

Information Risk and Risk Management

Assessment: <Solution Name>

|  |  |
| --- | --- |
| Author(s): |  |
| Reviewer(s): |  |
| Date: |  |
| Version: |  |

Contents

Executive Summary 3

Project Rationale 3

Scope Statement 3

Statement of Sensitivity 3

Solution Business Model 3

Risk Summary 3

Introduction 5

This Document 5

Privacy Impact Assessment in Brief 5

Threat / Risk Assessment in Brief 5

Risk Assessment in Brief 5

Risk Management Recommendations 5

Risk Assessment 7

Introduction 7

Privacy Impact Assessment 9

Threat / Risk Assessment 15

Observations 16

Appendix A: Privacy and Risk Assessment Questionnaire 17

Appendix B: Additional Notes and Comments 18

Appendix C: Practical and Vulnerability testing Results 19

Appendix D: Participants 20

University of Toronto 20

<Others> 20

Appendix E: Document Control 21

Version History 21

Reviewers 21

# Executive Summary

## Project Rationale

<Solution Name>, is an institutional system that <provides X service to Y constituents, hosted in Z locations, and is managed by Q organizations>. <The service contains A data for B purposes>.

<Solution Name> is being introduced to <address a new issue or opportunity / replace an existing service that is at end of life / other reason>

## Scope Statement

This document considers System A, System B and, System C. Upstream and downstream systems are out of scope. As the number of external service interfaces is substantial, it is recommended that they be reviewed individually as stand-alone risk assessment exercises. The University’s network on which these services operate are out of scope.

## Statement of Sensitivity

As <Solution Name> interacts with <define> data, <Solution Name> is considered <Public / Confidential / Protected> in nature. Technical recommendations, if any, will reflect the University’s information security guidelines for data at this level of sensitivity.

<Detail the impact of risk to data stored within, or services provided by the solution. Detail penalties or costs associated with the unauthorized, uncontrolled disclosure of modification of assets, the loss or lack of availability of assets, or the inability to monitor or account for the receipt / delivery of the assets. Specify any external contractual and / or legal data protection requirements (e.g. FIPPA, PHIPA, PCI-DSS, etc.)>

## Solution Business Model

<Detail how the proposed solution vendor, if any, intends to support themselves through the provision of this product / service – this has implications on data re-use, service longevity, legal compliance, and data recoverability.>

## Risk Summary

The following table identifies the risk categories assessed, and identifies if they exceed, meet or do not meet current University of Toronto practices and / or performance expectations given the sensitivity of the information handled, threats associated with that data, and known vulnerabilities in the technology or environments through which that information passes.

*This summary is preliminary at this time, and may change with the introduction of new information.*

|  |  |  |
| --- | --- | --- |
| Category | Meets or Exceeds  (Yes, No, N/A) | Remediable  (Yes, No, N/A) |
| Privacy Impact Assessment – PbD Framework |  |  |
| Threat / Risk Assessment – Current Practice |  |  |

The remainder of this document expands on the risk profile of, and risk mitigation recommendations for the project in progressively greater detail.

# Introduction

## This Document

This document consists of the Privacy Impact Assessment (PIA) and the Threat / Risk Assessment (TRA) for the product or service being introduced by the project.

The PIA assesses, documents and addresses privacy risk in the development, implementation and operation of projects to verify project alignment with privacy standards and legal requirements.

The TRA assesses, documents and addresses the risks to Information assets and recommends risk mitigation measures that can, if implemented, lower the risks to acceptable levels.

## Privacy Impact Assessment in Brief

A Privacy Impact Assessment (PIA) is a process for assessing, documenting and addressing privacy risk in the development, implementation and operation of projects which affect personal information. A PIA analyzes data activities and handling of personal information to verify project alignment with privacy standards, legal requirements, including the *Freedom of Information and Protection of Privacy Act* (FIPPA), University policy, practice, and stakeholder privacy expectations. A PIA is an evolving document that describes and evaluates privacy risks as a project progresses, helping decision makers understand and address those risks as they become evident.

## Threat / Risk Assessment in Brief

A Threat / Risk Assessment (TRA) is a process for assessing, documenting and addressing risk to information assets. Threats and risks are articulated in relation to how sensitive or valuable the information is, and what vulnerabilities are inherent in the environments through which the information passes, is stored, or is used.

## Risk Assessment in Brief

The purpose of completing the PIA and TRA are to make clear the potential risks and risk management options associated with the proposed solution. In deciding whether to adopt a solution or not, University decision makers must decide to accept or reject the residual risks identified by the PIA and TRA processes. (See [Summary of Residual Risks](#_Summary_of_Residual_1) Chart on page 5)

## Risk Management Recommendations

### Summary of Privacy Recommendations

#### Proactive not Reactive; Preventative not Remedial

<Summary of Recommendations>

#### Privacy as the Default Setting

<Summary of Recommendations>

#### Privacy Embedded into Design

<Summary of Recommendations>

#### Full Functionality – Positive-Sum, not Zero-Sum

<Summary of Recommendations>

#### End-to-End Security – Full Lifecycle Protection

<Summary of Recommendations>

* + - 1. ***Visibility and Transparency – Keep it Open***

<Summary of Recommendations>

#### Respect for User Privacy – Keep it User-Centric

<Summary of Recommendations>

### Summary of Information Security Recommendations

<Summary of Recommendations>

# Risk Assessment

## Introduction

### Purpose of This Document

The **Risk Impact Assessment** document details how information is, or is proposed to be used by a project; the sensitivity of that information; the University’s obligations to protect that information; threats and vulnerabilities which create risk of misuse of that information; and options to manage risk to enable the University to meet those obligations if unacceptable unmanaged risks exist. The two tools that the RIA uses to achieve these ends are the Privacy Impact Assessment (PIA) and the Threat / Risk Assessment (TRA) – as both of these tools deal with risk to information, there is some overlap in content, however the focus of each is distinct and different: The PIA is primarily concerned with the anticipated uses of information and the intentions of service designers in support of maintaining the privacy of personally identifiable information; the TRA, a more technical document, is primarily concerned with identifying vulnerabilities in proposed systems and services, and how those vulnerabilities may be mitigated to create a more secure operational environment for all information within it. Further details of how the PIA and the TRA achieve their ends are detailed below.

### What is a Privacy Impact Assessment?

A **Privacy Impact Assessment** (PIA) is a process for determining and addressing privacy risk during the development, implementation and post-completion operation of services that involve or affect personal information. A PIA is a living document that develops with the service project, aligning with project milestones and decision points. A PIA typically contains a description of the project, a detailed transaction-level examination of data flows and an assessment of how those data flows align with legal, policy, practice and stakeholder expectations. This analysis, together with mitigation strategies for identified privacy concerns, provides a tool for decision makers to understand the privacy risk present in the project. The purpose of this document is to delineate the risks along with possible mitigations for each. The remaining residual risks to privacy, after possible mitigations have been applied, is also set out for decision makers to decide whether residual risks are acceptable to the University or may require further mitigation.

Many methodologies exist for conducting PIAs. The University structured its PIA on the **Privacy by Design** (PbD) principles developed by the **Information and Privacy Commissioner** / Ontario (IPC). The assessment is structured around one overarching question about compliance with each of the seven PbD principles and a set of more detailed questions to more closely examine how the principle has been implemented. It is the University’s experience that this approach yields a more detailed and complete understanding of privacy implications than older, more traditional PIA approaches, particularly given the inability to obtain detailed, transaction-level data flows from the proposed cloud service provider.

The University is regulated under the Ontario **Freedom of Information and Protection of Privacy Act** (FIPPA) legislation. Protection of privacy is not only a legal requirement, but a reasonable expectation for activities involving personal information. Careful protection of personal information is a necessary, responsible institutional practice, particularly in response to increasing threats to personal privacy. The focus of this assessment is to highlight risks to privacy in order to ensure that:

* Personal information is protected against unauthorized collection, use and disclosure;
* All information created or maintained through this project remains accessible to the University for proper institutional purposes;

A critical focus of the PIA is the IPC's foundational privacy principle that the privacy of the University’s staff and faculty not be an afterthought to the external service provider, but rather has been built into the project from the beginning. The PIA delineates flows of personal information, examines privacy risks at identified critical points and transactions, including analysis of FIPPA-specific risk. These analyses are compiled into a summary of residual risk remaining after possible mitigations are applied, to be accepted or rejected by University decision makers.

### What is a Threat / Risk Assessment?

A **Threat / Risk Assessment** (TRA) is a process for determining the risk to assets, based on the value of those assets, threats which may cause the assets to be destroyed, or inappropriately divulged, accessed or modified. The TRA also attempts to inform choices for risk mitigation during the development, implementation and post-completion operation of services that involve or affect information or information handling / storage / administration infrastructure.

As with a PIA, a TRA is a living document that develops with the service project, aligning with project milestones and decision points. A TRA contains an enumeration of information assets, their sensitivity, and details how controls are applied to that information throughout its lifecycle. The TRA will indicate the level of risk exposure at each stage of the information lifecycle, and whether this level of risk meets, exceeds, or is on par with currently accepted risk for information of similar sensitivity in similar contexts.

The TRA will identify:

1. Data within the scope of the TRA;
2. Data sensitivity to:
   1. Risk of disclosure, alteration, loss, and unrecorded use or repudiation of receipt;
   2. Agents or events that could cause such undesired outcomes to be realized; and
   3. Vulnerabilities that would enable threats to have an impact.
3. Risk mitigation strategies that address specific vulnerabilities.

This analysis also encompasses all of the above for supporting access, change, continuity, and accountability control systems.

## Privacy Impact Assessment

### Summary

Overall, the XXXX system meets the Privacy needs of the University. There are no recommendations for the following sections:

* Proactive not Reactive; Preventative not Remedial
* Privacy Embedded into Design
* Full Functionality – Positive-Sum, not Zero-Sum
* Visibility and Transparency – Keep it Open
* Respect for User Privacy – Keep it User-Centric

There are minor gaps identified in the Privacy as the Default Setting and End-to-End Security – Full Lifecycle Protection that are described in those sections.

|  |  |  |
| --- | --- | --- |
| Category | Meets or Exceeds  (Yes, No, N/A) | Remediable  (Yes, No, N/A) |
| Privacy Impact Assessment – PbD Framework |  |  |
| Proactive not Reactive; Preventative not Remedial |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Analysis – Privacy By Design

#### Proactive not Reactive; Preventative not Remedial

The *Privacy by Design* (*PbD*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen.

* 1. Is there clear commitment at the highest levels to set and enforce high privacy standards?

<Yes / No>

<Details>

* 1. Does the project anticipate and prevent privacy invasive incidents before they happen?

<Yes / No>

<Details>

* 1. Is there a methodology to recognize and correct poor privacy design, practices and outcomes well before they occur?

<Yes / No>

<Details>

* 1. What gaps remain?

<Details>

#### Privacy as the Default setting

* 1. Is personal information automatically protected in IT system, business practice and physical design?

<Yes / No>

<Details>

* 1. Is the purpose for the collection, use, retention and disclosure of personal information clearly communicated to the individual at or before the collection?

<Yes / No>

<Details>

* 1. Is the collection, use, retention and disclosure of personal information limited to the strict minimum necessary, and consistent with individual consent, including secure destruction?

<Yes / No>

<Details>

* 1. Does the project meet or exceed the requirements of FIPPA?

<Yes / No>

<Details>

* 1. What gaps remain?

<Details>

#### Privacy Embedded Into Design

* 1. Is privacy embedded into the architecture of IT systems and operations in a holistic, integrative and creative way?

<Yes / No>

<Details>

* 1. Has a systemic, principled approach to embedding privacy been adopted, relying upon accepted standards and frameworks, which are amenable to external reviews and audits?

<Yes / No>

<Details>

* 1. Has a detailed privacy impact and risk assessment been carried out and published, documenting the privacy risks and measures taken to mitigate those risks?

<Yes / No>

<Details>

* 1. What gaps remain?

<Details>

#### Full Functionality – Positive-Sum, not Zero-Sum

* 1. Are all system requirements optimized to include full functionality, privacy and security?

<Yes / No>

<Details>

* 1. Are all legitimate non-privacy objectives embraced and accommodated in an innovative, positive-sum manner?

<Yes / No>

<Details>

* 1. What gaps remain?

<Details>

#### End-to-End Security - Full Lifecycle Protection

* 1. Are there strong security measures in place throughout the lifecycle of the data so that the data is retained securely?

<Yes / No>

<Details>

* 1. Are the security measures consistent with standards developed by recognized bodies?

<Yes / No>

<Details>

* 1. Do the security standards assure the confidentiality, integrity and availability of the personal information including secure destruction, appropriate encryption and strong access controls and logging methods?

<Yes / No>

<Details>

* 1. What gaps remain?

<Details>

#### Visibility and Transparency – Keep it Open

* 1. Is responsibility for privacy-related policies and procedures documented, communicated and assigned to a specific individual?

<Yes / No>

<Details>

* 1. Is there trust of the vendor and is privacy protection assured by the vendor through contractual or other means, e.g. no data mining, no ads?

<Yes / No>

<Details>

* 1. Is information about the policies and procedures relating to the management of personal information readily available to individuals?

<Yes / No>

<Details>

* 1. Have complaint and redress mechanisms been established and communicated to individuals?

<Yes / No>

<Details>

* 1. Have steps been taken to monitor, evaluate and verify compliance with privacy policies and procedures?

<Yes / No>

<Details>

* 1. What gaps remain?

<Details>

1. Respect for User Privacy – Keep it User-centric
   1. Are data subjects empowered to play an active role in the management of their own data?

<Yes / No>

<Details>

* 1. Has free and specific consent been established for the collection, use or disclosure of personal information and can consent be withdrawn? Are individuals given a clear Notice of the uses and disclosures or their personal information?

<Yes / No>

<Details>

## Threat / Risk Assessment

### Analysis

<The proposed solution> contains considerable sensitive, personal information that represents a considerable risk to the University, should it be improperly disclosed, modified, or managed.

A review of the solution and its technical infrastructure indicates that control mechanisms in the <network / server / application> <meet / do not meet / exceed> the University of Toronto’s Information Security Baseline. <Recommendations are indicated, with additional details in the following section, as appropriate>.

|  |  |  |
| --- | --- | --- |
| Category | Meets or Exceeds  (Yes, No, N/A) | Remediable  (Yes, No, N/A) |
| Threat / Risk Assessment – Current Practice |  |  |
| Access Controls |  |  |
| Change Controls |  |  |
| Business Continuity Practices |  |  |
| Access, Change, and Fault Reporting |  |  |

#### Access Controls

“Does the solution’s identification and authentication component integrate with existing University systems in support of single credential and once-only sign-on? Are they of sufficient strength to thwart circumvention, replay, or other attacks on authorized access?”

<Details>

#### Change Controls

“Does the solution’s authorization mechanisms integrate with existing University systems? Are they of sufficient strength to thwart known attacks?”

<Details>

#### Business Continuity

“Does the solution implement continuity controls sufficient to ensure the availability of the solution, as per the University’s needs?”

<Details>

#### Access, Change and Availability Fault Monitoring

“Are Access, Change, and Availability controls tested on a periodic basis (no less than annually), or after every significant change to the solution or its environment? Are solution events proactively reported and analysed on an on-going basis to identify potential attacks?”

<Details>

### Testing Results

The results of compliance, sufficiency, and practical / vulnerability audits / assessments of the solution, if any.

<Details>

# Observations

<Plain-English comments on the results of testing and their implications for the Threat / Risk Assessment Analysis section. Comments may, but is not limited to reflecting on the sufficiency of testing, the veracity of provided information, or the maturity of the product or service.>

# 

Appendices

1. Privacy and Risk Assessment Questionnaire

<Insert responses to ‘Privacy and Risk Assessment Questionnaire’>

# Additional Notes and Comments

<Any information that you think is relevant to the assessment that has not been addressed above, please provide it here.>

# Practical and Vulnerability testing Results

<Insert results here, if practical and vulnerability tests were conducted>

# Participants

The following is a listing of partners and their role in this document.

## University of Toronto

### Information + Technology Services

|  |  |
| --- | --- |
| Name | Role |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### Freedom of Information and Protection of Privacy office

|  |  |
| --- | --- |
| Name | Role |
|  |  |
|  |  |

## <Others>

### <Name>

|  |  |
| --- | --- |
| Name | Role |
|  |  |
|  |  |
|  |  |
|  |  |

# Document Control

## Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Summary of Changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Reviewers

This table identifies leaders that have been involved in the development of the document. This is not a list of sign-offs or approvals.

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer | Role | Version | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |