Privacy Impact Assessment

University of Windsor Considerations in Moving Student Email to the Cloud

1. Executive Summary:

The University of Windsor is exploring moving student webmail to an off-campus provider. To fully understand the implications of such a move, the University is trying to understand the risks involved. These risks are to student email data and also to the reputation of the University.

Two vendors are being considered, Google via Google Apps for Education and Microsoft via Live@EDU. Both providers are large, mature corporations with many Universities world-wide using their services. Over a thousand higher-education institutions in the United States and more than 90% of Australian Universities use these services. It is becoming a growing trend among Canadian Universities to utilize these services.

After consideration of questions asked to both vendors, understanding the risks from legal, technical and procedural sources and examining Terms of Use agreements from both vendors, it is likely that moving the service off-campus does not change the risk to student email or other University of Windsor data.

2. Introduction:

A privacy impact assessment (PIA) is a process for determining and addressing privacy risk during the development and implementation of projects that involve or affect personal information. The PIA is an analysis of how project data flows align with legal, policy, practice and stakeholder privacy expectations. The PIA is a tool for executives to understand and address privacy risk in the project. The PIA is a living document that will continue to develop as the project develops. It borrows heavily from work done at other Universities in Canada as they examined privacy impact on their move to an outside provider.

As a result of consultation with campus stakeholders concerning student e-communication, the Executive Director of IT Services has recommended that the University consider an outsourced solution for student email. The two external service providers being considered are U.S. based : Google and Microsoft.

Security and privacy are linked, effective security is necessary to have privacy. The University committee looking at the implications of moving student email off-campus regards 'security' as the effective and reliable mitigation of risk to confidentiality, integrity, availability and

accountability for use of data, in the context of solutions-specific vulnerabilities, and the sensitivity of data to risk.

3. Introduction to the Project:

A project team has been created to evaluate the University of Windsor Student Email service with the goal of determining whether the service should be moved to an outside provider. This model of technology service is known as "Cloud Computing". Cloud computing has been defined as "new generation of computing that utilizes distant (internet based) servers for data storage and management". [1]

Currently the University uses the web-based application Communigate Pro for student email. Email quotas are set at 100 Megabytes. Students have 20 Megabytes of space to create their own web pages. Reasons for considering moving the student email service include:

- Increased email service to students by providing new features and a higher level of service for existing features. Examples are more storage space, easier provisioning with mobile devices and easier methods to work together in a team environment are all possibilities.
- Additional web based applications for word processing, spreadsheet, presentations calendar sharing, and chat.
- Lower cost to deliver improved service.

Two cloud computing options are being considered and compared to the University of Windsor's current service offering. The options area:

- Google Apps for Education
- Microsoft Live@EDU

4. Project Description:

The project is focused on evaluating multiple areas of service and risk. Consideration has been given to:

- Service offerings and benefits
- Security, Privacy & Policy
- Technical differences between competing options and fit with the University's infrastructure
- Cost

[1] http://www.financenewmexico.org/glossary.html (March 28, 2011)

Initial concerns that were raised regarding privacy and policy that needed to be examined included:

- FIPPA policy and general privacy concerns with respect to UWindsor internal email traffic on the Internet
- Existing University of Windsor policy that affect the student email service
- Concerns regarding possible email hosting in the United States and the PATRIOT Act

This document focuses on the privacy and policy aspects of the project. It attempts to identify as many risks as possible and outline strategies to mitigate risk. While it is impossible to identify all risks in any particular situation, a number of other Universities have moved to the Cloud computing model and have identified their plans to address the situations they have determined. This document borrows heavily from the risks identified by other institutions[2] and proposes University of Windsor solutions to them.

5. Nature of Information at Risk

The University of Windsor currently uses email to communicate with students to achieve a variety of purposes.

- respond to general queries.
- Registration information
- Payroll information
- communication in regards to accommodation of disabilities;
- academic marks, standing, and censure;
- financial matters;
- updates of personal / contact information;
- course requirements

Given that these communications take place via email, and that email between students is not separated from email between students and the University, all email must be regarded as being as sensitive as the most confidential of these communications. The sensitivities are as follows:

(a) Communication in regards to accommodation of disabilities: Personally identifiable and health-related information.

(b) Academic censure, standing and marks; and, personal/contact information: Personally identifiable information – FIPPA protected.

[2] Many thanks to the work that have been done by the University of Alberta and the University of Toronto (http://www.google.ca/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.its.utoronto.ca%2FAssets%2FITS%2BDigital%2BAssets%2Fpia.pdf&rct=j&q=interim%20privacy%20impact%20assesment%20student%20e-communications&ei=176RTZv1DIragQeT5Z0Z&usg=AFQjCNET_ie2wtO6HIHO_e7l4RIpkhsTVg&cad=rja)

6. Risks

Risks in an email environment are many and varied, but the primary concern relates to the following:

- Inappropriate access (disclosure / duplication / modification / deletion) to / of individual accounts, includes data mining, user/account profiling or any form of tracking, account access by foreign governments (e.g. U.S. Patriot Act), ;
- Loss of data in bulk;
- Loss of service; and
- Lack of accountability for use.

Given that each system under consideration provides the same basic functionality, using the same information (and absent system-specific architectural information), the threats to information are the same across all solutions.

It is important to understand that any email communication has a low expectation of privacy. The current University of Windsor system provides network security between the faculty/staff system by physically securing the network connection between the two systems, however what any individual does with an email they receive cannot be guaranteed. Two general risks are that the receiving individual may share the email, or they may forward the email to a system outside the University's control.

Email that is sent to an email address outside the University should not be considered private since it becomes a record of the intended party, and the travel path that the email takes cannot be guaranteed. It may travel through a large number of jurisdictions which may keep records. Generally an email that is sent outside the University should be treated similar to sending a postcard through regular mail.

Aggregate Sensitivity

Unless alternative arrangements are made in the handling of PHIPPA/FIPPA protected data, all email must be considered confidential and must be encrypted when in transit between the University of Windsor network and the service provider. No service providers offer encryption of data at rest, so protection of data stored at the service provider will need to be handled contractually and through SAS 70 auditing. If FIPPA protected data is removed from email sent by the University to students, while potentially private in nature from a student's point of view, the content of email is no longer classified by the University as confidential; while still requiring adequate access controls, non-confidential data does not require encryption outside of the University network.

System Specific Risks

System-specific vulnerabilities will be detailed after technology-level vendor discussions. Broadly speaking, vulnerabilities can be characterized as residing in the following areas:

Identification

In email, access identification is often the same as, or a portion of, a user's email address, which is communicated in clear text as part of the body of an email message; as such, access identifiers are low-sensitivity data, and the risk due to disclosure of access identifiers is low.

Authentication

Access credentials can be observed in transit, recovered from storage / memory, captured when input, or retrieved by administrators. As access credentials (i.e. passwords) are typically re-used many times before refresh, and provide full access to users' data when used in combination with easily-guessed access identifiers, access credentials are considered high –sensitivity data. As such, they must be protected from disclosure while in storage, transmission, use and administration.

Authorization

Account permissions are typically stored and administered by the service – vulnerabilities to account permissions are associated with vulnerabilities to system administrator access (Identification, Authentication and Monitoring). Management of system administrator-level vulnerabilities are tied to the reputational risk to the service vendor.

Isolation

In the absence of having unauthorized access to Identification and Authentication credentials, attempts may be made to circumvent access controls (typically through software vulnerabilities and/ or social engineering attacks), so that possession of such credentials is not required to achieve unauthorized access to data. Management of access control-circumvention vulnerabilities are tied to the reputational risk to the service vendor.

Continuity

Loss of access to data may be temporary or permanent, depending on the vulnerability exploited. Management of continuity-level vulnerabilities are tied to the reputational risk of the service vendor.

Monitoring

Failure to monitor system and user activity severely limits the ability to trace / detect unauthorized service use, or attempts to circumvent access controls. Both Microsoft's and Google's solutions offer the University of Windsor the ability to provide its own activity monitoring, which is a requirement of the completed service architecture.

7. Risk Mitigation and Management:

This section lists the significant risk factors (from above) and the strategies for mitigating or managing those risks. First, the mitigation and management measures that are common to a number of risks are explained,

- **Common FIPPA Practices** – the vendor is aware of and will use privacy policies and practices consistent with the FIPPA Act (See Appendix A – List of Policies).
- **Information Security Policies and Procedures** – the vendor's practices and procedures must be consistent with existing University of Windsor policies and procedures that speak to the security of information as well as those policies and procedures under development (See Appendix A – List of Policies).
- **Experienced Organizations** – the project contractor is experienced in working with the protection of personal information and sensitive information and records and has well established privacy policies.
- **Experienced staff** – both the University and the vendors have staff experienced in the collection, use, disclosure and protection of personal information and the secure management of other records. University staff is well versed in the requirements of FIPPA while Vendor's staff are equally well versed in the provisions of American privacy legislation as well as the Vendor's Privacy Policy.
- **Corporate IT Infrastructure** – The Vendor is experienced in providing, monitoring, backup and recovery, and defences from attack.
- **The Vendor's Information Security Architecture, Operations and Controls** – Google's provides a white paper report identifying its commitment and strategy for ensuring its customer's data is "safe, secure and private".[3] The white paper states that Google invest billions of dollars to "ensure the most secure, reliable environment for data and applications". Google attracts and recruits some of the top information and technical security expertise. Google focuses on several key security domains in safeguarding customer information:
    - Organizational and Operational Security – Policies and procedures to ensure security at every phase of design, deployment and ongoing operations.

[3] Google Inc., *Comprehensive review of security and vulnerability protections for Google Apps, February 2007.*

        - Development Security
        - Operational Security
        - Security communities and Advisories
    - Data Security – Ensuring customer data is stored in secure facilities, on secure servers, and within secure applications.
        - Physical Security
        - Logical Security
        - Information Accessibility
        - Redundancy
    - Threat Evasion – Protecting users and their information from malicious attacks and would-be hackers.
        - Spam and Virus Protection
        - Application and Network Attacks
    - Safe Access – Ensuring that only authorized users can access data, and the access channel is secure.
        - End User Protections
        - Customer Managed Security Controls
    - Data Privacy – Ensuring that confidential information is kept private and confidential
- **Secure messaging infrastructure** – Messages and transmission of University personal information and records between the Vendor and the University of Windsor are encrypted messages and travel through an encrypted tunnel over public networks. The industry standard is secure transmission protocol Secure Socket Layer (SSL version 3) which protects data and transmissions from eavesdropping and compromise while in transit over the internet. The banking and financial industries also use SSL as one of the means to secure data transmissions during online banking transactions.
- **The Vendor will collect no new personal information beyond that which has been collected and provided to the Vendor under appropriate authorizations and protocols of the University**. Accounts will be established for authorized University users of the Vendor's services of email and calendaring using the Identity Management protocols and processes of the University, and the transmission or sharing of credential information, for which the online web application authentication protocol Shibboleth is used.

  Shibboleth is an open source online application authentication standard, and does not require the transmission or sharing of credential password information. It enables external partner web services (such as the Vendor) to make informed

authorization decisions for individual access of protected online resources in a privacy-preserving manner.[4] For all sessions involving connecting to the U of W email service through a web browser, the connection request is redirected from the Vendor to the U of W's IMS Identity Management System (IMS). Therefore, for web based sessions, all authentication is conducted by the U of W's existing authentication service and credential repository. For all sessions involving connecting without a web browser, such as through a handheld PDA or smartphone, these involve the remote email service protocols IMAP and POP. In these IMAP and POP cases, the user is authenticated directly at The Vendor through a one-way encrypted hash the U of W provides. Through a secure VPN connection between the U of W and The Vendor, a one-way encrypted hash needed for authentication is transmitted to The Vendor from the U of W's Identity and Access Management system. The one-way encrypted hash is provided with an initial account setup, updated when credential information is changed and with de-provisioning of accounts. Password and credential changes can only occur through the U of W's centrally managed password service (a component of the IMS), and weak or known vulnerable passwords (such as the name of our city or sports teams) are immediately flagged and disallowed. Other password issues are also flagged by the password service, such as inactivity or a high number of unsuccessful login attempts.

- **Any personal information collected through the use of or application of tools available through The Vendor will be done under the authority of the University of Windsor and within the requirements of the FIPPA.** The contract will limit access to and use of this information to the purposes and staff of the University ensuring control over the information by the University.
- **Users will be expired in an orderly fashion upon termination of association with the University to avoid proliferation of accounts.**
- **Secure physical workspaces** – all the Vendor's employees and contractors work in office environments that are physically secure.
- **Online access controlled** – all employees and contractors at The Vendor's and the University of Windsor have online accounts protected by online access controls including sign-on passwords and need-to-know access restrictions.
- **Privacy policies and guidelines** – through the agreement for services all organizations , including The Vendor's will be deemed to be governed by the FIPPA.

[4] Internet2. *About Shibboleth. http://shibboleth.internet2.edu/about.html. October 1, 2009*

- **Training** – employees / contractors at The Vendor's are trained in the relevant aspects of:
  - FIPPA;
  - Records Management; and
  - Information Security.
- **Contractual obligations** – the contract with The Vendor's will address those items recommended in the *Guide to Managing Contracts under the FIPPA.*
- **Contractors are bound by confidentiality agreements that meet the standards set by the University.**
- **Audits** – Industry Standard Audits (SAS70 Type 2) will be performed regularly and be provided to the University to confirm procedures for physical security, systems security, and privacy practices are in place and followed. Clauses to this effect have been included in the contract with The Vendor's
- **Threat and Risk Analysis** – a Threat and Risk Analysis will need to be performed from end-to-end on the integrated systems on a regular basis by the Office of the Executive Director, Information Technology Services (ITS) in conjunction with the Information and Privacy Office. The rights for the University to assess and review the performance of The Vendor and the industry standard audits of The Vendor will be explicitly stated in the contract.

8. Exit Options:

Exit options need to be considered on two different planes.

Users of an outsourced University system, who do not want to receive email on this system, need to have a method for identifying that they do not want to receive private information through email. Such students may register with the Registrar's office.

The University needs to have an exit strategy should they decide that they want to stop using the outsourced email service. Both Google and Microsoft have indicated technology exists which would allow the University to move email off their systems in a timely manner.

9. University of Windsor policies affected by project

The University has two policies that are relevant to student email. They are the "University of Windsor Policy Concerning the Use of E-mail as an Official Means of Electronic Communication with Students" (Student email policy - Appendix B) and the "Acceptable Use Policy" (AUP - Appendix C)

No change is required of either policy. However, consideration needs to be given to students who do not agree to use email as a communication device, as is allowed in the "University of Windsor Policy Concerning the Use of E-mail as an Official Means of Electronic Communication with Students". The recommendation is that students who do not want to use email register at the Registrar's Office.

10. Recommendations:

Both vendors are subject to the US PATRIOT Act, however it is not clear, given reciprocal law-enforcement agreements between the United States and Canada, that hosting student email outside of Canada to greater risk than at present. Anne Cavoukian, the information and privacy commissioner of Ontario says this about Lakehead University moving their service to Google Apps for Education:

> "Schools shouldn't let the Patriot Act get in the way of outsourcing data hosting services to American companies ...there's no problem with Lakehead outsourcing to Google so long as they did their due diligence on the contractual agreement made regarding usage of the data.[5]

The provision of web-based services is a large part of the business model for both firms. Thus both firms devote considerable attention to security and offer strict auditing. As such, the risk of unauthorized access due to technical ot procedural vulnerabilities are not higher than at present.

Each platform offers sufficient functionality to satisfy the core requiremetns of the University of Windsor's intention to provide secure, reliable email to students. Provided the University can negotiate a contract that protects the University's interests in privacy, security and auditing as outlined in this document, the recommendation is to move forward with either of the vendors. Thus the decision on which vendor to partner with should be based on technical functionality for the University and the anticipated business relationship between the University of Windsor and the vendor.

[5] http://www.itbusiness.ca/it/client/en/home/News.asp?id=50660&PageMem=2 (May 5, 2011)

Appendix A

Associated Policies with Student Email and Cloud Computing

The following policies have been identified to impact student email:

- University of Windsor Policy Concerning the Use of E-mail as an Official Means of Electronic Communication with Students (http://www.uwindsor.ca/its/sites/uwindsor.ca.its/files/Student Email policy october 6 version.pdf)
- Acceptable Use Policy (http://www.uwindsor.ca/its/acceptable-use-policy)

Appendix B

University of Windsor Policy Concerning the Use of E-mail as an Official Means of Electronic Communication with Students

Support of the Policy

- If you need to Activate your UWin ID, reset a forgotten password or remember your UWin ID, you need to go to the UWin Account page by clicking here.
- **July 3, 2007** - The University plans to raise the disk quota allocated to students in the summer of 2007. The implementation of higher disk quotas is dependent on the installation of new Storage Area Network in IT Services. As of the start of July, the new SAN is in and is installed. New disk space will be allocated to the Student email system the week of July 23. Increased quotas for students is currently planned for completion by July 30, 2007.
- **July 30, 2007** - On Sunday, July 29th, the Student Webmail System was upgraded with new configurations. The student accounts now have the following quotas:

Max Account Size (email quota)	100 Meg
Max Web size (web quota)	20 Meg
Max Web Files (number of files for web page)	500
Maximum Message Size (single email with attachment)	10 Meg

Policy

Last Date Modified: October 6, 2006

1. **When conducting official University business, electronic communication from the University will be delivered to a student's University of Windsor (UWin) e-mail address.**
2. **All official electronic communication from the University will be deemed to have been delivered when it arrives at a student's UWin e-mail address.**
3. **Students must use their UWin e-mail account when electronically communicating (including corresponding with faculty and staff) with the University.**

Guidelines

1. Upon registering at the University of Windsor, each student is assigned a University of Windsor e-mail address. This system is referred to as the UWin E-Mail System. Students have the following responsibilities:

1.1 Activate their UWin e-mail address at www.uwindsor.ca/uwinid. Students should do this before the time that they register for any courses at the University.
1.2 This policy will pertain to all students who have registered for their first course at the University.
1.3 Ensure that time-critical e-mail is accessed, read and acted upon in a timely fashion.
1.4 Keep their e-mail box size within the appropriate limits to ensure delivery of e-mail.

1.5 Use their UWin e-mail address when corresponding with the University to ensure that the receiving party can appropriately identify the sending party.

2. All faculty and staff will communicate with students through their UWin e-mail address.

Rationale

1. Single E-Mail Communication Channel - The University of Windsor recognizes the need for timely and efficient communication between current students, faculty and staff. This policy clearly establishes a single e-mail communication channel to help reach this goal.

2. Privacy of Electronic Communication between the University and Students - The University of Windsor takes seriously its responsibility to interact with students in a secure manner that protects their privacy. The only effective way to maximize the probability that e-mail between the University and students remains private is to communicate through the UWin system.

3. Protection of Identity – using the UWin e-mail system maximizes the authenticity of a sender's identity when communicating electronically. Using the UWin e-mail system for corresponding with students, faculty and staff means that the receiver of the e-mail has reasonable assurance that the sender of the e-mail is the signing party.

Implications of the Policy

1. The UWin E-Mail System - The University has a responsibility to provide students with a secure, managed, highly-available e-mail system with appropriate disk space and response time for them to carry out their electronic correspondence.

2. Sending E-Mail to the University community – Students using email to conduct official business with the University, including communicating with faculty, are expected to use their UWin address. E-Mails received from students using the UWin system will be treated as legitimate.

3. Acceptable Use and Confidentiality of Passwords - Students must treat passwords with the security and respect that they require. Students are expected to follow the Campus Acceptable Use Policy (www.uwindsor.ca/aup), which they accept when activating their UWin ID. It is recommended that students do not use automatic login features at any PC that they use.

*4. **Forwarding of E-Mail from the UWin System*** - Students may forward their e-mail to another e-mail address. This functionality is available inside the UWin system. Students should understand however that when doing this, there is an increase in the risk that the e-mail will not remain private.

Consequences of not using the UWin account – Students may miss key information or possible deadlines if they do not read their e-mail from the University of Windsor. Students who do not use their UWin account for corresponding with the University will be deemed to have not responded. In situations where a student does not have access to a computer, the university may make alternate arrangements, upon receipt of a request from the student.

Timing of the Policy

The policy will become effective on January 1, 2007.

Contact for the Policy

IT Steering Committee may be contacted for questions or clarifications of the policy. Inquiries may be made to the office of the Executive Director of IT Services.

Appendix C

University of Windsor Acceptable Use Policy

The intent of this acceptable use policy is to provide rational guidelines for the appropriate use of the University of Windsor's computing and networking facilities, including both hardware and software. The policy recognizes that deliberate, malicious use of these facilities has been, and will likely continue to be, rare. The policy further assumes an attitude of cooperation, goodwill, and appropriate network "etiquette" on the part of university faculty, staff and students using our central facilities. The approach is therefore one of broad guidance rather than restrictive control.

The dynamic growth of networking, both on campus and around the world, raises some specific concerns regarding the nature of interpersonal and inter-institutional communication over the network. Issues of copyright, censorship, legal liability, and others , have not been resolved to the point where a universal approach to any one issue has been adopted. As debate over those issues continues, common sense is the most pragmatic approach to defining acceptable use of our own networking services.

General Principles

1. The issued userid is for YOUR PERSONAL USE ONLY.
2. The computing and networking facilities of the University of Windsor support instructional, research, public service, and other intellectual pursuits by students, faculty and staff that are consistent with the university's mission.
3. Since campus network services enable open scholarly communication on a world-wide basis, they are subject to the acceptable use guidelines established by regional and national networks (e.g. Onet and the Internet). Individuals who make use of these external networks should familiarize themselves with the applicable guidelines, copies of which are available from Information Technology Services.
4. Anyone using an external network, or an administrative system, requires a unique ID and password.
5. The holder of a computer ID and password is responsible for protecting campus computing facilities from unauthorized access by keeping the password confidential and by changing it regularly.

Acceptable Use

Generally, any computing or network communication activities which fall within these general principles are considered acceptable use of campus computing and networking facilities.

Unacceptable Use

Confirmed incidents of unacceptable use will result in sanctions ranging from verbal warnings, to revocation of computing privileges, to expulsion, and criminal prosecution. Unacceptable uses include:

1. Uses that violate federal or provincial laws, or university bylaws and policies such as those concerning information confidentiality.
2. Any uses that unduly interfere with the work of others or with the work of host systems. This includes, but is not limited to: unauthorized use of a computer ID or password; seeking information about or attempting to modify the University's computer security system; and knowingly propagating computer viruses or electronic chain letters.
3. Unauthorized copying of proprietary software, publications or files.
4. Uses of commercial software that in any way violate the applicable licensing agreement.
5. Uses related to commercial activities including, but not limited to, distribution of advertising material, offering network information or services for sale or personal gain, and private enterprises.
6. Computer information that portrays either men or women or their body parts in a pornographic or derogatory manner.