

Information Risk and Risk Management

Staff and Faculty E-Communications Outsourcing Project

|  |  |
| --- | --- |
| Author(s): | Matt WilksAxel JohnstonMartin Loeffler |
| Reviewer(s): | Martin Loeffler |
| Date: | 09/16/2013 |
| Version: | 1.2.9 |

Contents

[Executive Summary 4](#_Toc366771250)

[Project Rationale 4](#_Toc366771251)

[Risk Summary 4](#_Toc366771252)

[Introduction 5](#_Toc366771253)

[This Document 5](#_Toc366771254)

[Privacy Impact Assessment in Brief 5](#_Toc366771255)

[Threat / Risk Assessment in Brief 5](#_Toc366771256)

[Risk Management Recommendations 5](#_Toc366771257)

[Summary of Privacy Recommendations 5](#_Toc366771258)

[Summary of Information Security Recommendations 6](#_Toc366771259)

[Cost Summary 6](#_Toc366771260)

[Risk Assessment 7](#_Toc366771261)

[Introduction 7](#_Toc366771262)

[Project Description 7](#_Toc366771263)

[Purpose of This Document 7](#_Toc366771264)

[What is a Privacy Impact Assessment? 7](#_Toc366771265)

[What is a Threat / Risk Assessment? 8](#_Toc366771266)

[Risk Assessment 10](#_Toc366771267)

[Privacy Impact Assessment Summary 10](#_Toc366771268)

[Privacy Impact Assessment Analysis 10](#_Toc366771269)

[Other Jurisdictions 11](#_Toc366771270)

[Carleton University 11](#_Toc366771271)

[Dalhousie University 11](#_Toc366771272)

[Queen’s University 11](#_Toc366771273)

[University of Alberta 11](#_Toc366771274)

[Lakehead University 11](#_Toc366771275)

[US peers (Washington, Arizona State, USC) 12](#_Toc366771276)

[alumni.utoronto.ca 12](#_Toc366771277)

[Resources Consulted 12](#_Toc366771278)

[*Threat / Risk Assessment Summary* 14](#_Toc366771279)

[*Threat / Risk Assessment Analysis* 15](#_Toc366771280)

[**1.** **Software to be installed on University of Toronto premises.** 15](#_Toc366771281)

[**2.** **Networked Hardware / Appliances – to be installed on University of Toronto premises.** 15](#_Toc366771282)

[**3.** **Outsource ('Cloud') Services – outside of University premises** 15](#_Toc366771283)

[**4.** **Professional Services** 17](#_Toc366771284)

[**5.** **Development Services** 17](#_Toc366771285)

[Appendix A: Privacy by Design Analysis 18](#_Toc366771286)

[Privacy by Design Summary 18](#_Toc366771287)

[**1. Proactive not Reactive; Preventative not Remedial** 19](#_Toc366771288)

[Does the Project take proactive and preventive measures? 19](#_Toc366771289)

[**2. Privacy as the Default setting** 22](#_Toc366771290)

[Is Privacy the Default setting? 22](#_Toc366771291)

[**3. Privacy Embedded Into design** 26](#_Toc366771292)

[Is Privacy Embedded into the Design? 26](#_Toc366771293)

[Stakeholder Expectations 27](#_Toc366771294)

[SAS70 Type II Attestation 29](#_Toc366771295)

[**4. Full Functionality – Positive-Sum, not Zero-Sum** 31](#_Toc366771296)

[Is there Full Functionality in a Positive Sum manner? 31](#_Toc366771297)

[Cloud Computing 32](#_Toc366771298)

[Data Residency 32](#_Toc366771299)

[Foreign Legislation 32](#_Toc366771300)

[**5. End-to-End Security - Full Lifecycle Protection** 34](#_Toc366771301)

[Does the Project Apply End-to-End Security, achieving Full Lifecycle Protection? 34](#_Toc366771302)

[Data Flows Analysis 34](#_Toc366771303)

[**6. Visibility and Transparency – Keep it Open** 37](#_Toc366771304)

[Does the project operate with visibility, transparency and openness? 37](#_Toc366771305)

[Verification of Privacy Policies and Commitments 38](#_Toc366771306)

[**7. Respect for User Privacy – Keep it User-centric** 40](#_Toc366771307)

[Is there a user-centric respect for User Privacy? 40](#_Toc366771308)

[Summary 40](#_Toc366771309)

[Appendix B: Analysis of Residual Risks 41](#_Toc366771310)

[Residual Risk Solutions 41](#_Toc366771311)

[Summary of Residual Risks 41](#_Toc366771312)

[Proxy Server Compromise 43](#_Toc366771313)

[Unknown Software Vulnerabilities 44](#_Toc366771314)

[Microsoft Employee Acting Without Authorization 44](#_Toc366771315)

[Accidental disclosure by a Microsoft employee 45](#_Toc366771316)

[Foreign Legislative Threat 45](#_Toc366771317)

[Attacks from within the cloud 46](#_Toc366771318)

[Mishandling of data by University of Toronto 47](#_Toc366771319)

[Updates to O365 Break Functionality 48](#_Toc366771320)

[Disclosure of Sensitive Data 48](#_Toc366771321)

[Improper Termination of Agreement 48](#_Toc366771322)

[Appendix C: FIPPA Risk Analysis 50](#_Toc366771323)

[Collection 50](#_Toc366771324)

[Use 51](#_Toc366771325)

[Disclosure 51](#_Toc366771326)

[Retention 52](#_Toc366771327)

[Disposal 53](#_Toc366771328)

[Security 53](#_Toc366771329)

[Appendix D: Office365 Dataflows and Processes 54](#_Toc366771330)

[Appendix E: USA PATRIOT Act 62](#_Toc366771331)

[Appendix F: FIPPA Definition of Personal Information 63](#_Toc366771332)

[Appendix G: Privacy by Design Principles 64](#_Toc366771333)

[Appendix H: CSA Privacy Code Principles 65](#_Toc366771334)

[Appendix I: Technology Overview 66](#_Toc366771335)

[SSL/TLS 66](#_Toc366771336)

[Shibboleth 66](#_Toc366771337)

[Appendix J: Cloud Computing Models 68](#_Toc366771338)

[Work Units 70](#_Toc366771339)

[University of Toronto 70](#_Toc366771340)

[Information + Technology Services 70](#_Toc366771341)

[Freedom of Information and Protection of Privacy office 70](#_Toc366771342)

[Microsoft 71](#_Toc366771343)

# Executive Summary

## Project Rationale

UTORmail, the University’s legacy institutional email service, is near end-of-life and requires significant investment to bring up to current industry standards. The University successfully migrated the student email system to the Microsoft Live@edu system in 2011 and is now considering moving the email services of staff and faculty to the Microsoft Office365 system, the successor to Live@edu.

The suite of tools offered through Office365 represents an improvement to the university status quo in the form of much larger mailbox quotas, calendaring services, Office Web Apps, and SharePoint Online Collaboration.

The objective of the project is to migrate faculty and staff e-communications to Microsoft Office365.

## 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 | Assessment | Remediable |
| Privacy Impact Assessment |  |  |
|  Privacy By Design Guidelines | Meets | NA |
| Threat / Risk Assessment |  |  |
|  Access Controls | Meets | NA |
|  Change Controls | Exceeds | NA |
|  Business Continuity Practices | Exceeds | NA |
|  Access, Change, and Fault Reporting | Meets | NA |

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.

In deciding whether to proceed 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 41)

## Risk Management Recommendations

### Summary of Privacy Recommendations

#### Proactive not Reactive; Preventative not Remedial

No recommendations.

#### Privacy as the Default Setting

No recommendations.

#### Privacy Embedded into Design

No recommendations.

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

No recommendations.

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

No recommendations.

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

No recommendations.

### Summary of Information Security Recommendations

#### Access Controls

No recommendations.

#### Change Controls

No recommendations.

#### Business Continuity Practices

No recommendations.

#### Access, Change, and Fault Reporting

No recommendations.

### Cost Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Ref | Recommendation | Cost | Benefit |

|  |  |  |  |
| --- | --- | --- | --- |
| NA | No Recommendations. |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

# Risk Assessment

## Introduction

### Project Description

Reports from I+TS staff demonstrated that UTORmail (the University’s legacy institutional email service) is near end-of-life and requires significant investment to bring up to current industry standards. As a result, the University migrated the student email system to Live@edu hosted by Microsoft. In light of this successful migration, the University is considering moving the email services of staff and faculty to the Office 365 platform, the successor to Live@edu. Staff and faculty are currently either using UTORmail (email only) or UTORExchange (email and calendaring) for their e-communications platform. The suite of tools offered through Office 365 represents an improvement to the university status quo in the form of ubiquitous calendaring, and much larger inbox quotas. Other features under consideration include Office Web Apps, and SharePoint Online Collaboration.

This project represents a major shift in the way that the University provides its email service to staff and faculty. Staff and faculty email will be stored off-campus in data centers that are not located in Canada, raising the issue of applicability of foreign legislation to this data and loss of local control. The addition of document collaboration tools will also result in confidential data being stored in off-campus data centers. With this shift away from internally managed email / document collaboration comes the need to establish a level of trust with Microsoft appropriate to the sensitivity of the personal and confidential information that will be stored in email and the other tools offered. Although Microsoft ensures the security and privacy of information on its systems, the University will oversee the continuing protection of private and confidential information in this process.

### Purpose of This Document

The **Information Risk and Risk Management** 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 IRRM 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;
* The contract signed with the external provider meets or exceeds FIPPA requirements.

### 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.

## Risk Assessment

## Privacy Impact Assessment Summary

Microsoft has demonstrated a strong commitment to Privacy and security to the University, in its online materials, and in the design of its services. Microsoft has and will annually continue to provide the University with the results of its SAS70 Type II external audit. This PIA finds that Microsoft’s physical and logical controls and staff training for data center employees evidence an approach to privacy consistent with University standards in the context of student e-communications.

## Privacy Impact Assessment Analysis

The University is regulated under FIPPA legislation. Consideration was given to PIPEDA (The Personal Information Protection and Electronic Documents Act) since the University is contracting with a private sector service provider. The website of the Federal Privacy Commissioner states; “...our Office is of the view that, as a general rule, PIPEDA does not apply to the core activities of municipalities, universities, schools, and hospitals.”[[1]](#footnote-1) Although Microsoft's commercial activities would normally be covered by PIPEDA, in this instance it is acting as an agent of the University and so relevant privacy requirements are those set out in FIPPA, which applies to the University. PIPEDA legislation is therefore not specifically addressed in this PIA, although Microsoft will comply with legal requirements applicable to it. 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 in the context of staff / faculty e-communications;
* All information created or maintained through this project remains accessible to the University for proper institutional purposes; and
* The contract signed with the external provider meets or exceeds the requirements of applicable legislation (FIPPA).

This PIA comprises a description of the staff and faculty e-communications project; stakeholder expectations; similar experiences of other universities and; a list of resources consulted. Particular attention has been given to the SAS70 Type II audit provided by Microsoft.

The PIA considers the use of a cloud platform for University e-communications. 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. The PIA considers, and must be read in conjunction with, the Office 365 contract with Microsoft.

## Other Jurisdictions

In addition to key stakeholder input, experiences of universities that outsourced email services were examined. Thousands of universities worldwide have outsourced email services, including several in Canada, such as University of Alberta (U of A), which outsourced student, staff and faculty email to Google Inc. At this early stage in adoption of cloud e-communications, other universities’ experiences provided useful context for the University of Toronto exercise.

### Carleton University

Carleton University deployed Office 365 to their student population in March 2012. As a result of the success of that project and their experience thus far, they have initiated a project to move Faculty and Staff e-mail to Office 365 in the foreseeable future. According to Jamie Campbell, Asst. Director, Information Security & Operating Platforms at Carleton “The email protection services (e.g. anti SPAM, antivirus) provided as part of Office 365 exceed the in-house email security services used to protect our legacy student email service. As a result, students have been less exposed to these types of security attacks since our move to Office 365”

### Dalhousie University

### Queen’s University

### University of Alberta

U of A outsourced student, faculty and staff email to Google’s *Apps for Education* platform in March 2011. Vice Provost Jonathan Schaeffer stated; “moving to Google will ultimately have a positive and transformative effect on teaching and learning on campus.” The University of Alberta conducted a detailed Privacy Impact Assessment which was reviewed by the Alberta Privacy Commissioner. Other Canadian Universities followed U of A’s Google negotiations with great interest and provided support. “More than 20 Canadian universities and the Canadian University Council of Chief Information Officers sent Google letters of support during a low point in negotiations last July, indicating interest in accepting Gmail if a legal framework like the one the U of A wanted was in place.”[[2]](#footnote-2) U of A’s success in negotiating a contract that prohibits Google from mining user data or sharing personal information with third parties is expected to support the inclusion of similar terms in similar contracts at other universities, including the U of T contract with its service provider.

Lakehead University
Lakehead University (Lakehead) has used Google for faculty, staff and student email since 2007. A grievance was filed by the Lakehead University Faculty Association, stating that Lakehead was violating privacy and academic freedom by outsourcing faculty email to a US company (subject to the USA PATRIOT act). The arbitrator found for Lakehead and dismissed the Faculty Association's grievance[[3]](#footnote-3).

### US peers (Washington, Arizona State, USC)

USC, ASU and U Washington shared many details of their Google experience:

1. Few uptime issues; if there is downtime, people seem to understand and accept more readily than when local systems go down.
2. Students self-migrate and adopt services readily
3. “Students thrilled!” – Kari Barlow, AVP University Technology Office, ASU
4. “Our experience has been positive. Each of the moves [they have other outsourcing arrangements as well] has decreased our costs, improved our reliability, and made our services more predictable. This is a core element of our information technology strategy, and it has accelerated our advancement.” Dr. Adrian Sannier, VP and University Technology Office, ASU
5. USC annual IT survey for students has had Google Apps as the favourite service since it was introduced.

alumni.utoronto.ca
The Division of University Advancement has offered alumni accounts in partnership with Google for some years. They report:

1. Alumni experience has been good. Alumni respond well to the offer.
2. Close to 15,000 active accounts although more are on the system.
3. Of affinity services, Google Mail is most popular, helping drive alumni to other offerings and communities.
4. Graduating students are eager to take advantage of service. They appreciate the storage and the service levels. They have not experienced problems with email forwarding as with other services.

While most of these examples are from universities who chose to use Google’s email services, the fundamental questions of privacy and security remain the same with Microsoft’s *Office365*.

## Resources Consulted

Some of the key resources consulted in the creation of this PIA are:

* *P*[*rivacy by Design: The 7 Foundational Principles*](http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf)[[4]](#footnote-4) (Ann Cavoukian, Ph.D.)
* [*Modelling Cloud Computing Architecture Without Compromising Privacy*](http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf)[[5]](#footnote-5) (NEC Company and Information Privacy Commissioner Ontario, Canada)
* [*Operationalizing Privacy By Design: The Ontario Smart Grid Case Study*](http://www.privacybydesign.ca/content/uploads/2011/02/pbd-ont-smartgrid-casestudy.pdf)[[6]](#footnote-6)
* [*Privacy in the Clouds*](http://www.privacybydesign.ca/content/uploads/2008/05/privacyintheclouds.pdf)[[7]](#footnote-7) (Ann Cavoukian, Ph.D.)
* [*7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age*](http://www.privacybydesign.ca/content/uploads/2006/10/7laws_whitepaper.pdf)[[8]](#footnote-8) (Ann Cavoukian, Ph.D)
* Microsoft’s RFA response (provided by Microsoft under NDA)
* SAS70 Type II Attestation (provided by Microsoft under NDA)
* Online Services Information Security Policy (provided by Microsoft under NDA)
* [*Microsoft and Data Privacy – Helping to Protect Personal Information in the Digital Age*](http://download.microsoft.com/download/B/C/A/BCAD4354-99E8-4A80-BCE3-210A74ECFA6C/Microsoft_and_Data_Privacy_final.pdf)[[9]](#footnote-9) (Microsoft)
* [*Microsoft and Data Retention*](http://download.microsoft.com/download/7/9/8/7988DF4C-142E-4A29-96BE-2384C524AB68/TwC-Enterprise-CTZ%203-Data%20Governance-Data%20Retention-BackgrounderFS.docx)[[10]](#footnote-10) (Microsoft)
* [*Privacy Guidelines for Developing Software Products and Services*](http://download.microsoft.com/download/3/8/5/385BEAE9-72E9-4F7F-A798-9D54F896351A/privacy_guidelines_for_developers.pdf)[[11]](#footnote-11) (Microsoft)
* [*Privacy in the Cloud Computing Era – A Microsoft Perspective*](http://download.microsoft.com/download/3/9/1/3912E37E-5D7A-4775-B677-B7C2BAF10807/cloud_privacy_wp_102809.pdf)[[12]](#footnote-12) (Microsoft)
* [*Securing Microsoft’s Cloud Infrastructure*](http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf)[[13]](#footnote-13) (Microsoft)
* [*Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*](http://www.cloudsecurityalliance.org/csaguide.pdf)[[14]](#footnote-14) (Cloud Security Alliance)
* *University of Alberta PIA For Outsourcing Email* (provided by UofA under NDA)

*Threat / Risk Assessment Summary*

The security – both physical and logical – applied by Microsoft provides risk mitigation every bit as good as, and in many ways better, than what currently is provided by the University of Toronto to any of the University’s many email systems. As such, a decision to proceed to out-source the provision of email services to Office 365, will accrue a net security benefit to the University, with an investment of time and effort considerably less than that required for the University to provide the same benefit in-house. That said, there are a number of observations that came out of the process of pursuing the Office 365 service:

1. It is clear that the business relationship is key, and that near-constant contact was required to ensure that matters of service implementation were successfully resolved to the University’s satisfaction – the University must be prepared to sustain this level of collaborative effort, as the greater part of the potential of the Office 365 service is yet to be realized, and will not be realized without appropriate effort.
2. While the University of Toronto engages in internal security vulnerability testing and does respond to information security incidents in a timely manner, it is recommended that the University develop regular, formalized, network and IT service vulnerability scanning and Computer Security Incident Response (CSIRT) practices in support of our obligations as customers of Office365. This practice may be more economical to develop internally than to source externally, while providing the same value, and would bring the University’s practices more in line with that of current best practice.
3. The University should consider maintaining a core of knowledge about the management and provision of email services, should the University ever decide that re-insourcing emails services is an attractive option.
4. The impact of recent allegations in the media that Internet traffic, even encrypted Internet traffic, is not secure in the context of a threat with nation-state level resources has been evaluated in this assessment. Network traffic, once it leaves the University’s physical network, has never been considered to be a secure form of communication; as such, the security of information outside of the University’s networks cannot be decreased. In addition, the nature of work done at the University is often performed over remote networks, and / or in collaboration with individuals at other institutions – even if systems physically located on the University network are a common nexus point. As such, given the already highly distributed nature of our work that is dependent on non-University of Toronto networks, the use of an outsourced network service provider does not represent a new exposure to risk.

*Threat / Risk Assessment Analysis*

Threat / Risk Assessment Questionnaire

*Note: Not every section (Software / Hardware / Outsourced and Contracted services) will be appropriate for all projects – only complete the appropriate sections.*

1. **Software to be installed on University of Toronto premises.**

Not applicable

1. **Networked Hardware / Appliances – to be installed on University of Toronto premises.**

Not applicable

1. **Outsource ('Cloud') Services – outside of University premises**
	1. ***Identification and Authentication***
		1. Is the solution SAML 2.0 compliant (i.e. will it work with Shibboleth federated access control software) for the purpose of authenticating users?
* Office 365 will authenticate via Microsoft Active Directory Federation Services which is SAML 2.0 compliant.
	1. ***Authorization***
		1. What degree of granularity does the solution offer in defining roles?
* Office 365 provides for a great degree of granularity in defining roles and assigning permissions.
	1. ***Isolation***
		1. What security standards are followed in the operation of the service?
* Office 365 facilities and services are protected as detailed in Microsoft’s internal security standard, which meet or surpass the University of Toronto’s security standards.
	+ 1. Is compliance with internal security standards assessed via a SAS 70 Type II or a CSAE 3416 (formerly CICA 5970) compliance audit, at least annually?
* Yes. SAS 70 Type II.
	+ 1. What external application vulnerability scans / assessments / audits are done? How often?
* Microsoft routinely has Penetration testing performed by internal and external parties.
	+ 1. Does data transit non-Canadian networks? If so, where?
* Yes. The United States of America.
	+ 1. Is data stored outside of Canadian borders? If so, where?
* Yes. The United States of America.
	1. ***Continuity***
		1. What level of availability does the service offer?
* Both Office 365 and University of Toronto services are robust and redundant in design, however, are subject to potential service outages from intervening network service providers – this is an exposure that all users of the Internet are vulnerable to, given the shared nature of the Internet.
	+ 1. What provisions are in place to exit the service?
* The University of Toronto has exit options available to it, should the Office 365 service prove unsatisfactory for whatever reason, such that user data can be fully recovered and migrated to another service provider, or back under the direct administration of the University if so desired.
	+ 1. What provisions are in place to protect intellectual property?
* Routine back up of data, and all back ups are encrypted and secured to the same standards as production data.
	+ 1. What provisions exist for decryption key escrow, for encrypted solutions?
* Not applicable as key escrow is not required for this solution.
	1. ***Reporting***
		1. What activity and resource usage reports are provided?
* The University of Toronto keeps a log of all successful user authentications.
* The University of Toronto keeps a log of all successful authentications by administrative users.
* Activity within the Office 365 service may be monitored through PowerShell scripts.
	1. ***Functionality***
		1. Does the solution follow web standards, such as “REpresentational State Transfer” (REST), or Open Web Application Security Project (OWASP)?
* Yes.
	+ 1. If handling credit card data, is the solution PCI-DSS compliant?
* Credit card data is not handled.
	+ 1. What other, auditable, IT standards are followed (such as operational or security standards)? How often are the audits performed?
* Office 365 facilities and services are protected as detailed in Microsoft’s internal security standard, which meet or surpass the University of Toronto’s security standards. Compliance with these internal standards are verified by annual SAS70-II audit, however the standard itself is protected by NDA (“Non-Disclosure Agreement”) and cannot be published but the University. Attestations made in Microsoft’s internal security standard were verified by a physical inspection of the Microsoft Chicago data centre.
	+ 1. Are the annual results of audits and certifications made available to customers?
* Yes.
1. **Professional Services**

Not applicable.

1. **Development Services**

Not applicable

# Privacy by Design Analysis

Given the nature of cloud computing, the University must ascertain that Microsoft facilities, datacenters and technology resources around the world provide a secure, privacy-protective environment. As a reasonable baseline, this environment should be at least as sound as the U of T resources that it will replace.

## Privacy by Design Summary

Ontario Information and Privacy Commissioner Dr. Ann Cavoukian developed a set of design principles for privacy protective service and systems development, called *Privacy by Design (PbD)*[[15]](#footnote-15), which can be used to address the systemic effects of information technologies and large-scale networked data systems by assessing compliance with seven overarching privacy principles.

One key principle is “Privacy by default” -- privacy assurance and verification, with full commitment from leadership - must be an organization's default mode of operation.

A positive sum approach must also be taken (security, functionality and privacy optimally implemented to support system goals and each other) for IT systems, business practices and physical design and networked infrastructure.

The broadest objectives of *PbD* -- ensuring optimal privacy with effective individual control over personal information can be accomplished by following the seven foundational principles. The principles, set out in Appendix G, are used in this PIA to analyze, establish and demonstrate whether this project meets or exceeds IPC, legal, and community privacy expectations.

## **1. 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. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before the fact, not after.4

### Does the Project take proactive and preventive measures?

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

Yes. How?

#### Microsoft

In a speech in 2010 at the University of Washington, Microsoft CEO Steve Ballmer observed that Microsoft and other online service providers have a responsibility to lead in privacy protection:

“As a big company, we’ve got to lead on privacy.... We have a responsibility, all of us, not just to socially respect the user, but to build the technology that will protect the anonymity, the privacy, the security of what I say, who I say it to, where I go, what’s important to me.”[[16]](#footnote-16)

In 2000, Microsoft established a Corporate Privacy Group and appointed Richard Purcell as senior director of privacy, which was the first appointment of a chief privacy officer by a multinational company. Microsoft has articulates its commitment to Privacy by Design on the Microsoft Privacy website (<http://www.microsoft.com/privacy/bydesign.aspx>), which is comprised of people, processes, technologies, features and research intended to secure infrastructure and client data. All new Microsoft employees receive privacy training. Microsoft’s central privacy team develops and implements programs for every aspect of their ecosystem, from products, services and processes through physical systems and infrastructure.

The “Microsoft Privacy Standard for Development” governs the development and deployment of Microsoft consumer products, enterprise products, and Web services. It is incorporated into their baseline development guidelines known as Security Development Lifecycle (SDL) with the objective of ensuring that Privacy is built in to all services from the beginning. After development, products and services undergo privacy review designed to ensure ongoing compliance with privacy policies and standards.

In addition to these fundamental privacy commitments, Microsoft also engages in digital privacy technology research. Current projects include a Cryptographic Cloud Structure. The Microsoft privacy website details the importance of projects like this (emphasis added):

“Researchers are working on cryptographic tools that will enable an individual or organization to help secure data stored in the cloud, *even if the data resides on a computer infrastructure that is not controlled or trusted by the user*. Potential outcomes of this project include tools that enable patients to generate and store keys to encrypt their information and give them full control over which organizations can access which portions of their health information.”[[17]](#footnote-17)

#### University of Toronto

University of Toronto leadership values privacy and endorses the seven Foundational Privacy by Design Principles. The University supports a culture of privacy and recognizes the work of Ontario's Information and Privacy Commissioner, in developing the PbD principles.

The University is officially committed to the principles of FIPPA, conducts faculty and staff privacy training, and operates under privacy guidelines, policies and comprehensive data protection guidelines, including a security baseline, designed to support a security culture where systems and procedures are crafted to prevent and address emerging security challenges[[18]](#footnote-18). These resources incorporate and detail core privacy principles including data minimization, need-to-know, record schedules and secure destruction. The University recognizes and follows Privacy by Design principles, the highest security standards, and conducts TRAs and PIAs for projects involving personal and confidential information.

One way that the University demonstrates its strong commitment to privacy and security is by maintaining full time director level positions and active programs to oversee protection of privacy and of information security.

##### Does the project anticipate and prevent privacy invasive incidents before they happen?

Yes. How?

#### Microsoft

Microsoft uses risk management processes[[19]](#footnote-19) such as asset management, physical and logical access controls, change management and security surveillance to attempt to identify and mitigate risks before they become problems. In addition to proactive and preventive privacy measures, Microsoft monitors its infrastructure closely to ensure its security and privacy controls are effective. While Microsoft security controls and management processes are designed to reduce the risk of security incidents, it would be naïve to expect problems and attacks not to happen. Microsoft employs a Security Incident Management (SIM) team to respond to attacks, 24 hours a day, 7 days a week. The SIM has a 6 phase incident response process including training, identification, containment, mitigation, recovery and analysis of lessons learned.

#### University of Toronto

The University is undertaking this PIA to anticipate and prevent privacy issues before they happen. Prior to the expected implementation date a working group will be established specifically to anticipate potential incidents. Key stakeholder feedback will be solicited in various ways. The University benchmarked other jurisdictions’ and institutions’ projects and experiences.

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

#### Microsoft

As described, Microsoft uses a dedicated team of individuals to monitor its infrastructure and services for security and privacy incidents. This Security Incident Management team is expected to respond to issues at all times, to assess and mitigate computer security incidents involving Microsoft's Online Services, while clearly communicating relevant information to senior management and other concerned parties within Microsoft.

In addition, Microsoft conducts many types of internal risk assessments to understand and mitigate the possibility of privacy and security incidents.

#### University of Toronto

The University Information Security team takes an active role to identify and remedy potential privacy breaches. Penetration testing is performed regularly and results given to departments to enable them to better secure resources. The University also uses Intrusion Detection and Prevention Systems (IDS and IPS) to actively monitor the network to detect and prevent threats to critical resources. The Information Security team regularly reviews authentication logs to look for aberrant behaviour that might indicate accounts that have been compromised.

##### What gaps remain?

There are no outstanding gaps. Both Microsoft and the University of Toronto take a proactive approach to protection of privacy. From top leadership to operations, both demonstrate a clear and consistent commitment to the privacy and protection of data that they steward. All reasonable efforts are made to discover, assess, and mitigate potential risks and threats as early as possible.

The University has to be proactive in assessing the nature of the data in the other services offered under Office 365 as well. Applications like document sharing and office web apps host much more different kinds and different levels of sensitive data.

## **2. Privacy as the Default setting**

We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by *default*.4

### Is Privacy the Default setting?

##### Is personal information automatically protected in IT system, business practice and physical design? Yes. How?

#### Microsoft

Microsoft makes privacy its default by employing a deny-by-default design in its physical and logical operations, with policies that deny access by default, following a least privilege principle and reviewing access privileges on a periodic basis.

#### University of Toronto

The University takes a strong stance on protecting data and minimizing access to data by default. The University’s Data Protection Guidelines state:

“Data must be protected from unauthorized access or alteration while the data are in use, in physical or electronic storage, in physical transport or electronic communication, or under administrative access. Access to confidential information must be on a need-to-know basis only; need-to-know requirements must be documented as a requirement of job duties or contractual obligations.“[[20]](#footnote-20)

The Guideline states that access controls for confidential or personal information must be “… proportionate to the risk to the University due to unauthorized disclosure, deletion, modification or duplication of data.”

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

The University articulates its coverage under, and scope of applicability of personal information as protected by FIPPA legislation:

 FIPPA and its Application to the University of Toronto

Beginning June 10, 2006 Ontario universities, including the University of Toronto, are covered by the [Freedom of Information and Protection of Privacy Act](http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm%22%20%5Ct%20%22_blank%22%20%5Co%20%22Click%20here%20to%20download%20a%20copy%20of%20the%20Freedom%20of%20Information%20and%20Protection%20of%20Privacy%20Act) (the Act), which supports access to University records and protection of privacy.

Some key purposes of the Act are:

1. To provide the public a right of access to university information subject to limited exemptions; and
2. To protect the privacy of individuals with respect to personal information about themselves held by universities and to provide individuals with a right of access to that information.

As a publicly funded institution, the University of Toronto has upheld these principles in its operations for many years. [University Statement](http://www.governingcouncil.utoronto.ca/Assets/Governing%2BCouncil%2BDigital%2BAssets/Policies/PDF/ppnov022006.pdf).

What information is covered by the Act?

Most records in the custody or under the control of the University are subject to the Act and the great majority of these will be available if requested. A few types of records, however are specifically excluded so the Act does not apply to them. A few other types are covered by the Act but exempt from disclosure to protect public concerns, privacy, University operations or other important interests.

**Some records which will generally be accessible under the Act include:**

1. Those containing your own personal information;
2. Most university administrative records;
3. Records about the subject matter or amount of funding of University research;
4. Records of University staff employment expenses.

**Examples of records which may not be accessible under the Act include:**

1. Those that are neither in the custody nor under the control of the University;
2. Records donated to the University Archives by a private individual or corporation;
3. Most University labour relations or employment records;
4. Records respecting University research, except the subject matter and the amount of funding related to research;
5. Records available to the public or expected to be published within ninety days;
6. University teaching materials.

(<http://www.fippa.utoronto.ca/about.htm>)

In addition, the University uses a notice of collection:

The University of Toronto respects your privacy.

Personal information that you provide to the University is collected pursuant to section 2(14) of the University of Toronto Act, 1971.

It is collected for the purpose of administering admissions, registration, academic programs, university-related student activities, activities of student societies, safety, financial assistance and awards, graduation and university advancement, and reporting to government agencies for statistical purposes.

At all times it will be protected in accordance with the Freedom of Information and Protection of Privacy Act. If you have questions, please refer to [www.utoronto.ca/privacy](http://www.utoronto.ca/privacy%22%20%5Ct%20%22_blank) or contact the University Freedom of Information and Protection of Privacy Coordinator at McMurrich Building, room 104, 12 Queen's Park Crescent West, Toronto, ON, M5S 1A8.

##### 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. How?

#### Microsoft

The University has ensured that the contract with Microsoft explicitly restricts the collection, use and disclosure of all personal information. The relevant section of the contract reads:

 “Microsoft shall not collect, use or disclose any Personal Information of End Users, or any derivatives of such Personal Information, except to provide the E-Mail Service to End Users and perform its obligations under this Agreement or except as otherwise permitted under this Agreement.”

Microsoft encourages data minimization wherever possible, which reduces the risk to personal information. In its “Privacy Guidelines for Developers” document, developers are instructed to consider all possible uses of data, including secondary uses such as marketing analyses and recommends that data only be collected as necessary for immediate planned uses. It also suggests that wherever possible, data be aggregated and removed entirely if no longer needed.

The SAS 70 report provided to the University demonstrates secure destruction of data which has reached the end of its lifecycle.

#### University of Toronto

The University is committed to the principle of data minimization as noted. The University’s Data Protection Guidelines state: “Access to confidential information must be on a need-to-know basis only; need-to-know requirements must be documented as a requirement of job duties or contractual obligations.”

University privacy practices also require that no more personal information be collected than is needed for official University purposes.

##### Does the project meet or exceed the requirements of FIPPA? Yes. How?

The personal information placed in the O365 system by staff and faculty is regulated under the FIPPA legislation. Consistent with its regulation under FIPPA, the University analyzed how well Office 365 meets FIPPA privacy requirements and explored mitigation strategies to best reduce privacy risk. The details are in Appendix J. It is divided into six sections: collection, use, disclosure, retention, disposal of data and security. Many mitigations are contractual and excerpts of the agreement with Microsoft have been included in the analysis. Although the agreement does not state that Microsoft will comply with FIPPA, the University is satisfied that Microsoft’s contractual commitments support privacy protection consistent with FIPPA standards.

##### What gaps remain?

One new technology being introduced with O365 is the SharePoint collaboration software. This allows users of the system to share documents and create public or private team sites to further collaborative efforts. While the privacy controls are well laid out and are not shared by default in most cases[[21]](#footnote-21), care should be taken to ensure that staff and faculty do not inadvertently make documents public that should otherwise be private. Since the ability to do so, exists with existing technologies, this is not a material new risk.

## **3. Privacy Embedded Into design**

*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.4

### Is Privacy Embedded into the Design?

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

#### Microsoft

Microsoft has documented guidelines for its developers to follow when developing software products and services.[[22]](#footnote-22) These guidelines address core privacy or security principles.

The document includes such privacy-protecting practices as:

###### Data Minimization

* “One of the best ways to protect a customer’s privacy is to not collect his or her User Data in the first place.”
* “Employee access to User Data should be limited to those who have a legitimate business purpose for accessing the data.”
* “The risk of data exposure can be further minimized by reducing the sensitivity of stored data wherever possible.”
* “The longer data is retained, the higher the likelihood of accidental disclosure, data theft, and/or data growing stale. User Data should be retained for the minimum amount of time necessary to support the business purpose or to meet legal requirements.”

###### Notice, Choice, and Consent

“All products and services that collect User Data and transfer it must provide an explanation (“give notice”) to the customer. The customer must be presented with a choice of whether to provide the information, and consent must be obtained from the customer before PII can be transferred from the customer’s system.”

###### Security

“Security is an essential element of privacy. Reasonable steps should be taken to protect PII from loss, misuse, unauthorized access, disclosure, alteration, and destruction.”

###### Access

“Customers must be able to access and update PII that is stored remotely. When customer contact preferences are collected, customers must be able to view and update their preferences.”

###### Data Integrity

“Reasonable steps must be taken to ensure that PII is accurate, complete, and relevant for its intended use.”

#### University of Toronto

The University of Toronto embedded privacy design into the infrastructure that will be interfacing with the Office 365 system.

Encryption of mail flowing between the University’s mail routers and Microsoft’s is provided by a service called Forefront Online Protection for Exchange (FOPE). The functioning of this service is reinforced through firewall rules, managed by the University of Toronto, that block traffic on unencrypted ports, and through the configuration of the U of T Message Router to only accept encrypted traffic, regardless of network port.

The University will provide authentication services for Office365, to retain control of user names and passwords, and for the most part, to avoid passwords flowing through Microsoft’s servers. This is described in more detail in principle 5, Data Flows section.

##### 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. How?

### Stakeholder Expectations*[[23]](#footnote-23)*

The University is currently holding meetings with a representative sample of staff and faculty stakeholders.

It is clear that the variety of information staff and faculty will store on the service is much more diverse than that stored by students (see section 5, “Information at Risk” for more detail). In addition to this, there are a number of types of activities that staff and faculty carry out over email. These include, but are not limited to, administrative functions, teaching, research and personal activities. The addition of document sharing (Skydrive) and website creation (Sharepoint) will certainly increase the volume of data being shared through the system. These and other issues will be addressed in the consultations.

#### Stakeholder Committee

Members of the committee include:

|  |  |
| --- | --- |
| Faculty |  |
| Mike Luke | Committee Chair |
|  | Chair, Department of Physics |
| Lisa Austin | Associate Professor, Centre for Innovation and Policy, Faculty of Law |
| Don Boyes | Senior Lecturer, Geography |
| Corey Goldman | Senior Lecturer, Department of Ecology & Evolutionary Biology. |
|  | Assoc. Chair (Undergraduate Studies) |
| Hugh Gunz | Professor of Organizational Behaviour |
|  | Associate Chair, Department of Management, UTM |
| Kelly Lyons | Associate Professor, Faculty of Information |
| Cynthia Messenger | Senior Lecturer and Director Writing and Rhetoric Program, Innis College |
| **Staff** |  |
| Robert Cook | CIO |
| Erin Jackson | Director, Central Admin. Human Resources |
| Helen Lasthiotakis | Assistant Dean & Director, Office of the Dean, FAS |
| Zoran Piljevc | Director – IITS, UTSC |
| Wes Robertson | Director, Discovery Commons Faculty of Medicine |
| Rosanne Lopers-Sweetman | CAO, Faculty of Kinesiology and Physical Education |
| **Assessors** |  |
| Jeremy Graham | Operations Manager, Academic and Collaborative Technologies |
| Martin Loeffler | Director, Information Security and Enterprise Architecture |
| Marden Paul | Director, PGA&C and Project Director |

#### Stakeholder Feedback

The following privacy / security issues were discussed and responded to by the Stakeholder Committee:

1. Microsoft offers a chargeable service that allows the tracking of email receipt. Have you had reason to track email receipt in the past / do you anticipate you’ll want to do so again in future? Is it worth the expense to the University to subscribe to this functionality?
	* The committee responded that tracking email has been required in the past, for example: when investigating unauthorized access to email accounts, in identifying who may have read a mis-sent email that contained Personally Identifiable Information, and in troubleshooting email that was not received. This type of service has been needed on the order of monthly; the committee felt that it was a worthwhile service to subscribe to, despite the fact that there was a cost associated with it.
2. Do you have any concerns with respect to cheating and plagiarism that uniquely arise from document sharing and collaboration features of Office365?
	* The committee responded that there were no concerns with regards to cheating and plagiarism that might uniquely arise from the document sharing and collaboration features of Office365.
3. Should we be investigating technical capacity to limit sharing of sensitive information with correspondents external to University?
	* The committee felt that Office365 afforded sufficient granularity of access management to mitigate the risk of unauthorized access to sensitive or research material, and that there were no additional controls required. Further, to apply technological controls to implement rule-based limitations on disclosure of information (e.g. Data Loss Prevention (DLP) tools) would be infeasible given the difficulty in creating rules to match the broad range of formats that can represent sensitive data.
4. What specific concerns should we be addressing / practices we should be encouraging with respect to medical data, research data, grade data?
	* If possible, the committee felt that it would be valuable to have access to required practices for the management of sensitive information as part of the Office365 interface – such as mouse-over information boxes or tabs that would reveal guidance when clicked on.
	* The possibility of implementing wholesale encryption of all data within Office365 was discussed, but was unworkable owing to a lack of vendors offering such a service and the fact that encryption unmanaged directly by the University did not reduce risk – it merely transferred it to the encryption service firm.
5. Are there other privacy risks that we have not yet identified, unique to faculty and staff?
	* The committee recommended that practical documentation and education materials should be developed and distributed to end-users so that end-users may understand new risks they may be exposed to, and as any changes or additions to privacy and security-related practices they’re expected to follow in the new environment of Office365.

###  SAS70 Type II Attestation

The SAS70 Type II report referenced in the Resources Consulted section contains highly detailed information provided about Microsoft’s internal systems. Since this was an essential verification for Microsoft security assurances, the following specifics are set out in detail.

SAS70 defines the standards that an auditor must follow when carrying out an audit of the internal controls in a service organization. That is, SAS70 is an audit standard, not a security or privacy standard. There are a few things to keep in mind about this report:

1. A SAS70 Type II Attestation is a measure of a company’s adherence to their defined controls; whether they are doing what they say they are. Since SAS70 does not define the security controls, it is not necessarily a good indication of the security of an organization. It is therefore important to understand what standard of security they have committed themselves to. In Microsoft’s case, they asked to be evaluated by the “ISO 27001: Specification for an Information Security Management System” standard.
2. It is important that the standard being audited be broad enough in scope to cover all of the infrastructure and software that the University’s personal information will be stored on. “ISO 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system **-** an overall management and control framework - for managing an organization’s information security risks.  It does *not* mandate specific information security controls but stops at the level of the management system.”[[24]](#footnote-24) The SAS70 Type II audit provided by Microsoft covers their management system, not specific controls that have been put in place. Understanding Microsoft’s overall management strategy for managing risk is as important as having a good grasp of the specific security controls in place.
3. A SAS70 Type II attestation is not a tool to monitor the ongoing state of security at an organization, but a review of past events, and the effectiveness of the controls in place to prevent security incidents. A Type II attestation will cover a specified length of time.

On the basis of the usefulness of the SAS70 Type II attestation, the following wording is included in the draft agreement with Microsoft:

 “Microsoft shall cause its external auditors to provide to Institution a SAS 70 Type II report (or equivalent) annually throughout the term of the Agreement on the design, existence, effective operation and continuity of Microsoft’s control procedures in respect of the data centers used to provide the E-Mail Service. Where the SAS 70 Type II report identifies material deficiencies in the data centers used in the performance of the E-Mail Service, Microsoft shall provide to Institution a remedial plan to address such deficiencies and shall report to Institution on the progress made in executing such plan.”

##### 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. How?

The University conducted a detailed Privacy by Design Privacy Impact Assessment process to thoroughly address risk assessment and document privacy risks and measures taken to mitigate those risks. Data flows were documented and analyzed for privacy impact and risk assessment, both in-house and at Microsoft (detailed analysis of these data flows is found under principle 5 below). The University published an early version of the PIA and intends to publish an implementation version on the University website. The PIA will continue to develop and guide the Office365 project through its lifetime.

##### What gaps remain?

Some residual risks have been identified in Appendix B: [Analysis of Residual Risks](#_Appendix_A:_).

## **4. Full Functionality – Positive-Sum, not Zero-Sum**

*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy *vs*. security, demonstrating that it *is* possible to have both.4

### Is there Full Functionality in a Positive Sum manner?

##### Are all system requirements optimized to include full functionality, privacy and security?

Yes. How?

The relationship between Microsoft and the University is a positive sum exercise in which each party seeks an optimal mix of ingredients. For the University, these include full functionality, privacy and security, features, low cost and flexibility. Through its agreement with a cloud vendor, the University seeks to provide a world-class email service for staff and faculty.

Microsoft has integrated both security and privacy into its Security Development Lifecycle (SDL)[[25]](#footnote-25) [[26]](#footnote-26), the Microsoft methodology for developing all software and services. This appears to be a highly effective approach for developing software that respects privacy in a positive-sum way.

##### Are all legitimate non-privacy objectives embraced and accommodated in an innovative, positive-sum manner? Yes. How?

Office 365 provides a level of service that it would be prohibitively expensive for the University to duplicate. Some of the benefits of Office365 include:

* Increasing mailbox storage to 25 GB, an increase of some 200 times
* Increased availability, redundancy of services
* Modern, usable web-based interface
* Leveraging the multi-billions of dollars of investment by Microsoft in their infrastructure, and their full time security staff
* Updates applied to infrastructure at no cost to the University
* Optional availability of online document storage

These features are key benefits to users and to the University, which in a positive sum context will be delivered together with strong privacy protections and sound security.

##### Is creativity and innovation used to achieve all objectives including privacy? Yes. How?

The University is undertaking to implement a new Active Directory service that will provide secure authentication for Office365 users via ADFS (‘Active Directory Federated Services’). ADFS will allow users of Office365 at the University to authenticate to University-managed access control and identity management services; this will allow the University to protect the privacy of usernames and passwords by processing them at the University without providing them to external service providers. This is discussed in more detail in the Data Flows section referenced in principle 5 below.

### Cloud Computing

Considerable effort was made to analyze the cloud computing model used by Microsoft to provide the *Office365* service. As the Internet has evolved, companies have increasingly leveraged economies of scale by centralizing computation resources in data centers and relying on the Internet to transfer information to and from these data centers and clients.

Traditional computing models focus on establishing a secure perimeter around a set of “trusted” machines that comprise the (University) network, with appropriate attention to endpoints of communication as information leaves the trusted environment.

In a Cloud computing context, the secure perimeter must be expanded around resources under control of the external provider (and beyond direct control of the University). This represents a significant risk to the University and care must be taken to ensure that this extension of trust is both reasonable and prudent. The general types of cloud computing services and modalities are described in Appendix J [Cloud Computing Models](#_Cloud_Computing_Models).

*Office365* is offered as a Software as a Service model and is run in a public, off-premises cloud wholly owned and operated by Microsoft. A key implication of this is that the University is effectively outsourcing the security of its email platform to Microsoft, from the network infrastructure all the way up to the application. It is essential that the University assess the reliability and trustworthiness of Microsoft’s reputation as well as the robustness and security of its hardware and software infrastructure. Care must be taken to ensure that the privacy of information is not an afterthought, but rather that privacy has been of central concern to the external provider at every stage of the development of its services and infrastructure. Microsoft's SAS70 Type II audited compliance with the ISO 27001 standard for an information security management system has been integral in establishing trust.

Microsoft offers transport layer encryption (protecting the data as it flows between the end-user and Microsoft) and strict, audited security controls.

### Data Residency

Given the nature of cloud-based services, there is a degree of uncertainty as to the exact location of the University’s data at any given time. Microsoft stated that the University’s data will reside within two datacenters, and in three locations within each datacenter. Under a non-disclosure agreement, Microsoft revealed to the University the approximate locations of its currently operating datacenters and their expected use for U of T Office 365 service.

##### What gaps remain?

### Foreign Legislation

In cloud environments, it is increasingly common for service providers to use globally distributed resources, which, by virtue of such distribution, are beyond geographic reach, and may be subject to the laws of foreign jurisdictions. The Ontario government publication, “*Guidelines for the Protection of Information when Contracting for Services*” attributes high risk to storage of sensitive information outside Canada. This risk must be addressed in every project or activity. This type of risk is usually addressed through contractual security and privacy assurances by the service provider to protect data in all contexts, at all times and in all locations. These assurances are provided by Microsoft in its agreement with the University.

Microsoft is a U.S. based corporation subject to U.S. legislation, including the USA PATRIOT Act. Information about the USA PATRIOT Act is set out in Appendix C.

Under its agreement with Microsoft, U of T will be given prior notice of disclosures by Microsoft when legally possible. This is the soundest assurance that can be provided by Microsoft. Users will be notified that their information will reside outside Canada before signing up for Office365.

## **5. End-to-End Security - Full Lifecycle Protection**

*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.4

### Does the Project Apply End-to-End Security, achieving Full Lifecycle Protection?

##### Are there strong security measures in place throughout the lifecycle of the data so that the data is retained securely? Yes. How?

### Data Flows Analysis

A fundamental PIA component is a description and analysis of information flows. This section comprises a high level overview of information at risk and key actors, and an analysis of personal information transactions within the system. Due to the closed nature of the *Office 365* system, these transactions can only be examined at a relatively high level of granularity.

An overview of Office 365 service data flows and processes, including, major parties, migration processes, email flow, protection, encryption, web/non-web access, backups and termination of service, is set out in Appendix E.

#### Summary

Transport encryption, which is used throughout the Office 365 system, protects information in transit, as it flows over the Internet from U of T to the Microsoft data centers and back.

#### Information at Risk

This PIA uses the FIPPA definition of personal information (see Appendix D). Email is used to communicate personal and confidential information and other Office365 services may be usable to store or communicate personal information. This information is protected under FIPPA legislation. The following chart highlights some of the types of confidential information that will potentially be stored on Office365. In each cell there is an assessment of the perceived impact to the University (sensitivity) of the information being disclosed, altered, deleted or accessed without record of use.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Confidentiality | Integrity | Availability | Accountability |
| Education Records | High | Low | Low | Med |
| Financial Data | High | Low | Low | Med |
| Investigations / Disciplinary Actions | High | Med | High | High |
| Personal Correspondence of Staff/Faculty | Med | Low | Low | Low |
| Research Data | High | High | Med | High |
| Medical Information | High | Low | Med | High |
| Authentication Tokens (Passwords) | High | Low | Low | High |

A full discussion of the potential for risk to these assets being realized is contained in the section ‘*Threat / Risk Assessment Analysis’.*

##### Are the security measures consistent with standards developed by recognized bodies? Yes. How?

Microsoft maintains a SAS70 Type II Audit certifying compliance with the ISO 27001 standard for Information Security Management Systems.[[27]](#footnote-27) [[28]](#footnote-28)

Microsoft achieved Federal Information Security Management Act (FISMA) certification & accreditation for its data centres in May 2012.[[29]](#footnote-29) This certifies that the security of Microsoft’s cloud computing infrastructure is sufficient for obtaining U.S. government contracts.[[30]](#footnote-30) [[31]](#footnote-31)

Industry standard transport layer encryption (SSL/TLS) has been required during transmission of all data across all life-cycle stages of this project.

##### 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. How?

The SAS70 report provided to the University by Microsoft indicates a comprehensive approach to infrastructure security. The company conducts risk assessments, implements security controls and regularly monitors the success of those controls to protect its resources. The document shows how in each of the three cornerstones of PbD (information technology, accountable business practices and physical design & infrastructure) Microsoft maintains a high level of security. The ISO 27001 and FISMA certifications indicate a security standard greater than that currently maintained by the University of Toronto.

In addition to the security standard outlined above, the agreement with Microsoft includes a number of contract points that ensure:

* Information confidentiality to the extent consistent with law and best efforts to give notice of disclosures;
* Information integrity consistent with reasonable standards;
* Return or destruction of confidential information and;
* Access controls, including security and confidentiality and on request return or destruction of confidential information.

##### What gaps remain?

There are no material residual gaps. This project considered the full life-cycle of the personal information that is to be protected and achieves a level of security that is appropriate to the sensitivity of the information that is going to be collected / used / disclosed.

## **6. Visibility and Transparency – Keep it Open**

*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.4

### Does the project operate with visibility, transparency and openness?

##### Is responsibility for privacy-related policies and procedures documented, communicated and assigned to a specific individual? Yes. How?

##### Privacy is a shared responsibility at the University. The FIPP Office takes the lead in providing training and advice to University units that interact with personal information.

##### Both Microsoft and the University will be provided with critical communication contacts and a process to address privacy questions and concerns.

##### 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. How?

A detailed analysis of the agreement was performed, comparing it against the FIPPA legislation. It was found that the agreement gives the University the assurance that Microsoft is operating within the bounds of FIPPA. In addition, the agreement states that, except for alumni, the University may opt to turn off advertising in all of the Office365 services (except Messenger, for which this is not possible)

“…Microsoft agrees not to display on the web interface to the E-Mail Service or any Thick Client interface to the E-Mail Service, any Advertisements that promote Microsoft or third party products or services, except that Microsoft may display such Advertisements on the web interface of the E-Mail Service available to Alumni.” (2.c.ii)

##### Is information about the policies and procedures relating to the management of personal information readily available to individuals? Yes. How?

The FIPP website provides information on the legislation and policies governing the management of personal information at the University,[[32]](#footnote-32) and the website of the Provost details University privacy and personal information practices.[[33]](#footnote-33)

Microsoft has detailed documentation about its security and privacy practices on its website. [[34]](#footnote-34) The SAS70 Type II report and FISMA certifications were shared with the University.

##### Have complaint and redress mechanisms been established and communicated to individuals? Yes. How?

There are two redress mechanisms in place at the University of Toronto:

1. The University’s FIPP Office addresses questions or concerns about personal information and looks into privacy concerns.
2. For technical support questions, the University has an established Help Desk available on the web and on the telephone. Help Desk personnel will receive specific training with respect to the Office365 service and the technical issues that may arise.

A privacy principle at Microsoft is the “monitoring and enforcement of compliance with their privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints and disputes.”[[35]](#footnote-35)

##### Have steps been taken to monitor, evaluate and verify compliance with privacy policies and procedures? Yes. How?

### Verification of Privacy Policies and Commitments

It is critical that the University can verify the commitments Microsoft has made about the privacy and security of their systems and procedures. The SAS 70 audit that the University obtained contains a third-party analysis of the claims that Microsoft makes. While this audit is an excellent first step, the University will go further to confirm that Microsoft’s service and actions are privacy protective and appropriately secure. Much of this verification will necessarily leverage relationships between the University and Microsoft.

These relationships have been developed across key areas including decision makers, legal practitioners, privacy officials, and technical staff dealing with the functional and security aspects of the project. Negotiations and understandings of University and Microsoft decision makers are reflected in the agreement between the two organizations. The agreement delineates the operational relationship, which enables the University to abandon the service if it does not continue to meet its needs on a positive-sum basis, including function, security and privacy.

While the contract does not explicitly detail all security and privacy actions, University technical staff are working with leading Microsoft technical experts to develop and define system parameters to meet University functional, security and privacy requirements, guided by Privacy by Design. As the system is rolled out and later through its operational life, Microsoft and University staff will continue to work together to ensure functionality, security and privacy.

Through this ongoing relationship, the University will continue to confirm that Microsoft continues to meet privacy and security expectations. It is expected that operational staff at both organizations will communicate clearly and completely to create an environment of mutually verifiable assurances in system design, configuration, implementation and operation. This speaks to accountable business practices, with the University and Microsoft relationship fostering a culture in which the right privacy actions are demonstrably taken and supported.

During the development of this PIA, Microsoft has responded to University privacy concerns, providing requested documentation. The University was assigned a Microsoft client representative, Karen McGregor, who provided useful access to other Microsoft resources. Microsoft consultants, Richard Wakeman and Dimtry Kazantsev, have assisted the U of T implementation team. In addition, U of T worked with David Fischer of Microsoft who is Senior Product Manager of Office365 Research and Development.

As the project progressed, the University realized that encryption of mail between the University’s mail routers and Microsoft’s is provided by a service called Forefront Online Protection for Exchange (FOPE). This service is not enabled by default, and the University requested that it be turned on for its test users. FOPE has now been tested by the University and is active.

During the initial phases of the operational relationship between Microsoft and the University of Toronto, support was provided by submitting a “ticket” to the online Microsoft support system. The time to resolve the issue could be upwards of a couple of weeks and in these cases the customer would not have access to their email account. To mitigate this issue Microsoft responded by giving our technical staff direct access (for a certain class of problems) to Dave Fisher, who is able to resolve the issues in a shorter time frame.

One area of ongoing concern is the application of updates to the cloud software by Microsoft. The University of Toronto has little or no control over the scheduling of these updates, and has no choice to opt-out of them if it wishes. In some cases, this can have negative impacts on the customer, as it did in January 2012, when Microsoft applied an update to their software that broke connectivity to Live@edu for many Android mobile devices.

With the move of staff and faculty to O365, the University should be aware that such disruptions of service could potentially have a greater impact on the University’s business if administrative staff had a long-running support request, or an update caused the loss of functionality to a subset of the population.

##### What gaps remain?

Although the contract supports privacy protection, and the Microsoft website features privacy design, the contract does not specifically state that Microsoft will support Privacy by Design principles. This is not expected to be an issue in the context of the expected mutually supportive relationship between the University and Microsoft, in which excellent and visible protection of privacy is essential to the University’s commitment to its communities and to Microsoft’s ongoing credibility as a world-class cloud service provider.

## **7. Respect for User Privacy – Keep it User-centric**

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.4

### Is there a user-centric respect for User Privacy?

##### Are data subjects empowered to play an active role in the management of their own data? Yes. How?

Microsoft makes a commitment to empowering users in their *Privacy Guidelines for Developing Software Products and Services*

Email is a core service for many of the daily activities that staff and faculty undertake. Email (along with the document sharing applications like Sharepoint) is fundamentally user-driven. Each user decides what information will be placed into the system.

##### 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. How?

The University should present a notice to staff and faculty as they register for this service that outlines how the service works, and what types of activities should and should not take place on the service.

## Summary

Microsoft appears to have a strong commitment to the privacy of the users of its products. Microsoft communicates an understanding that privacy must be built into a system at the very beginning; it provides extensive guidelines to its developers to enable them to incorporate privacy into their design. External audit documentation attests that Microsoft’s commitment to privacy extends through all levels of the organization, and shows that a comprehensive approach to protecting customer personal information has been implemented.

# Analysis of Residual Risks

### Residual Risk Solutions

Microsoft has several features to effectively manage privacy risk such as transport layer encryption (protecting data flows between the user and Microsoft) and strictly audited security and privacy controls. The University has worked with Microsoft to build reasonable privacy protections into the contract. The Universities experience with working with Microsoft using the Live@Edu system has been positive and provides reassurance that Microsoft is committed to and capable of protecting privacy.

### Summary of Residual Risks

| The following table provides a short summary of the risks and an accept/reject box for each. The source column indicates the relevant legislation or analysis from this PIA related to the particular risk.**Risk** | **Description** | **Mitigation** | **Areas of Concern** |
| --- | --- | --- | --- |
| Proxy Server CompromiseProbability - LowImpact – High | Microsoft authentication proxy server is compromised, revealing UTORids and passwords. |  | FIPPA*PbD* |
| Unknown Software VulnerabilitiesProbability: LowImpact: High | All complex software systems contain unknown vulnerabilities, some of which may be exploited to gain unauthorized access to data stored in the system. | Same as current state. No new risk. | *PbD* |
| Microsoft Employee Acting Without AuthorizationProbability - LowImpact – High | An employee at Microsoft decides to use his/her administrative access without authorization to access *Office365* user information, potentially for illegal purposes. | UofT staff could do this today. No new risk. | FIPPA |
| Accidental disclosure by a Microsoft employeeProbability - LowImpact - Medium | A Microsoft employee accidentally discloses a user’s personal information | UofT staff could do this today. No new risk. | FIPPA*PbD* |
| Foreign Legislative ThreatProbability - LowImpact - Medium | A request for information is made to Microsoft under USA PATRIOT Act or similar legislation |  | FIPPA |
| Attacks from within the cloudProbability - LowImpact – High | Due to the shared nature of cloud computing, vulnerabilities of *Office365* might be exploited by other customers of Microsoft’s cloud computing architecture |  | FIPPA*PbD* |
| Mishandling of data by UofTProbability - LowImpact – Low | A University of Toronto employee accidentally discloses a user’s personal information | UofT staff could do this today. No new risk. | FIPPA |
| Updates to O365 break functionalityProbability - MediumImpact - Privacy: Low Operational: High | Microsoft applies a software update to the O365 service that causes some users to lose a function that they rely upon to conduct business. | This could occur when current software is patched. MS have a robust testing process. No new risk. |  |
| Disclosure of Sensitive DataProbability - MediumImpact – High | The volume of sensitive information will increase with staff / faculty on the outsourced system. The residual risk increases accordingly. |  | FIPPA |
| Improper termination of agreementProbability - LowImpact - Privacy: Low Operational: High | Potential for the relationship between U of T and Microsoft to sour, ending the contract prematurely. | Contract has appropriate language to govern the termination of the relationship. MicroSoft is a mature vendor so risk is not material. |  |

 This appendix sets out the residual risks. The University performed detailed analysis of the data flows in order to identify all potential risks. Systems that interact with user information and staff who have administrative system control were considered. Network communications were also considered, but were excluded from detailed analysis here because properly implemented encryption reduces their risk to negligible levels. While careful analysis was performed, it is possible that unknown risks remain.

Several components of the U of T infrastructure will be leveraged to integrate *Office365* into the U of T email ecosystem. Possible risks affecting these infrastructure components were identified. Briefly, these previously existing risks include:

* Hacker attack of U of T infrastructure including email routing and identity management systems
* Errors of U of T staff responsible for managing or supporting email that lead to personal information exposure
* Inadvertent or malicious access or use of personal information by U of T systems staff.
* User password compromise through use of infected computers.

## Proxy Server Compromise

**Description of risk:**

Microsoft implemented a proxy server that allows non-Shibboleth enabled clients to use Shibboleth authentication. This allows them to integrate with the University’s identity management system for authentication and authorization. The user credentials will be sent to the proxy server, which will then communicate with the University’s identity system to authenticate the user. The authentication proxy will be used by email clients (such as Outlook or Thunderbird) and mobile devices to authenticate users to the *Office365* service. If an attacker (or unauthorized malicious Microsoft employee) was able to compromise (or ‘hack’) the proxy server, they might be able to collect user credentials as they flow through the server.

**Impact:**

UTORid credential theft, which could lead to user accounts being used for spam or fraud. There is also the risk of the theft of personal information.

**Existing Mitigations:**

* Microsoft already uses encrypted communications to and from the proxy server.
* Microsoft assures us that the credentials are not permanently stored on the proxy server. However, the passwords are briefly stored in the memory of the proxy server during the authentication process.
* The server is located in Microsoft’s physically secure data center (which can prevent physical tampering).
* Microsoft monitors all of their servers for signs of compromise or suspicious activity.

**Potential Mitigations:**

The University can optionally disable this method of authentication for its users, which would force users to use the web interface.

**Residual Risk:**

University of Toronto staff / faculty UTORids and passwords could potentially be harvested from a compromised Microsoft authentication proxy server.

Probability: Low, Impact: High.

## Unknown Software Vulnerabilities

**Description of risk:**

All complex software systems contain unknown vulnerabilities, some of which may be exploited to gain unauthorized access to data stored in the system.

**Impact:**

The personal information of one of more U of T staff or faculty members could be accessed by the attacker, with possible outcomes such as identity theft, harm to reputation or personal distress.

**Existing Mitigations:**

Microsoft integrated security and privacy into their Security Development Lifecycle which results in few software defects. Microsoft has also implemented comprehensive security training for their employees. Systems in their data centres are monitored continuously for evidence of security breaches.

**Residual Risk:**

While there are risks pertaining specifically to *Office365*, these are somewhat offset by the decommissioning of the UTORmail infrastructure that was serving students, staff and faculty. Microsoft’s concern for their reputation in the industry gives them sufficient motivation to ensure the security of their service.

Probability: Low, Impact: High

## Microsoft Employee Acting Without Authorization

**Description of risk:**

Given the nature of outsourcing the University’s email infrastructure, the University is trusting that Microsoft and its employees will be responsible with its data. If one of those employees were to maliciously violate corporate policy, they could abuse the personal information stored within their infrastructure. This occurred with Google’s Gmail in July 2010[[36]](#footnote-36).

**Impact:**

The personal information of one of more U of T staff or faculty could be misused by Microsoft staff acting without authorization, with possible outcomes such as identity theft, harm to reputation or personal distress.

**Existing Mitigations:**

Microsoft maintains excellent access control policies and mechanisms as evidenced by the material in their SAS 70 report.

**Residual Risk:**

 Only some of the University’s data would be vulnerable until the unauthorized access were discovered by internal audit, or otherwise detected. Depending on the effectiveness of Microsoft’s internal audit, such an exposure could last from days to months.

Probability: Low, Impact: Medium.

## Accidental disclosure by a Microsoft employee

**Description of risk:**

It is possible that a Microsoft employee could mishandle data or applications, leading to exposure of personal information. This happened in December of 2010, when a “configuration issue” in one of Microsoft’s services allowed address book information to be downloaded by unauthorized users.[[37]](#footnote-37)

**Impact:**

The personal information of one or more individuals may be inadvertently disclosed to unauthorized persons.

**Existing Mitigations:**

In their SAS70 report, Microsoft indicates that they provide security and privacy training to their employees.

**Residual Risk:**

Because of employee training, and limited access to information, the residual risk is low. If there was a window of exposure it would last until detected by internal audit, or until reported.

Probability: Low, Impact: Medium

## Foreign Legislative Threat

**Description of risk:**

Microsoft is clear about their requirement as a U.S. corporation to release information requested under the USA PATRIOT Act regardless of where that information is stored (even if it were housed on servers physically located in Canada). Microsoft is also prohibited from informing us about some types of USA PATRIOT Act requests.

**Impact:**

US authorities can request records of individual users, including emails, access logs and other personal information. In some cases the University will have no way of knowing if and when this is happening.

**Potential Mitigations:**

There are no mitigations for this, other than encryption. Products such as ‘PGP Desktop Email’, or the open source GnuPG are capable of encrypting the content of the email (but not the message headers, including sender, recipient and subject)[[38]](#footnote-38). These solutions are available to individuals, but would be either costly (PGP) or difficult to support (GnuPG) institution wide.

**Residual Risk:**

 Because Microsoft is prohibited from informing us that data was released under the USA PATRIOT Act, the University has no way of reliably determining the probability of such occurrences.

Probability: Low, Impact: Medium

## Attacks from within the cloud

**Description of risk:**

Within the same Microsoft data centers as *Office365* are other Microsoft services, including Azure. There is a potential for attacks within the data center (or cloud) to leverage shared resources in order to attack the University’s *Office365* service. The University could potentially experience a Denial of Service (DoS) attack, or a data breach leveraging shared hardware within the Microsoft data center.

**Impact:**

During a DoS attack, *Office365* services may be unavailable. A data breach leveraging shared hardware would likely result in a large amount of disclosed personal information.

**Existing Mitigations:**

* Microsoft monitors the networks and services within their data centers closely[[39]](#footnote-39):
“If any anomalies are detected, they will be investigated and resolved. Operational controls are incorporated to facilitate automated monitoring and early notification if a breach or problem occurs…”
* Microsoft invested significant effort into designing a secure data center infrastructure. They also routinely test their infrastructure to make sure it’s resistant against hackers[[40]](#footnote-40):
“Penetration testing performed by internal and external parties provides important insight into the effectiveness of security controls for the Microsoft cloud infrastructure. The outcome of these reviews and ongoing evaluation of the resulting controls are used in subsequent scanning, monitoring, and risk remediation efforts.”

**Residual Risk:**

 Attacks from within the cloud may be able to leverage shared infrastructure, but the entire infrastructure in managed by Microsoft. They monitor the infrastructure, and have the ability to quickly terminate any malicious processes.

Probability: Low, Impact: High

## Mishandling of data by University of Toronto

**Description of risk:**

During the migration to *Office365*, or during the ongoing management of the service, it’s possible that the University of Toronto could inadvertently mishandle user data. User credentials or personal information could be inadvertently disclosed, through unencrypted communications, or other means.

**Impact:**

In the event of inadvertent disclosure, the number of potentially affected users would likely be large, but the probability of the data being intercepted is low.

**Existing Mitigations:**

* The University will not send user credentials to Microsoft. The authentication will use Shibboleth, hosted and managed by the University, to integrate with the University’s existing identity management system.

**Potential Mitigations:**

* The University must ensure that all communication channels between the U of T and Microsoft are encrypted. Based on discussions with Microsoft, this should be possible, but some additional assurance that they will work with the University to enforce encryption is desirable.
* The University should define a set of best practices that define internal handling of confidential data.
* The University should audit its staff’s privileged access to *Office365* in order to detect any potential abuse.
* The University should have a plan for users to opt-out prior to migration.
* The University should have a plan for users to migrate to a different email service provider.

**Residual Risk:**

If the University implements the above mitigations, the residual risk should be minimal.
Probability: Low, Impact: Low

## Updates to O365 Break Functionality

**Description:**

With a cloud-based service such as O365, the vendor is in charge of software updates, and can apply them to their systems without consulting their user base. In some circumstances this can cause service outages.

**Impact:**

It is possible that access to email / calendaring / documents could be interrupted by a mis-applied software update.

**Potential Mitigations:**

* Since Microsoft controls the software, there is no mitigation for this risk.

**Residual Risk:**

Probability: Medium, Privacy Impact: Low, Operational Impact: High

## Disclosure of Sensitive Data

**Description:**

With the move of staff and faculty to the cloud-based O365, the University can expect that the amount of confidential information residing in the system will increase drastically.

**Impact:**

There will be much more sensitive information stored in the cloud, with the resulting increase in the impact to the University if this data is exposed.

**Potential Mitigations:**

* The potential mitigations for this have been discussed in detail in other sections of this document.

**Residual Risk:**

Probability: Medium, Impact: High

## Improper Termination of Agreement

**Description:**

The University must consider that the agreement with *Office365* will eventually come to an end. Derek Yuen indicated that it would take the University of Toronto at least six months to migrate data out of *Office365* with the current amount of data When it is eventually time to migrate out of *Office365*, the University must ensure that there is sufficient time to exit in a secure and appropriate manner.

**Impact:**

 The University could potentially lose all or part of stored messages within *Office365*.

**Potential Mitigations:**

* The University should ensure that its contractual agreement includes a clause that would provide U of T with suitable time to migrate its data out of *Office365*.
* When the time comes to end the agreement, the University should try to end it on good terms.

**Residual Risk:**

Microsoft is a professional organization with their reputation in the industry at stake. This is very unlikely to be a problem. There is little risk to privacy, as in the event of an abrupt termination of the agreement, Microsoft is more likely to delete data than disclose data.

Probability: Low, Privacy Impact: Low, Operational Impact: High

# FIPPA Risk Analysis

The following privacy risks apply to all six sections of the FIPPA analysis. These are:

1. Collection, use or disclosure of personal information inconsistent with FIPPA.
2. Individual dissatisfaction with University or Microsoft privacy actions.
3. Privacy complaints to the University, Microsoft or the IPC from individuals dissatisfied with the collection, use or disclosure of their personal information.
4. Harm to the University’s reputation.

Risks specific to each section are set out in that section.

## Collection

There is a risk that Microsoft or its affiliates could *collect* or *store* user personal information in a manner not authorized by the University. To help alleviate these concerns, Microsoft practices data minimization. [[41]](#footnote-41) Microsoft provides security and privacy training to its staff. Despite these assurances, proper notification need be provided to Office365 users informing them of the personal information that will be disclosed to Microsoft. In addition, since the Office365 service’s privacy policy is expected to change over time, University staff will continue to monitor it to ensure that changes continue to comply with Ontario privacy legislation, and that such changes are communicated to users.

The contract includes statements for protection of personal information in the collection stage:

* Except with respect to data provided to Microsoft for the purpose of providing the E-Mail Service to End Users, no Personal Information of End Users will be required to be provided by one party to the other under this Agreement. In providing the E-Mail Service Microsoft will be receiving information from End Users that may contain Personal Information. Microsoft shall not collect, use or disclose any Personal Information of End Users, or any derivatives of such Personal Information, except to provide the E-Mail Service to End Users and perform its obligations under this Agreement or except as otherwise permitted under this Agreement. (4.a)
* There are no cookies, actions tags, or any similar technology used by Microsoft in the E-Mail Services to obtain, track, monitor, implement any form of profiling, or assessment of Covered Data and Information except as may be described in this Agreement to provide and improve the E-Mail Service. (3.d.iv)
* In order to provide the Microsoft Services, Microsoft may collect certain information about Microsoft Service performance, End User machines and Microsoft Service use. (4.f) Microsoft assures us that this information is not Personally Identifiable Information.

Karen McGregor, Education Solution Specialist from Microsoft has provided the following information to the University:

“Service Data include performance data or information from the PC as to the browser being used so that the OWA experience can be optimized. Information is aggregated for reporting but not tracked with Personal Identifiable Information.”

The University Notice of Collection will explain purposes of collection of personal information.

The University is satisfied that Microsoft’s conduct, as stated in the Agreement, provides privacy protection of personal information in collection that is equal to or exceeds FIPPA.

## Use

There is a risk that Microsoft or its affiliates could *use* the personal information collected by the Office365 service in a manner not consistent with the intent of the collection. After Microsoft collects information, the University will be unable to confirm how the information is used so all uses use of the information in the Office365 service must be expressly set out in the contract.

The contract includes the following statements about use of personal information:

* …Microsoft shall not collect, use or disclose any Personal Information of End Users, or any derivatives of such Personal Information, except to provide the E-Mail Service to End Users and perform its obligations under this Agreement or except as otherwise permitted under this Agreement. (4.a)
* Each party shall take commercially reasonable security and other measures to protect the Covered Data and Information and Credentials under its control from unauthorized access, use, disclosure, alteration and destruction and will protect Covered Data and Information and Credentials in its possession and control as it protects its own confidential information of like nature. Such security measures will include authentication controls, encryption of Covered Data and Information while in transit, physical controls or other means in accordance with each party’s own information security policy. (4.c.i)
* In order to operate and provide the Microsoft Services, Microsoft may collect Personal Information about End Users as provided for under this Agreement. Microsoft may access or disclose Institution or End User information, including the content of End User communications, in order to: … (2) take action or pursue other remedies against suspected purveyors of spam, viruses, malware, phishing or other attacks that have in any manner disrupted or diminished, or may in the future in any manner disrupt or diminish, Microsoft’s services; ... (4.e)

With these provisions, the University understands Microsoft’s conduct to provide privacy protection of personal information in use that is equal to or exceeds FIPPA expectations.

## Disclosure

There is a risk that Microsoft or an affiliate could *disclose* personal information collected by Office365 in a manner not consistent with the intent of the collection. In addition to impacts listed in the introduction to this section, inappropriate disclosure of personal information could lead to identity theft and invasion of privacy. Mitigations to address these concerns include:

* Microsoft states in the agreement that it will implement security measures including “encryption of Covered Data and Information while in transit”. (4.c.i)
* A technical analysis of Office365 security infrastructure was performed based on a SAS70 Type II report and other documents available on the Microsoft website, referenced in the “Resources Consulted” section. The Microsoft security environment was found to be equivalent to or better than that of the University. See the “Privacy by Design” and “Data Flows” sections of this document for more detail. One relevant quote from the SAS70 states: “The Online Services Security Policy establishes the access control requirements for requesting and provisioning user access for accounts and services in the […] environment. The policy requires that access be denied by default, follow least privilege principles, be allocated through role-based controls, and be granted only upon business need. The policy also requires asset owners or associated agents to review the appropriateness of access and privileges on a periodic basis.”

The contract with Microsoft states:

* …Microsoft shall not collect, use or disclose any Personal Information of End Users, or any derivatives of such Personal Information, except to provide the E-Mail Service to End Users and perform its obligations under this Agreement or except as otherwise permitted under this Agreement. (4.a)
* …Microsoft may access or disclose Institution or End User information, including the content of End User communications, in order to: (1) comply with the law or respond to lawful requests or legal process; (2) take action or pursue other remedies against suspected purveyors of spam, viruses, malware, phishing or other attacks that have in any manner disrupted or diminished, or may in the future in any manner disrupt or diminish, Microsoft’s services; or (3) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of any individuals from a life threatening emergency. Solely with respect to any disclosure made pursuant to subsection (1) above, Microsoft will use commercially reasonable efforts to provide Institution notice, when legally permissible to do so, that a demand for Institution and/or End User information has been made, prior to the disclosure of any such information. In any instance where Microsoft is prohibited by law from providing notice, Microsoft will comply with any such lawful request or legal process demanding Institution and/or End User information. Solely with respect to any disclosure made pursuant to subsections (2) and (3) above, Microsoft will provide Institution notice, within a commercially reasonable amount of time that a disclosure has been made of Institution and/or End User information. (4.e)
* Microsoft shall, within a commercially reasonable period of time after discovery of any unauthorized or unlawful access to, loss or disclosure or alteration of or malicious compromise of any Covered Data and Information in its possession or control (a “Security Incident”): (4.c.vi)
	1. notify Institution of the Security Incident;
	2. investigate the Security Incident and provide Institution with detailed information about the same;
	3. provide reasonable assistance to Institution to the extent necessary to enable Institution to comply with applicable law implicated by the Security Incident;
	4. take steps to mitigate the effects and minimize the damage resulting from the Security Incident; and
	5. make changes to minimize the likelihood that the Security Incident will re-occur.

## Retention

The University must retain personal information for at least a year after the date of its last use. Confidential information must also be protected from destruction and kept accurate and up-to-date. Microsoft will maintain user information in its systems in accordance with terms of use agreed to by staff and faculty. Notice will be provided to the University as follows:

* Microsoft will notify Institution of any suspended or terminated End User email account. (4.c.ii)

It will be the University’s responsibility to retain records for one year consistent with FIPPA.

## Disposal

There is a risk that personal information stored in Office365 could be *disposed* of improperly, leading to a disclosure of personal information.

The Agreement states:

Microsoft will provide Institution with industry standard interfaces and protocols to enable Institution, at any time, to extract all Covered Data and Information, and, upon request, Microsoft shall destroy or return to Institution all Covered Data and Information, content, technology and materials forwarded to Microsoft by Institution or its End Users under this Agreement. (8.d)

Microsoft has also indicated in its SAS70 Type II report that it has an audited backup tape disposal process.

## Security

In addition to security analyses of Office365 set out elsewhere in this assessment, the agreement states:

* Microsoft shall cause its external auditors to provide to Institution a SAS 70 Type II report (or equivalent) annually throughout the term of the Agreement on the design, existence, effective operation and continuity of Microsoft’s control procedures in respect of the E-Mail Service. Where the SAS 70 Type II report identifies material deficiencies in the performance of the E-Mail Service, Microsoft shall provide to Institution a remedial plan to address such deficiencies and shall report to Institution on the progress made in executing such plan. (4.k)
* Each party shall take commercially reasonable security and other measures to protect the Covered Data and Information and Credentials in its possession and control from unauthorized access, use, disclosure, alteration and destruction and will protect Covered Data and Information and Credentials in its possession and control as it protects its own highly confidential information. Such security measures will include authentication controls, encryption of Covered Data and Information while in transit, physical controls or other means in accordance with each party’s own information security policy (4.c.i)

These clauses provide security assurances consistent with FIPPA requirements.

# Office365 Dataflows and Processes

#### Overview

The following section is adapted from the Live@edu PIA for students. Some of the information here may be inaccurate since the procedures surrounding the move of staff and faculty have not been fully worked through at time of writing. While some details may change, the main features of outsourcing email as outlined in these data flows will remain the same.

The following diagram is an overview of major parties involved in this service:



***Office365* User**

These are the users of the service, UofT staff and faculty, whose personally identifiable information will be stored in the system.

**Microsoft *Office365* Administrator**

These are administrators employed by Microsoft to staff their data centers and provide support for their *Office365* platform. From the standard *Office365* contract, Microsoft does “not use or allow access to personally identifiable information from education records, other than directory information, except in connection with services to be provided under the Agreement or as the Institution otherwise directs.”

**UofT *Office365* Administrator**

These are UofT administrators who will have some access to the *Office365* platform. UofT policy governs the access a UofT administrator has into the *Office365* system.

**Third Party Affiliates**

Microsoft has indicated that it may provide aggregate statistics to third party affiliates but ensures that no personally identifiable information will be revealed in this transfer.

#### Initial Setup

There are two steps in this process: provisioning and migration.

**Provisioning**

“Provisioning” refers to the process by which an account is created for a user on the *Office365* servers. This is a two step process:

 

1. A secure connection is established from the UofT account management system to the UofT provisioning server by a UofT system administrator. All communication over this channel is encrypted using the SSL protocol.
2. Using Remote Powershell, the UofT admin then establishes a secure connection to the Microsoft *Office365* service.
	1. The user’s first name, last name, WLID-eppn (UTORid@domain), WLID-uid (a one-way hash of the UTID) and email address are communicated to the Microsoft Office365 servers during this step
	2. This connection is authenticated with a UofT System Administrator username and password and all communication over this channel is over HTTPS, an internet protocol that is encrypted using the SSL protocol.

**Migration to *Office365***

Once provisioning is complete, migration user mailbox may begin. This is a four step process:



1. Using Remote Powershell, the UofT Administrator establishes a secure connection from the UofT *Office365* Migration server to the Microsoft *Office365* service. This connection is authenticated with a UofT System Administrator username and password and all communication over this channel is over HTTPS, an internet protocol that is encrypted using the SSL protocol.
2. A connection is then established with the UTORmail Mailbox server that contains the user’s email inbox. This connection uses the SSH protocol which is encrypted with SSL.
3. The user’s mailbox is “mounted” on the migration server, giving the migration server access to the contents of the user’s email inbox.
4. The user’s email is transferred to the *Office365* service, into the account that was provisioned for this user.

Once this process is complete, the UofT Administrator will update the mail routing data for the user’s email address. This will result in all new and queued messages for that user being processed and delivered to *Office365*.

From a privacy perspective, this migration process is well thought out. All of the connections to the *Office365* service are fully encrypted to ensure that communication between UofT and Microsoft is protected from eavesdroppers.

#### Email Flow

One of the primary sources of personally identifiable information in this service will be email. Microsoft has indicated that they support a protocol extension called “opportunistic SMTP” for encrypting the email flow between *Office365* and the users of their service. This means that the University is able to force encryption between UofT mail routers and the *Office365* mail servers (this is done by ensuring that the University’s mail routing servers will only initiate or accept connections to and from Microsoft that are encrypted). The digital certificates used to implement encryption can also function as a verification of identity (authentication). It should be noted that in the case of email flow, Microsoft uses the certificates primarily to encrypt the data, not provide authentication. In this context the primary concern is encryption, so there is little problem with Microsoft using the technology in this way.

**Forefront Online Protection for Exchange**

The encryption of mail flowing between the University’s mail routers and Microsoft’s is provided by a service called Forefront Online Protection for Exchange (FOPE). This service has been tested to be active by the University of Toronto. The functioning of this service is reinforced through firewall rules, managed by the University of Toronto, that block traffic on unencrypted ports, and through the configuration of the UofT Message Router to only accept encrypted traffic, regardless of network port.



**Incoming Flow**

1. Email arrives at the UofT Message Routing Servers from somewhere else in the world. UofT offers “Opportunistic TLS”, which means that if the sending email server supports encryption via TLS, the University prefers that method of exchange.
2. On the UofT routing servers a lookup is performed that determines whether a user is using *Office365* or whether they have opted-out and forwarded their mail elsewhere. (UTORexchange is included in this diagram only to indicate that staff / faculty email remains within the University and is not forwarded on to an external 3rd party).
	1. If the user uses *Office365*, the message is sent to the *Office365* servers over a secure channel encrypted with SSL/TLS.
	2. If the user has opted-out, the message is forwarded on to the 3rd party service provider the user has chosen. Here again, UofT is willing to use TLS to encrypt the exchange if the 3rd party agrees, although encryption will not be forced.

**Outgoing Email Flow**

All Email that leaves a user’s account on *Office365* will be routed through UofT’s message routing servers. Please note that this is based on preliminary information from UofT’s implementation team and may change slightly with the final architecture.



1. A user sends an email through the Microsoft *Office365* service.
2. That email is sent securely through an encrypted channel to the UofT Message Processors which will determine where the message is to be delivered.
3. The message will be delivered:
	1. Back to the *Office365* service over an encrypted channel if the recipient specified is another UofT *Office365* user.
	2. To the UTORexchange servers if the recipient specified is a staff / faculty member of UofT who uses the UTORexchange service.
	3. Otherwise, the message is routed out to the recipient’s email provider outside of the UofT.

The assurance that the University can force the encryption of email flowing between UofT and *Office365* provides an essential guard to privacy.

#### Web-Based Access to Office365

The University anticipates that the majority of users will access their email through a web-based interface. This is excellent from a privacy perspective because the type of authentication used for web-based services does not send the user’s username and password to *Office365*. The services included under this authentication method are:

* Outlook Web Access



1. The user initiates a request to connect to *Office365* through a web browser or other web technology. This session is conducted over HTTPS, which is encrypted with SSL/TLS.
2. The *Office365* server redirects the user to UofT’s Identity Provider (IdP) for authentication.
3. The UofT IdP will present the user with the standard UofT login page into which the user will type their UTORid and password. The UofT login page is encrypted with SSL/TLS.
4. Upon successful login, the UofT IdP server will send the user back to *Office365* (over SSL) with an assertion, which includes the following attributes:
	1. User’s WLID-eppn (UTORid@domain)
	2. User’s WLID-uid (a one way hash of the UTID)
	3. An authentication token that indicates to *Office365* that UofT has authenticated the user
5. The user now has an established web-based session with *Office365* and begins to use their services. This session is encrypted with SSL/TLS for the entire duration.

#### Non Web-Based Access to Office365

While the University does anticipate that the majority of users will connect to *Office365* through web-based technologies, there will undoubtedly be some who use other methods to connect. The authentication procedure is slightly different in this case, as is detailed in the following diagram. The services included under this authentication method are:

* IMAPS, POP3S (Mail receiving protocols)
* SMTP (Mail delivery protocols)
* LDAP, LDAPs
* Outlook Anywhere (RPC/https)
* Exchange Web Services
* ActiveSync



1. A secure connection is established with the *Office365* servers, encrypted with SSL/TLS. Authentication is requested by *Office365*.
2. User sends their authentication credentials consisting of their username (UTORid) in the form *utorid@mail.utoronto.ca* and their password.
3. *Office365* infers from the @mail.utoronto.ca portion of the username the proper Identity Provider (IdP) to contact and sends the username / password pair to the IdP over an encrypted channel.
4. UofT’s IdP validates the credentials and responds with an assertion that includes:
	1. User’s WLID-eppn (UTORid@domain)
	2. User’s WLID-uid (one way hash of the UTID)
	3. An authentication token that indicates to *Office365* that UofT has authenticated the user
5. The user can begin to use the *Office365* service over their encrypted channel.

It is important to note that in this process Microsoft has assured UofT that no usernames and passwords are ever stored on the *Office365* servers. The username and password are only kept temporarily in memory for the purposes of authenticating the user and are then removed.

#### Backups

Protecting the data in a system includes making sure that it is regularly backed up in case of a failure. Microsoft has provided assurances in the SAS 70 report that data is encrypted before it is backed up, and backup tapes are securely destroyed at the end of their lifecycle.

#### Termination of Service

When an *Office365* user is no longer a staff/faculty member of the University they will no longer have access to *Office365*’s services through the University. *Office365* does not have access to staff status data, and therefore relies on UofT to terminate service. *Office365* will hold all the contents of all deleted accounts for 30 days, at which point the information will be disposed of.

# USA PATRIOT Act

The University of Alberta email outsourcing project website provides useful information about the USA PATRIOT act, which is included here for reference.[[42]](#footnote-42)

**Q. Does the US Patriot Act allow the US government to access my personal information?**

A. Yes. The Patriot Act allows for the US Government to access personal information that is held or accessible by anyone within the United States or any US citizen by two different methods. The first tool which the US Government possesses is found in Section 215 of the Patriot Act. Under this section the relevant Government agency must apply to a court for an order allowing them to access the personal information in question. The information which can be collected pursuant to this court order is very broad. The second tool which the US Government has is found in Section 505 of the Patriot Act. It is under this section that the Government can issue National Security Letters whereby they can request that personal information be disclosed to them. The information can be accessed where it meets the following criteria: that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. No court order is necessary for a National Security Letter to be issued; however, the type of information that is retrievable is more limited than through that available in a Section 215 (see above) order.

It should be noted that Canadian authorities have very similar abilities to access personal information to those in the USA PATROIT act, in Canadian legislation such as the Criminal Code, the Canadian Security Intelligence Service Act and the National Defense Act, among others. A key difference is that in general Canadian legislation requires warrants for seizure of personal information to be issued by a judge. Commenting on PIPEDA case #313 (*Bank’s notification to customers triggers PATRIOT Act concerns)*, the federal Privacy Commisioner states:

“The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities. Despite the objections of the Office of the Privacy Commissioner, the Personal Information Protection and Electronic Documents Act has been amended since the events of September 11th, 2001, so as to permit organizations to collect and use personal information without consent for the purpose of disclosing this information to government institutions, if the information relates to national security, the defense of Canada or the conduct of international affairs. In addition to these measures, there are longstanding formal bilateral agreements between the U.S. and Canadian government agencies that provide for mutual cooperation and for the exchange of relevant information. These mechanisms are still available.” [[43]](#footnote-43)

At a recent symposium on cloud-based email services hosted by Ryerson University, Ontario Privacy Commissioner Dr. Ann Cavoukian stated:

“Whether you have the PATRIOT ACT doesn’t matter, there will always be law enforcement techniques that will access certain types of [personal] information. What you should concern yourself with is the kind of accountability that you will be able to maintain if your email system should go into the cloud. … In my book, you can outsource your services but you cannot outsource accountability.”

#  FIPPA Definition of Personal Information

FIPPA s. 2 defines personal information as follows:

“personal information” means recorded information about an identifiable individual, including,

1. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
2. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
3. any identifying number, symbol or other particular assigned to the individual,
4. the address, telephone number, fingerprints or blood type of the individual,
5. the personal opinions or views of the individual except where they relate to another individual,
6. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
7. the views or opinions of another individual about the individual, and
8. the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; (“renseignements personnels”)

# Privacy by Design Principles

1. **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. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

1. **Privacy as the Default**

We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by *default*.

1. **Privacy Embedded into Design**

*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

1. **Full Functionality – Positive-Sum, not Zero-Sum**

*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy *vs*. security, demonstrating that it *is* possible to have both.

1. **End-to-End Lifecycle Protection**

*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

1. **Visibility and Transparency**

*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

1. **Respect for User Privacy**

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

# CSA Privacy Code Principles

**1. Accountability**
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

**2. Identifying Purposes**
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

**3. Consent**
The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

**4. Limiting Collection**
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

**5. Limiting Use, Disclosure and Retention**
Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

**6. Accuracy**
Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

**7. Safeguards**
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

**8. Openness**
An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

**9. Individual Access**
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

**10. Challenging Compliance**
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

# Technology Overview

## SSL/TLS

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) provide security for data that is in transit through the use of cryptographic protocols. SSL/TLS provides a vital piece of a privacy-respecting software solution by protecting with encryption all of a user's communications with a remote third-party. A SSL/TLS session is initiated by the two parties (in most cases this is a client and a server) taking part in what is called a "handshake". The essential features of this handshake include:

1. The server and client decide on the strongest form of encryption that both support.
2. The server sends its identification to the client in the form of a digital certificate.
3. The client verifies the validity of the server's certificate by ensuring that the authority that issued it is a trusted third-party (called a certificate authority).
4. The client generates a random number that will be used to encrypt all further communications, encrypts it in a way that only the server can read, and sends this encrypted number to the server.

Once the handshake has been completed as detailed, all further communications between the server and client during the session are securely encrypted with this random number that the two have exchanged. For the purposes of this document when service supporting SSL/TLS is referred to, it is meant that the communications between server and client for that service implement this protocol to ensure all transmissions between them are encrypted and unreadable by anyone else *while in transit*.

## Shibboleth

Shibboleth is a framework for the exchange of authentication and authorization information between organizations without the need for either organization to see the usernames or passwords of the other. The protocol underlying Shibboleth is the Security Assertion Markup Language (SAML) which defines how security assertions are made between two organizations that trust one another. This technology provides a key building block in protecting a user's privacy since it does away with the need to transmit such highly personal information as a user's password to an organization outside of the University of Toronto. The Shibboleth technology is mainly used for web-based applications although work is underway to enable it to support "rich" clients like Outlook and Thunderbird as well.

A typical SAML authentication process has a number of steps which are summarized in the diagram below. In this diagram, three parties are referenced:

1. IdP (Identity Provider) - The organization that is providing the authentication credentials; in this case, the University of Toronto
2. SP (Service Provider) - The organization that is providing a service; in this case, Microsoft Office365.
3. User Agent - This is the user who is accessing Office365 through their web browser.



Figure 1: SAML 2.0 Authentication Flow [[44]](#footnote-44)

1. A user accesses a resource hosted by a SP that is protected, requiring authentication.
2. After discovering the user's IdP either through configuration or a WAYF (Where Are You From) screen, the SP responds with an XHTML form specially crafted to bounce the user over to their IdP for authentication.
3. The user issues an authentication request to their IdP, and the user is identified with an appropriate access control mechanism.
4. The IdP passes back a SAML assertion in an XHTML form that is crafted in the form of an "assertion".
5. The user once again requests the assertion service at the SP.
6. The SP processes the request, creates a security context (often referred to as "logging in") and directs the user to the target resource.
7. The user once again requests the target resource.
8. Since the security context has been established, the SP returns the requested resource.

# Cloud Computing Models



Figure 2 -- Left: Clear Distinction between the Trusted and the Untrusted; Right: Fuzzy Security Perimeter[[45]](#footnote-45)

Cloud Computing has become an umbrella term for so many emerging technologies, that some clarification of what is meant is necessary. A paper released by the *Cloud Security Alliance* provides a helpful delineation of Cloud *Service* and *Deployment* Models.

#### Cloud Service Models[[46]](#footnote-46)

* **Software as a Service (SaaS)** – This is the capability provided to a consumer to run the provider’s applications in a cloud infrastructure. The applications are made accessible from various client devices usually through a thin-client interface such as a web browser. In this model the consumer does not manage or control any of the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
* **Platform as a Service (Paas)** – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
* **Infrastructure as a Service (IaaS)** – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

#### Cloud Deployment Models[[47]](#footnote-47)

* **Public Cloud** – The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
* **Private Cloud** – The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.
* **Community Cloud** – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.
* **Hybrid Cloud** – The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

# Work Units

Relevant University and Microsoft units collaborated on the Privacy Impact Assessment.

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

## University of Toronto

### Information + Technology Services

|  |  |
| --- | --- |
| Name | Role |
| Bob Cook | Information + Technology Services, CIO |
| Martin Loeffler | Information Security, Director, Security Lead |
| David Auclair | Information Security, PIA Author |
| Matt Wilks | Information Security, PIA Author |
| Axel Johnston | Information Security, PIA Author |
| Paul Ruppert | Integrated Client Services, Director |
| Marden Paul | Planning, Governance and Assessment, Director |
| Vicki Vokas | Web Services Project Office, Manager |
| Alex Nishri | Integrated Client Services, Manager -- Email and UTOR Services |
| Derek Yuen | Integrated Client Services, Project Manager |
| Peter Ip | Integrated Client Services, Chief Integration Engineer |
| Paul Fardy | Integrated Client Services, Authentication Specialist |
| Michael Simms | Integrated Client Services, Network Services Specialist |
| George Katterloher | Integrated Client Services, Network Services Specialist |
| Hong Zhu | Integrated Client Services |
| Stanley Alleyne | Integrated Client Services |
| Richard Sanford | Integrated Client Services |
| Chad Holden | Integrated Client Services, Web Architect |
| Mike Clark | Integrated Client Services, User Experience Designer |
| Crisan Diaconu,  | EASI, Technical Writer |
| Peter Eden, | Supervisor, Network Administration, Security review |
| Kevin Howie,  | Assistant Dean, Operations, Security review |
| Wes Robertson, | Director, Information Technology, Security review |

### Freedom of Information and Protection of Privacy office

|  |  |
| --- | --- |
| Name | Role |
| Rafael Eskenazi | FIPP Director |
| Howard Jones | FIPP Coordinator |

## Microsoft

| Name | Role |
| --- | --- |
| David Fisher | Senior Product Manager, Office365 Research and Development |
| Brad Tipp | Education Solution Specialist, Office365 |
| Richard Wakeman | Solution Architect, Microsoft Consulting Services |
| Raj Mukherjee | Senior Product Manager, Online Services |
| Gabe Long | Release Manager, Office365 Support |
| John Weigelt | National Technology Officer, Microsoft Canada |
| Chris Tardif | Principal Consultant, Microsoft Consulting Services |
| Karen McGregor | Education Solution Specialist, Microsoft Canada |
| Shann McGrail | Education Director, Microsoft Canada |
| Mike Tremblay | Director, Public Sector |
| Glen Donegan | Account Manager for U of T |

1. Municipalities, Universities, Schools, and Hospitals, 2006 <http://www.priv.gc.ca/fs-fi/02_05_d_25_e.cfm> (December 2010) [↑](#footnote-ref-1)
2. [http://www.edmontonjournal.com/technology/inks+Gmail+deal+with+Google/3949065/story.html](http://www.edmontonjournal.com/technology/inks%2BGmail%2Bdeal%2Bwith%2BGoogle/3949065/story.html) [↑](#footnote-ref-2)
3. <http://www.canlii.org/en/on/onla/doc/2009/2009canlii24632/2009canlii24632.pdf> [↑](#footnote-ref-3)
4. <http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf> [↑](#footnote-ref-4)
5. <http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf> [↑](#footnote-ref-5)
6. <http://www.privacybydesign.ca/content/uploads/2011/02/pbd-ont-smartgrid-casestudy.pdf> [↑](#footnote-ref-6)
7. <http://www.privacybydesign.ca/content/uploads/2008/05/privacyintheclouds.pdf> [↑](#footnote-ref-7)
8. <http://www.privacybydesign.ca/content/uploads/2006/10/7laws_whitepaper.pdf> [↑](#footnote-ref-8)
9. <http://download.microsoft.com/download/B/C/A/BCAD4354-99E8-4A80-BCE3-210A74ECFA6C/Microsoft_and_Data_Privacy_final.pdf> [↑](#footnote-ref-9)
10. [http://download.microsoft.com/download/7/9/8/7988DF4C-142E-4A29-96BE-2384C524AB68/TwC-Enterprise-CTZ 3-Data Governance-Data Retention-BackgrounderFS.docx](http://download.microsoft.com/download/7/9/8/7988DF4C-142E-4A29-96BE-2384C524AB68/TwC-Enterprise-CTZ%203-Data%20Governance-Data%20Retention-BackgrounderFS.docx) [↑](#footnote-ref-10)
11. <http://download.microsoft.com/download/3/8/5/385BEAE9-72E9-4F7F-A798-9D54F896351A/privacy_guidelines_for_developers.pdf> [↑](#footnote-ref-11)
12. <http://download.microsoft.com/download/3/9/1/3912E37E-5D7A-4775-B677-B7C2BAF10807/cloud_privacy_wp_102809.pdf> [↑](#footnote-ref-12)
13. <http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf> [↑](#footnote-ref-13)
14. <http://www.cloudsecurityalliance.org/csaguide.pdf> [↑](#footnote-ref-14)
15. <http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf> [↑](#footnote-ref-15)
16. <http://www.microsoft.com/presspass/exec/steve/2010/03-04Cloud.mspx> [↑](#footnote-ref-16)
17. <http://www.microsoft.com/privacy/research.aspx> [↑](#footnote-ref-17)
18. <http://www.its.utoronto.ca/rules-and-regulations/regulations_guidelines/Information_Security_Guidelines.htm> [↑](#footnote-ref-18)
19. [http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf](http://cdn.globalfoundationservices.com/documents/WP_Securing_Microsoft_Cloud_Infrastructure.pdf), page 11 [↑](#footnote-ref-19)
20. <http://www.its.utoronto.ca/rules-and-regulations/regulations_guidelines/informationsecurity/Data_Protection_Guidelines.htm> [↑](#footnote-ref-20)
21. Documents created in a personal space are private by default. Documents created in a shared folder inherit the privileges of that folder, so the potential for sharing a document accidentally exists. [↑](#footnote-ref-21)
22. <http://download.microsoft.com/download/3/8/5/385BEAE9-72E9-4F7F-A798-9D54F896351A/privacy_guidelines_for_developers.pdf> [↑](#footnote-ref-22)
23. http://www.its.utoronto.ca/tri-campus\_it/its\_info/ITS\_Comm\_and\_Consult/studentecomm.htm [↑](#footnote-ref-23)
24. *ISO/IEC 27001 Certification Standard*, <http://www.iso27001security.com/html/27001.html> (Novemember 2010). [↑](#footnote-ref-24)
25. <http://msdn.microsoft.com/en-us/library/ms995349> [↑](#footnote-ref-25)
26. <http://go.microsoft.com/?linkid=9746120> [↑](#footnote-ref-26)
27. <http://en.wikipedia.org/wiki/ISO/IEC_27001> [↑](#footnote-ref-27)
28. [Microsoft ISO 27001 Certifications](http://www.bsiamerica.com/en-us/Assessment-and-Certification-services/Management-systems/Certificate-and-Client-Directory-search/Search/Search-Results/?pg=1&licencenumber=IS+533913&searchkey=licenceXeqX533913XandXcompanyXeqXMicrosoft) [↑](#footnote-ref-28)
29. <http://blogs.technet.com/b/gfs/archive/2010/12/01/microsoft-s-cloud-infrastructure-receives-fisma-approval.aspx> [↑](#footnote-ref-29)
30. <http://en.wikipedia.org/wiki/FISMA> [↑](#footnote-ref-30)
31. <http://csrc.nist.gov/groups/SMA/fisma/index.html> [↑](#footnote-ref-31)
32. <http://www.fippa.utoronto.ca/Page4.aspx> [↑](#footnote-ref-32)
33. [http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/fippa.pdf](http://www.provost.utoronto.ca/Assets/Provost%2BDigital%2BAssets/Provost/fippa.pdf) [↑](#footnote-ref-33)
34. <http://www.microsoft.com/privacy/default.aspx> [↑](#footnote-ref-34)
35. <http://go.microsoft.com/?linkid=9741061> [↑](#footnote-ref-35)
36. <http://techcrunch.com/2010/09/14/google-engineer-spying-fired/> [↑](#footnote-ref-36)
37. http://www.pcworld.com/article/214591/microsoft\_bpos\_cloud\_service\_hit\_with\_data\_breach.html?tk=mod\_rel [↑](#footnote-ref-37)
38. Besides being technically hard to implement, encrypting only the message body is of dubious value given the circumstances. As Fred Carter of the IPC said at the Email Symposium held at Ryerson University: “Without minimizing the importance of encryption … all the action is in traffic data and who is talking to whom. A PGP type system doesn’t [protect], in fact it actually facilitates … [the ability to] track everyone [a person] is communicating with and how frequently. … Maher Arar was hung because of who he spoke with, not because of anything he said.” [↑](#footnote-ref-38)
39. <http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf>, page 17 [↑](#footnote-ref-39)
40. <http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf>, page 20 [↑](#footnote-ref-40)
41. <http://go.microsoft.com/?linkid=9746120>, page 9 [↑](#footnote-ref-41)
42. *Frequently Asked Questions*, 2010 <http://www.vpit.ualberta.ca/email/index.php?ref=faq#PrivacyShow> (December 2010) [↑](#footnote-ref-42)
43. *PIPEDA Case Summary #313 (Bank’s notification to customers triggers PATRIOT Act concerns)*, 2005 <http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.cfm> (December 2010) [↑](#footnote-ref-43)
44. https://secure.wikimedia.org/wikipedia/en/wiki/SAML\_2.0 [↑](#footnote-ref-44)
45. *Modelling Cloud Computing Architecture Without Compromising Privacy*, 2010 <http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=961> (July 2010), p. 6 [↑](#footnote-ref-45)
46. *Security Guidance for Critical Areas of Focus in Cloud Computing v2.1*, 2009 <http://www.cloudsecurityalliance.org/csaguide.pdf> (November 2010), p. 15-16 [↑](#footnote-ref-46)
47. ibid., p. 17 [↑](#footnote-ref-47)