**Guide to Completing a Privacy Impact Assessment (PIA)**

**What is a PIA?**

A privacy impact assessment (PIA) is a process that assists public bodies in identifying and managing the privacy risks arising from new or substantially changed projects, initiatives, systems, and processes that collect, use, disclose, secure, or store personal information.

Completing a PIA is a legal requirement for all public bodies under S.69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). *FIPPA* requires public bodies to conduct a PIA on any new initiative, or when there is a significant change to an existing initiative, involving the collection, use, disclosure, or security of personal information.

In addition to being a legal requirement, PIAs help to identify deficiencies in privacy protection. It can assist management in making informed decisions and avoid privacy breaches by ensuring that Vancouver Island University (the University) is complying with *FIPPA*. The PIA demonstrates accountability by including privacy as part of the design of new initiatives or systems.

**What is Personal Information**

Personal information is defined as any recorded information about an identifiable individual, other than business contact information. Personal information includes, but is not limited to, name, birth date, gender identity, marital status, financial information, health information, educational history, unique identifier numbers, etc. Personal information also includes information that can be used to identify an individual through association or reference.

Business contact information is information used to contact an individual at a place of business such as the individual’s name, position name or title, business telephone number, business address, business email, and business fax number.

**When to Complete a PIA**

PIAs should be completed during the initial development of any new system or program or prior to any significant change being made to an existing system or program.

The PIA must be completed and signed off by the University’s Head or designate, prior to the implementation or launch date of a new initiative or system.

**Data-linking Program / Common or Integrated Program or Activity**

If the initiative involves a data-linking program or common or integrated program or activity, as defined by *FIPPA,* the University must notify the Office of the Information and Privacy Commissioner of British Columbia (OIPC) at an early stage of the development of the PIA.

Data-linking means the linking, temporarily or permanently, of two or more data sets using one or more common keys. A data-linking program means a program of a public body that involves data-linking of at least one data set in the custody or under the control of a public body is linked with a data set in the custody or under the control of one or more other public bodies or agencies without the consent of the individuals whose personal information is contained in the data set.

A common or integrated program or activity is defined as a program that provides one or more services through a public body and one or more other public bodies or agencies working collaboratively, or one public body working on behalf of one or more other public bodies or agencies and is confirmed by regulation as being a common or integrated program or activity.

**Who is Responsible for a PIA**

PIAs should be drafted by the program manager responsible for the implementation of the initiative, system, or program. The University’s Privacy Officer/Head or delegate is responsible for the approval of the PIA ensuring compliance with *FIPPA* before implementation. In developing a PIA, the project manager must work closely with the Privacy Officer and, when necessary, the Information Technology Department.

**How to Write a PIA**

A PIA template that includes instructions on how to complete it can be accessed here.

**Questions**

If you have any questions regarding this Guide or the completion of a Privacy Impact Assessment, please contact PIA@viu.ca.

**Additional Resources:**

*Freedom of Information and Protection of Privacy Act*: <https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00>

BC Government PIA website: <http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page>

**Part 1 - General**

|  |  |
| --- | --- |
| **Name of Department:** |  |
| **PIA Drafter:** |  |
| **Email:** |  | **Phone:**  |  |
| **Program Manager:** |  |
| **Email:**  |  | **Phone:**  |  |

**1. Description of the Initiative**

**2. Scope of this PIA**

**3. Related Privacy Impact Assessments**

**4. Elements of Information or Data**

|  |  |
| --- | --- |
| **Information Type** | **Information Collected**  |
| Personal Information | **From Students:** **From Third Parties:****From VIU Employees:** |
| Contact details | **From Students:****From Third Parties:****From VIU Employees:**  |
| Account information |  |
| Commercial information  |  |

|  |
| --- |
| *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 unsigned to* *PIA@viu.ca**. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.* |

**Part 2 – Protection of Personal Information**

**5. Storage or Access outside Canada**

**6. Sensitive Personal Information**: Does the project/initiative involve very sensitive personal information? Examples of sensitive personal information include personal health information, genetic and biometric data, personal financial information, geolocation data, criminal records, counselling records, HR records and payroll records. **If so,** will the sensitive personal information collected be stored outside of Canada?

**7. Data-linking Initiative\***

This is not considered a data-linking initiative as contemplated in s.36.1 of FIPPA.

|  |
| --- |
| **In FIPPA, "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. If so, you will need to 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;
 |  |
| 1. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;
 |  |
| 1. 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.
 |  |
| **If you have answered “yes” to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.** |

**8. Common or Integrated Program or Activity\***

This initiative is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

|  |
| --- |
| **In FIPPA, “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.** |
| This initiative involves a program or activity that provides a service (or services); |  |
| 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; |  |
| The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation. |  |
| **Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.** |  |

**9. Personal Information Flow Diagram and/or Personal Information Flow Table**

|  |
| --- |
| **Personal Information Flow Table** |
|  | **Description/Purpose** | **Personal Information**  | **Type (Collection, Use or Retention)** | **FIPPA Authority** |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |

**10. Risk Mitigation Table**

|  |
| --- |
| **Risk Mitigation Table** |
|  | Risk | Mitigation Strategy | Likelihood | Impact |
| 1. |  |  | Low | High |
| 2. |  |  | Low  | High |

**11. Collection Notice**

**Part 3 – Security of Personal Information**

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

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

**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 ministry notify them of the update, correction or annotation?**

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

**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 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?**

**Part 5 – Further Information**

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

**21. Access for Research or Statistical Purposes: 21. Will the information collected be used for research or statistical purposes?**