University of Toronto

Data Protection Questionnaire

This intake form is for information risk assessments of projects or applications, managed internally or through a vendor. The information submitted will allow us to understand the purpose of your project and what is at risk. Skip any questions that you think do not apply, or you don’t have answers to.

Questions in the form helps us establish the:

* purpose and scope of the project
* privacy controls for the data being collected or used
* nature of the agreement with the vendor (if applicable)

If you would prefer to complete this form in the Enterprise Service Centre, please go to: <link here>

# Document Control Information

## Project and Sponsor, University of Toronto

|  |  |
| --- | --- |
| Date |  |
| Project Title |  |
| Sponsoring Department |  |
| Departmental Data Custodian | *who is primarily responsible for the governance of the data collected on the system?* |
| Project Lead  Please enter name and contact details |  |

Contents

[1 Document Control Information 1](#_Toc80275937)

[2 Project Information 2](#_Toc80275938)

[3 Information Collection 6](#_Toc80275939)

[4 Privacy Protection questions 8](#_Toc80275940)

[5 Vendor related questions – answer if known. 9](#_Toc80275941)

# Project Information

|  |
| --- |
| Is this Service Provided by an external vendor or by UofT? *This helps us determine who is responsible for implementing the different security standards assessed.* |
| \_\_\_\_On Premise, managed internally  \_\_\_\_Externally hosted (Off-prem, cloud or Software as a Service)  \_\_\_\_On Premise, managed by a vendor  \_\_\_\_Managed by Internal Staff on a cloud system (e.g. managed by UofT staff in AWS, Azure)  \_\_\_\_Other |
| Project Summary – Current State *If applicable, provide a brief description of the current processes, applications or systems involved that you are looking to improve. Explain the current issues or areas for improvement that is the objective of the proposed project.* |
|  |
| Project Summary – Proposed State *Include any documents or presentations that describe the business case for the solution when you submit this form.*  *Please provide a brief description of the product or service (solution), its purpose, how it functions, service scope and the benefits it is expected to provide to the sponsoring unit, and to the University as a whole. The purpose should outline whether the solution being introduced addresses a new issue or opportunity, replaces an existing service that is at end of life, reduces risk, or a combination of the above.* |
|  |

|  |  |
| --- | --- |
| Data Flow *Provide an overview of how user / University data is collected into the system, where it is stored, and what system components are involved, including any integrations with existing institutional systems (e.g. SSO/Weblogin, ROSI, HRIS, Quercus, etc.). If you have any network or data flow diagrams, you may include it here.* | |
|  | |
| Expected Project launch date When are you planning the product or service be in operation? | |
|  | |
| How long will you be using this application / system? *For example, is this a pilot, proof of concept or limited engagement with the vendor, or will you be using this solution on an ongoing basis. If there is a contract, how frequently will the contract be renewed? This information will help us scope the assessment.* | |
|  | |
| Comment on the impact to your department or the project / service in the event of: *Understanding the impact on your operations of an accidental or malicious compromise on a system is key to understanding and managing risks to University data. Please comment on how important processes in your department may be impacted in each of these cases.* | |
| Unauthorized access to the system or data: |  |
| Unauthorized modification of the system or data: |  |
| Loss of availability to the system or data: |  |

# Information Collection

|  |  |  |  |
| --- | --- | --- | --- |
| Is any personal information collected? *Personal information is any data that can be used to identify a specific individual. Information can be recorded in any format, such as paper records, electronic records, digital photographs, video/audio recordings or maps. Understanding the personal data involved in the project helps us assess the impact should that data be compromised.* | | | **YES/NO**  **(if NO, proceed to section 4)** |
| Approximate number of data subjects/individuals from whom information will be collected or for whom information will be stored annually. *Student and Alumni contact information is protected by FIPPA legislation, and is classified as Level 3 data. Faculty and Staff contact information is publicly available, and is considered to be Level 1 data. Context is important: security controls and protections of a system using/storing the data will have different requirements based on the data classification. Controls in a system storing or processing Level 3 data need to be stronger than those of a system storing or processing Level 1 or Level 2 data.* | | | Student:\_\_\_\_\_  Faculty:\_\_\_\_\_  Staff:\_\_\_\_\_  Alumni:\_\_\_\_\_ |
| Identify the kinds[[1]](#footnote-2) of information involved in the project. Please add rows as needed | | | |
| Data Collection: *Add each data field collected or created through use of the system and the purpose each data point serves.*  *Limiting data collection reduces the risk and /or impact of loss or unauthorized access, use or disclosure for both the individual and the organization*.  *Click here for more information on* [*Limiting Data Collection*](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_collection/)*1* | | | |
| **Information Type or Data field Collected**  Example: First name, last name, email, IP address (Add rows as needed.) | **Purpose of Collection**  Example: Account registration/creation, functionality of system, security log | How is this information collected | |
|  |  |  | |
|  |  |  | |
|  |  |  | |

|  |  |
| --- | --- |
| What is the highest classification of data collected? Please see the [UofT Data Classification](https://isea.utoronto.ca/policies-procedures/standards/data-classification/)  Indicate (level 1, level 2, level 3, level 4 or unknown) | |
| Level 1: \_\_\_\_\_  Level 2: \_\_\_\_\_  Level 3: \_\_\_\_\_  Level 4: \_\_\_\_\_  Unknown:\_\_\_\_\_ | |
| Who will have access to this data / who will the data be shared with? *Please indicate what actions/purposes are being carried out by the individual(s)/role(s) that are accessing information.*  *Limiting access only to those necessary to fulfill the purposes for which it was collected reduces the risk and / or impact of unauthorized access or modification of the data to both individuals and the organization*  *Information on* [*Limiting Use, Disclosure, and Retention*](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/) | |
| Position | Reason for access / for sharing |
|  |  |
|  |  |

# Privacy Protection questions

|  |  |
| --- | --- |
| Notification and Collection – please provide the following: [[2]](#footnote-3) *Under most circumstances, a notice of collection should be displayed whenever you are collecting personal information. If you do not currently display notice of collection, please speak to the*[*FIPP Office*](https://governingcouncil.utoronto.ca/fipp))*about whether you need to develop one for this project.You may also refer to the* [UofT expanded notice of collection](https://governingcouncil.utoronto.ca/sites/default/files/2019-10/EXPANDED%20NOC%20OCT%202019%20FOR%20WEBSITE.pdf). | |
| Provide notice of collection and details of where it is displayed. Otherwise explain why you do not need one. |  |
| Provide details regarding Information retention duration / policy *Discuss with Information Security and the FIPP office as needed*  *Limiting retention is a key component of reducing risks to both individuals and the organization By disposing a*nd securely destroying *information after it is no longer needed, institutions reduce the potential impacts of risks associated with unauthorized access to information.*  *Information on* [*Limiting Use, Disclosure, and Retention*](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/) | |
|  | |

# Vendor related questions – answer if known.[[3]](#footnote-4)

|  |  |
| --- | --- |
| Product Acquisition: Is this a paid or free service? *Understanding the terms under which data is shared with third parties is important to assessing whether the vendor will manage and protect University data to a standard that ensures we can fulfill our privacy and security obligations.* | Subscription:\_\_\_\_\_  License / Acquired: \_\_\_\_\_  Negotiated Contract: \_\_\_\_\_  Free: \_\_\_\_\_ |
| Partners and Sub-contractors - Does the Vendor provide the entire solution? If not, please list partners and sub-contractors. *For example, does the full solution require plug-ins, add-ons or integrations with services developed by other vendors?* | **Yes / If not: List** |
| Does the Vendor intend to share University-provided information with external partners or third parties? This question includes PII as well as business data.[[4]](#footnote-5) *This information can typically be found in the service agreement and/or privacy policy of the vendor.* | **No/ If Yes: List information** |
| Provide Links to Vendor’s website(s) |  |

1. <https://isea.utoronto.ca/policies-procedures/standards/data-classification/> [↑](#footnote-ref-2)
2. The University must ensure that the institution collects personal information only if it has the authority to do so and that notice of collection is provided to the individual in accordance with FIPPA. For more information on collection regulations as it is governed in FIPPA please see sections 38 and 39 of the Act. [↑](#footnote-ref-3)
3. A separate questionnaire will be sent to the Vendor if needed. [↑](#footnote-ref-4)
4. The University requires notification of all external / third-party data sharing agreements. The University prohibits sharing of released PII / PHI with solution partners, except upon explicit permission of the University. Re-use of data outside of stated and agreed-to uses is prohibited, and all data must be verifiably destroyed / returned to the University in event of the sale or change in ownership status of the firm (e.g. bankruptcy). The University at all times retains ownership of solution data. [↑](#footnote-ref-5)