating or participating in customized processes. Forms and processes will relate to grant and contract proposals, grant and contract management, and both Human Ethics and Animal Care forms and process management.

3. Related Privacy Impact Assessments

Vancouver Island University is also implementing this service and shared with us their PIA which was used for this PIA. VIU indicated that Vancouver Island Health Authority recently implemented this same service for all their research activities and their Research Ethics Board and completed a PIA and security assessment within their own organization. This is a very stringent process. Elements of that PIA were shared to assist in developing this current document.

4. Elements of Information or Data

Personal: Employee name, email address and work phone.

Other: Grant applications, related tracking data, human ethics applications and animal care applications. Budget related to the above, and actual amounts awarded.

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.

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

The information will be stored in Canada. The entire web site is hosted in Calgary, Alberta, Canada, in a datacenter owned by Datahive Inc. Security noted below.

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;	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
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.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

**** 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). Contact your public body's privacy office(r) to determine how to proceed with this notification and consultation.***

For future reference, public bodies are required to notify the OIPC of a" data-linking initiative" or a "common or integrated program or activity" in the early stages of developing the initiative, program or activity. Contact your public body's privacy office(r) to determine how to proceed with this notification.

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

Please provide a diagram and/or table that shows how your initiative will collect, use, and/or disclose personal information (see examples below). Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. It should also outline the flows of personal information wherever it is transmitted or exchanged.

Both a flow diagram and a table must be included if the PIA is related to a common or integrated program or activity or a data-linking initiative.

All information is hosted on one system and entered through SSL secured web interface(s). No data transfer of personal information occurs. All information flow is internal to the university, with no external (i.e. public or other body) disclosure.

9. Risk Mitigation Table

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employee personal information could be compromised in data entry via web browsers	Transmission encrypted over SSL connection, and the ID utilized is a localized one (employee ID not required). All communication with the web site is secured by SSL/TLS encryption.	Low	Low
2.	Intrusion into cloud servers	See below	Low	Low

10. Collection Notice

NA.

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 your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

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

- 24X7X365 CCTV monitoring of all access and building entry points;
- man trap
- security personnel that monitor closed circuit surveillance of all building access points and key interior areas;
- biometric plus card scan security system and procedures that control and electronically track all entries and exits to the facility
- Datahive will control all access to the Data Center and other areas containing Process Pathways equipment to ensure protection of that equipment;

- Procedures to ensure access to any area containing Process Pathways equipment is restricted to authorized Datahive employees only

ENVIRONMENTALS:

- N+1 redundancy in all power delivery equipment (Hydro feeds, UPS devices, Generator, PDUs etc.) that will tolerate the servicing of any electrical and/or mechanical equipment without interruption to the Process Pathways computing environment;
- Uninterruptible Power Supply (UPS) that is fed by diverse Hydro feeds and backup generators power;
  - o will continuously supply conditioned power to all Process Pathways equipment;
  - o will supply a minimum of s.15 of battery life for all Process Pathway equipment, and subsequently indefinite period while on generator power;
  - o will supply N+1 protection scheme that ensures if any one of the UPS devices or their components fails or requires maintenance there is sufficient capacity to continue to run the Process Pathways equipment without interruption;
- generator power for Process Pathways equipment that will
  - o automatically start within s.15 of a power failure;
  - o supply enough power to all Process Pathways equipment;
  - o continue to sustain the computer environment without interruption until the primary power is restored to the facility;
- power conditioning for all Process Pathways devices that provides protection against surges in power, maintains a continuous voltage feed to these devices during temporary voltage reductions, such as a brownout;
- generator to support building emergency lighting, elevators, office areas, security systems
- N+1 protection scheme that ensures if any one of the air conditioning units fails or requires maintenance there is sufficient capacity to continue to cool the Process Pathways equipment including data network;
- a highly sensitive fire detection system uses particle detection system to alert Datahive prior to a fire starting;
- a "zoned dry pipe" fire suppression system with the capability of spraying water in the specific area where fires occurs and suspending water flow once a specific heat threshold is obtained;
- water detection units with alarms

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

HTTPS only on local browsers; caching in browsers disabled.

Network Security:

Security is ingrained in network services through its basic architecture, specialized security tools, and the policy and procedures which govern its management. For example,: separate physical network segments for public ("front-end"), private ("back-end"), and backup and administration; vLANing, NATing and VIPing; Packet per Second "Storm" controls; encrypted assess controls; default deny-all policies; and more

Firewall and VPN:

Firewall and Virtual Private Networking (VPN) services are built on state-of-the-art Juniper ISG technology. This enterprise-class security solution uses the latest Application Specific Integrated Circuit (ASIC)

technology to enable wire-speeds for advanced security features, such as: stateful packet inspection firewalling and client-based and site-to-site VPN services

Intrusion:

Firewall and Virtual Private Networking (VPN) services are built on state-of-the-art Juniper ISG technology engineered using the latest Application Specific Integrated Circuit (ASIC) technology to enable wire-speeds for advanced security features, such as: stateful packet inspection firewalling and client-based and site-to-site VPN services

Abuse Management

The security team works proactively with all its upstream providers and clients to deal with network abuse issues employing strict Acceptable Use Policy (AUP) that governs its network and protects the integrity of its service. DDoS management occurs in concert with upstream providers and Prolexic: the industry leader in DDoS protection services

See attached document for details of security overall: **note that most of this document is intended for Deployed Systems. The hosted solution has specifics listed in Section E**

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

Emily Carr University IT security policies.

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.

Access only by the named individual and by system operators, using single-sign on password authentication. We will work with vendor-based authentication and later migrate to an LDAP solution (single sign-on)

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

Server logs and software logs.

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?

Users can update (or remove or disable) any information about themselves through web portal access.

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.**

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?**

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 your privacy office(r).	

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 your privacy office(r).	

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, using the definition from FOIPPA.

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

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) 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 Office(r).

Alisha Walsh		December 9, 2015
Privacy Officer/Privacy Office Representative	Signature	Date

Part 7 – Program Area Signatures

Jerri-Lynne Cameron		December 9, 2015
Program/Department Manager	Signature	Date
James Rout, AVP, Learning Services + Information Technology		December 9, 2015
Contact Responsible for Systems Maintenance and/or Security	Signature	Date
Dr. Ron Burnett		December 9, 2015
Head of Public Body, or designate	Signature	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.