University of Guelph

Threat Risk Assessment (TRA) for the Student Email Initiative

January 2014
DRAFT

CONFIDENTIAL – NOT FOR DISTRIBUTION

Disclaimer

This Threat and Risk Assessment (TRA), conducted by Deloitte LLP, analyzes the security issues related to the transition of student email and calendaring solutions at the University of Guelph from the current email system to the Google Apps for Education suite. This TRA analyzes the security implications relating to the policies, procedures and system controls in place or planned for the email transition initiative. This TRA is intended to provide policy and strategic planning advice concerning the policies and management practices of University of Guelph and Google and to serve as an educational tool for senior management and Staff. This TRA relies on information provided by the University of Guelph project team and does not constitute an audit or assurance engagement as described in the professional standards issued by the Chartered Professional Accountants of Canada (CPA Canada). Furthermore, the findings and recommendations within this TRA are not a legal opinion or other form of assurance or legal advice with respect to University of Guelph's legal compliance with applicable legislation, best practices or information security standards. Legal compliance remains the responsibility of University of Guelph.

The content of this TRA is subject to change pending stakeholder validation.

Table of contents

1 Executive summary

1.1 Overview

The University, located in Guelph, Ontario, is one of Ontario's top rated comprehensive universities. The University has about 23,000 students and 7 faculties/colleges, and provides 12 degree programs, with primary focus on health, food, the environment and community. In addition to on campus courses and programs, the University provides distance education and remote learning.

The University is planning an initiative that will transition Undergraduate students to the Google Apps for Education email and calendaring suite from the existing Gryph Mail system. The initiative will move all email and calendaring tools for students into a cloud environment. The goal of the initiative is primarily to enhance student experience, but has the added benefit of achieving cost optimizations in operating and capital expenses, improving efficiencies, and enabling business continuity for those services. Contract negotiations with Google are currently underway, and project implementation that was initially expected to be completed in stages starting in fall 2013 and ending in spring/summer 2014 is currently planned to be completed by fall 2014.

1.2 Project objective and scope

The objective of the Threat and Risk Assessment (TRA) is to evaluate the threats and risks to the University and to student information and systems that will be operated in conjunction with Google Apps for Education email and calendaring. The TRA is intended to identify security risks and provide recommendations to mitigate or reduce the risks to levels acceptable to the University. The TRA process looks at the security and process controls in place, risk scenarios, and the threats posed by internal and external agents. This information is evaluated to determine risks and recommend activities/controls to reduce or mitigate identified risks.

1.3 Approach

Deloitte interviewed key personnel and reviewed relevant documentation to understand business processes and the underlying systems architecture that will be operating in conjunction with Google Apps for Education email and calendaring. The TRA was conducted in accordance with the Harmonized Threat and Risk Assessment (HTRA) methodology jointly developed by the Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment Canada (CSEC).

The TRA included the following steps:

- An analysis of the sensitivity of critical assets related to their confidentiality, availability and integrity (refer to Section 3).
- A threat assessment (refer to Section 4) to rate the threats that might reasonably occur either deliberately or accidentally taking a number of parameters into consideration such as assets, system architecture, location, history and open source data. The resulting assessment considered internal threats that were largely accidental, and to a lesser extent deliberate.
- Identification of existing safeguards and vulnerabilities (refer to Section 5). Certain vulnerabilities were identified and taken into consideration to formulate risk scenarios based on an assessment of existing safeguards (in relation to threats as identified in Section 4 and the sensitivity of the assets as identified in Section 3). Risk scenarios are provided in Section 6.
- Risk and recommendations to mitigate the identified risks were identified based on the assessment steps outlined above and are identified in Section 6.

1.4 Areas of identified risk

The goal of security risk management is to maintain security risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms. The table below summarizes the security risks identified through the TRA process, and categorizes levels of risk from low to high. Risk is determined by the value of the asset, threat likelihood and impact, and the vulnerabilities and safeguards in place. The goal of security risk management is to maintain security risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms. Criteria for ranking are set as follows:

- **Low:** There is a remote possibility that the risk will materialize and/or the impact of the risk is minor.
- **Moderate:** The possibility of the risk materializing is very low although the impact of such a risk is high, OR the possibility of the risk materializing is high but the impact of such a risk is minor, OR the impact and likelihood of the risk occurring are both determined to be moderate.
- **High:** There is a high probability that the risk will materialize if no corrective measures are taken and the impact of the risk is high.

The student information that the University handles has medium confidentiality and integrity ratings. Handling assets with medium ratings require a certain level of safeguards to provide a low risk of compromise. The University has safeguards in place; however, vulnerabilities exist which increase the risk level. The University is currently operating in a Medium risk range but this can be mitigated to Low.

Risk scenario	Title	Current Risk	Targeted residual Risk
1	Cisco IronPort Mail Gateway Misconfiguration/Misdirection	High	Low
2	Compromise of the Cisco IronPort Mail Gateway	High	Low
3	Exploitation of passwords/password compromise and opportunity for unauthorized access to email	Moderate	Low
4	Compromise of Google security	Moderate	Low
5	Potential challenges with email security monitoring and compromise detection	High	Low
6	Centrally enforced email security settings vs. end-user security settings	Moderate	Low

1.5 Recommendations

The following seven (7) recommendations are made to remediate the risk to the University. Many of these recommendations are already planned activities by the University, as noted in the recommendations.

Recommendation #1: Implement well documented processes (and automated processes if possible) to handle provisioning, modification and de-provisioning of email accounts to reduce the likelihood of email gateway misconfiguration.

Recommendation #2: The University should incorporate a process to ensure there is central monitoring of system, network and application logs to help detect any misdirection/misconfiguration issues relating to the IronPort so they can be rectified in a timely manner. Security Incident and Event Management (SIEM) systems should be considered as part of this to enable automated correlation and alerting of events and reduced manual monitoring of data.

Recommendation #3: The University should implement regular vulnerability testing on externally facing systems such as the IronPort as verification that all known vulnerabilities are patched or otherwise mitigated for these systems.

Recommendation #4: At a minimum, there should be a requirement to enforce both the use of alphanumeric passwords and enforcing regular password changes.

Recommendation #5: The University should insist that Google include contract provisions on how security incidents should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.

Recommendation #6: The University should insist that Google include contract provisions on how the monitoring and detection of compromised email accounts should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.

Recommendation #7: The University should work with Google to ensure that centrally set email security settings cannot be overridden by end users/students.

1.6 Next steps

University management needs to make an executive decision that weighs business requirements against security recommendations specified in this report. Options that are available to manage the current risks include:

- Transfer the risk to Google or others;
- Avoidance of the risk by adjusting scope, processes, etc.;
- Acceptance of the risk; or
- Risk reduction through proactive risk mitigation activities.

This report is focused upon facilitating the risk reduction option through the recommendations for risk reduction summarized in Section 6 in this report. This table also offers relative costs to reducing the current risks associated with the Google Apps for Education email and calendaring initiative. Recommendations are also prioritized as being high, moderate, or low.

The TRA is a point-in-time assessment as of the date of this report, and information collected from documentation and interviews represents an accurate depiction of the University and the Google Apps for Education email and calendaring initiative. The University will assume ultimately responsibility for the completion of remediation activities identified through the deliverables.

2 Overview of Solution Architecture

2.1 Overview of Current Email System

Gryph Mail is the University's integrated collaboration suite. Gryph mail features email, calendars, address books, document editing tools, and file storage (briefcase), all accessible from a web browser. Gryph Mail is built on Zimbra, a leading open source messaging and collaboration platform.[1] All students are issued a University of Guelph email address upon admissions/registration to the University. As per the University Calendar (Graduate and Undergraduate), email is considered the primary mode of communication between Faculty / Administration and the student. The Introduction section of the calendar states that "*The University issued email address is considered an official means of communication with the student and will be used for correspondence from the University. Students are responsible for monitoring their University-issued email account regularly*". As such, students are not permitted to "opt-out" of the University provided email service (i.e., provide the University with a different email address). Moreover, the University considers the student calendar as a binding contract and thus, by extension, all correspondence with students via the University email accounts as official and binding as well.[2] All Staff, Faculty, students, employees, affiliates, and members of the University community can access Gryph Mail using their central login ID which can also be used to access other University services such as Internet, downloads, website publishing, computer labs and printers.

There are three ways Gryph Mail can be accessed:

- **Web Client:** The web client is the preferred method of accessing email, the calendar, address book and collaboration tools. The web client is accessed through a browser (Internet Explorer, Firefox, Chrome) by going to mail.uoguelph.ca. There is also a mobile web client that supports smaller screens on smartphones through the device's internet browser. This can be accessed at mail.uoguelph.ca/zimbra/m/zmain

- **ActiveSync/Exchange:** The University allows email clients (such as Outlook) and mobile devices (BlackBerry, Android, iPhone) to connect with Gryph Mail that have ActiveSync/Exchange connection capabilities. This method allows for access to email, calendaring, the address book and tasks.

- **IMAP (Internet Mail Access Protocol):** The University allows IMAP as another means for mail clients and mobile devices to connect to Gryph Mail. IMAP only facilitates mail delivery. To access calendaring and other functions, they will have to be set up separately.

- **POP (Post Office Protocol):** The University allows POP to be used for retrieving email but it is not recommended. POP can only receive mail and changes made to mail clients or mobile devices cannot be reflected in Gryph Mail. The University recommends to those who opt to use POP that they do not select "Remove messages from server" in their mail client as this will result in all emails being removed from the mail server and mail only being visible in the mail client using POP.

Gryph Mail also provides users with the option of using extensions, also known as Zimlets. These are like plugins which when installed provide additional functionality to email users. There are a few default

[1] Zimbra was sold by VMware to Telligent in July 2013, post which Zimbra and Telligent merged into a single company under the Zimbra brand.
[2] Per information gathering meetings with the Chief Privacy Officer and the Office of the Registrar. December 16, 2013.

Zimlets that ship with Zimbra and some more have been developed by the University's Computing and Communication Services for enhanced utility. For a list of available extensions refer to Figure 1 below:

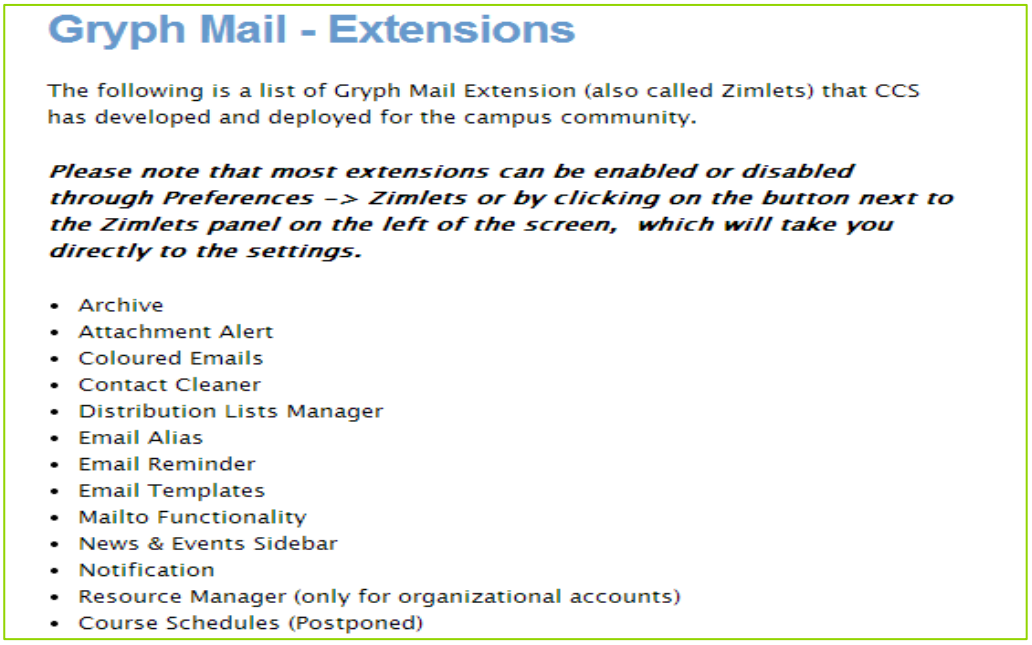

Figure 1: Gryph Mail Extensions

In addition to the Zimbra email suite used for Gryph Mail, the University uses Cisco's IronPort email security appliance. This system is the primary email gateway for the University from the outside world, and all email gets scanned for security risks on the IronPort. Once email has been validated by the IronPort appliance, it is relayed to the Gryph Mail system.

2.2 Proposed Email Solution

The University will be migrating its email service for all Undergraduate students by the fall of 2014 from the current Zimbra platform to the Google hosted email service, Google Apps for Education. Google Apps for Education is a suite of hosted email (e.g. Gmail) and collaboration applications that integrate with Google Docs and Google Calendar that enables a seamless user experience in a University setting. Since this is cloud based service based on the Software-as-a-Service (SaaS) model, it allows users access to their emails through any device with internet access. Google stores and processes all user data in its data centres around the world and takes care of all the backend IT maintenance activities for the service such as software updates, hardware upgrades, maintenance, and security.

All Faculty, Staff and Graduate students will remain on the Zimbra system. Although the University has selected Google Apps for Education, the configuration specifications and division of responsibilities between the University and Google are yet to be finalized. The use of Google as a service provider will include the cross-border transfer of the University data, as stated in the Google contract, [3] data will be processed in the "United States or any other country".

The University has planned to transition all Undergraduate student accounts to the Google Apps service while Faculty, Staff and Graduate student accounts will continue to use Gryph Mail for email and calendaring. Once deployed, all Undergraduate students will receive their new Guelph emails, hosted by Google, and will not be permitted to opt-out of the University email. Rather, as is the case under the

[3] Google Apps for Education Agreement, Section 1.1 – "*As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data*"

current email system, students will be permitted to forward their Guelph email to another email service. As described above, the University uses the University issued email accounts as the primary mode of communications with students and will respond only to the student's Guelph email even if the student sends an email from any other account.

Although students can forward their email received in their Guelph email account to another email account the University will always use the University issued email to correspond with the student. However, if the student responds to an email from the University using another email account, the University will still only respond to the student's Guelph email.

As the separation of Staff / Faculty and student email system requires the ability to properly route email between the existing Zimbra solution (Staff/Faculty/Graduate students) and the Google email system (Undergraduate students), a method of routing email is required that will ensure email for users that exist gets delivered to the user at the correct system, and that email for non-existent users is properly handled. At the time of this assessment, two separate methods were being considered:

- Routing of email based on username. For this method, all email is addressed to user@uoguelph.ca, and the Internet facing mail gateway performs a lookup to determine the correct email routing. This routing method is shown in Figure 2 below.
- Routing of email based on domain. For this method, a second DNS domain is added (for example, student.uofguelph.ca), and email is routed by the gateway based on the domain. In this example, user@uoguelph.ca is routed to the Zimbra system, user@student.uoguelph.ca is routed to the Google email system. This routing method is shown in Figure 3 below.

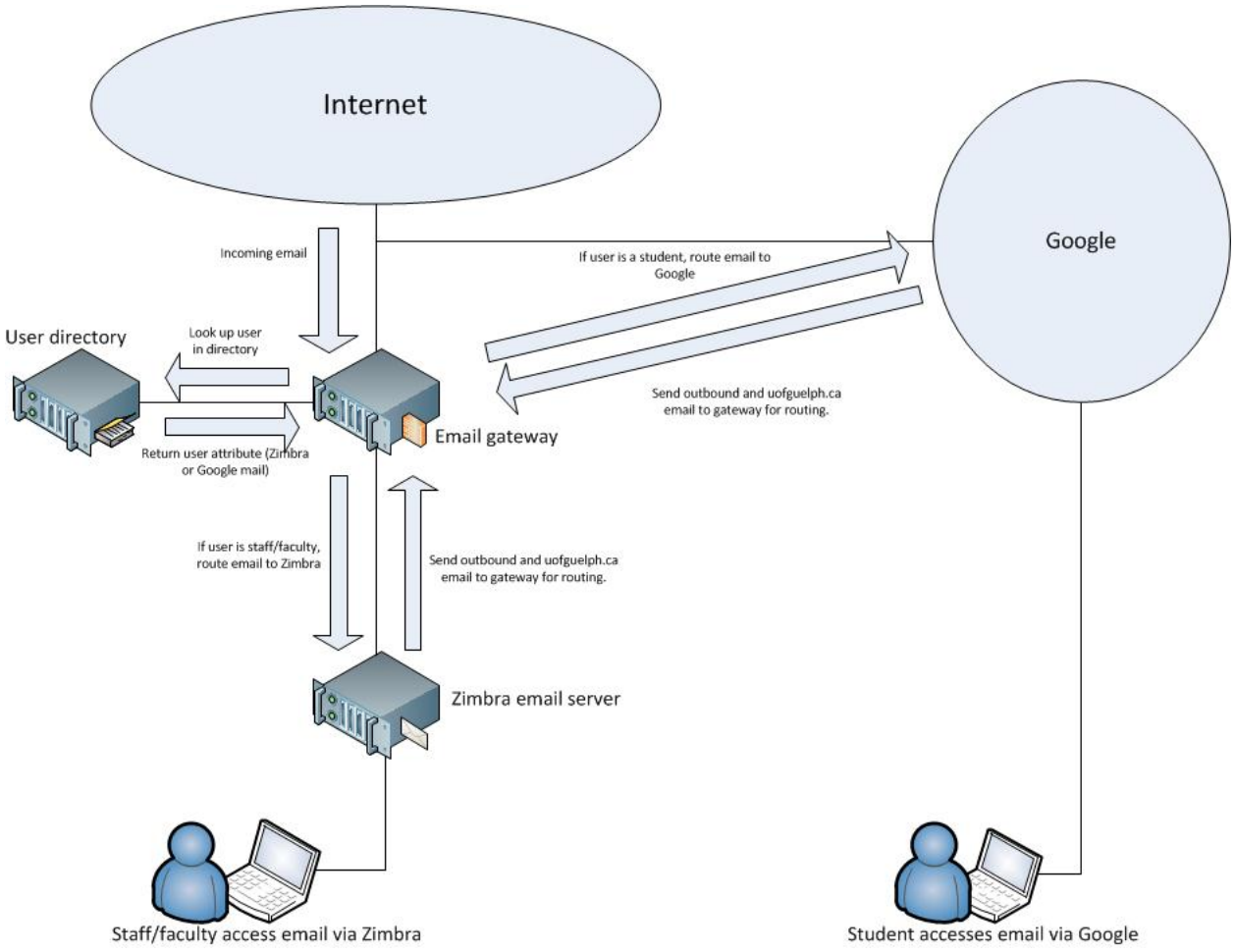

Figure 2: Conceptual Overview of Single Domain Email Solution

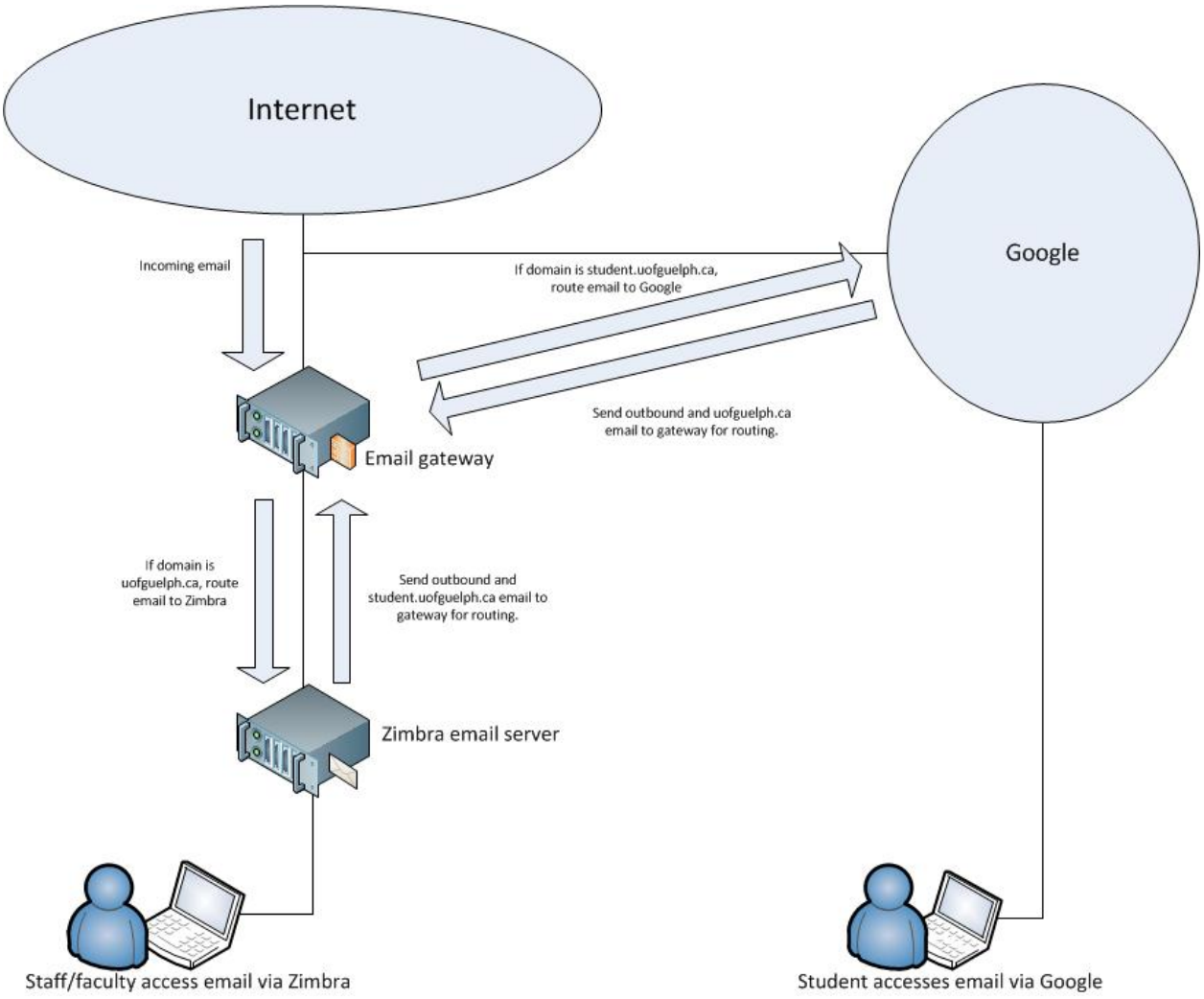

Figure 3: Conceptual Overview of Dual Domain Email Solution

2.3 Safeguards and controls provided by the University

The University provides several safeguards for the current email system and the campus network as a whole. These safeguards include the following:

Network firewalls
Network firewalls are in place to protect the campus network. Any threats or vulnerabilities identified are dealt with, either through updates or blocking malicious traffic as needed.

Email gateway
Cisco's IronPort email gateway security appliance is used by the University. All sent and received email gets scanned by the IronPort for security risks. Most email security risks can be handled by the IronPort, such as viruses, spam and phishing. Once email has been handled by the IronPort, email is relayed to the Gryph Mail system.

Taking into consideration the proposed options being contemplated for implementing Google Apps for Education email for students, all email will still go through the IronPort providing protection from viruses, spam and phishing.

Email gateway monitoring
University IT Security Staff, on a regular and periodic basis, monitor activity on the Cisco IronPort email gateway. If a security incident is detected, such as a compromised email account showing unusual activity, incident response procedures are followed to ensure the incident is properly handled and dealt with by the University.

2.4 Password settings

The Central ID is used not only to access email but also to access other University services, such as internet, computer labs and printers. The password standards for the Central ID are as follows[4]:

- *case-sensitive*
- *8 to 14 characters in length*
- *hard to guess by somebody else, but easy for user to remember so they don't have to write it down*
- *should not be a word that can be found in a dictionary of any language*
- *should include members of at least three groups of: capital letters, lower case letters, numbers, and simple punctuation or special characters such as $ ( ) ! + - _ . = { }*
- *please note that these characters are not allowed as they may be problematic for some applications: < > ' " ; , @ \ % & `*
- *should be changed regularly*

The initial password that is set during account creation is through a random password generator. There is no requirement that this password be changed during the first login or any subsequent logon and there is no enforcement of any password change requirement. It is important to note that the University's password policy and configuration requirements are designed in a manner that allows the passwords to be leveraged by both new and old systems deployed at the University. This means that many legacy systems may not be able to handle the strong password controls supported by newer systems.

For changing user passwords, the University's Computing and Communication Services (CCS) provides a free service called Password Insurance to anyone with a Central Login ID. Using Password Insurance, users can reset their passwords or retrieve forgotten passwords by answering a secret question at any time from any computer connected to the internet. For any queries or issues that cannot be handled by Password Insurance, users can contact the IT Help Desk for support and resolution.

Password Insurance can only be used to reset / retrieve passwords only if the user had previously subscribed to Password Insurance. Otherwise, the user has to get in touch with the IT help desk. For Undergraduate students who seek assistance from IT Help Desk for password resets, they will need to present or communicate their student identification number and be prepared to answer a series of questions to confirm their indemnity prior to having their password reset. Similarly, for Faculty, Staff and Graduate students that seek assistance from the IT Help Desk for password resets, they will need to present or communicate their identification number or contact an IT administrator / departmental contact assigned to them to have their password reset.

The Password Insurance home page with a link to retrieve password is shown in Figure 4:

[4] https://www.uoguelph.ca/ccs/apps/password/change/

Password Insurance

Password Insurance is a free service provided by CCS to anyone holding a Central Login Account that allows users to reset their own password at anytime, from any computer with an internet connection. Reduce the risk of being locked out of your account - if you ever lose your password, come back here and answer your secret question to retrieve your new password on the spot.

Log in to subscribe or change your settings for Password Insurance:

Central Login ID

Password

Sign in

Forgot your Password?

If you have previously subscribed to Password Insurance, retrieve your password here.

Figure 4: Change Password Webpage

The retrieve password page is shown in Figure 5:

Password Insurance

Get a new password

Note: you must already be subscribed to Password Insurance.

Enter your Central Login ID

Continue

Figure 5: Retrieve Password Webpage

The current password controls may not be sufficient to ensure appropriate security. Legacy systems prevent the University from setting strong password controls. Though the initial password that is set during account creation is through a random password generator, there is no requirement that this

password be changed during the first login or subsequently and there is no enforcement of any password change requirement. For the integration with Google, users will utilize their Central Login Account to access the Google application suite. Since, in this case the Identity Provider (IDP) and Service Provider (SP) are not in the same organization, a Federated Single Sign-On Solution is implemented. The University has implemented a Shibboleth Federated Single Sign-On[5] solution. The process is described in the Figure 6.

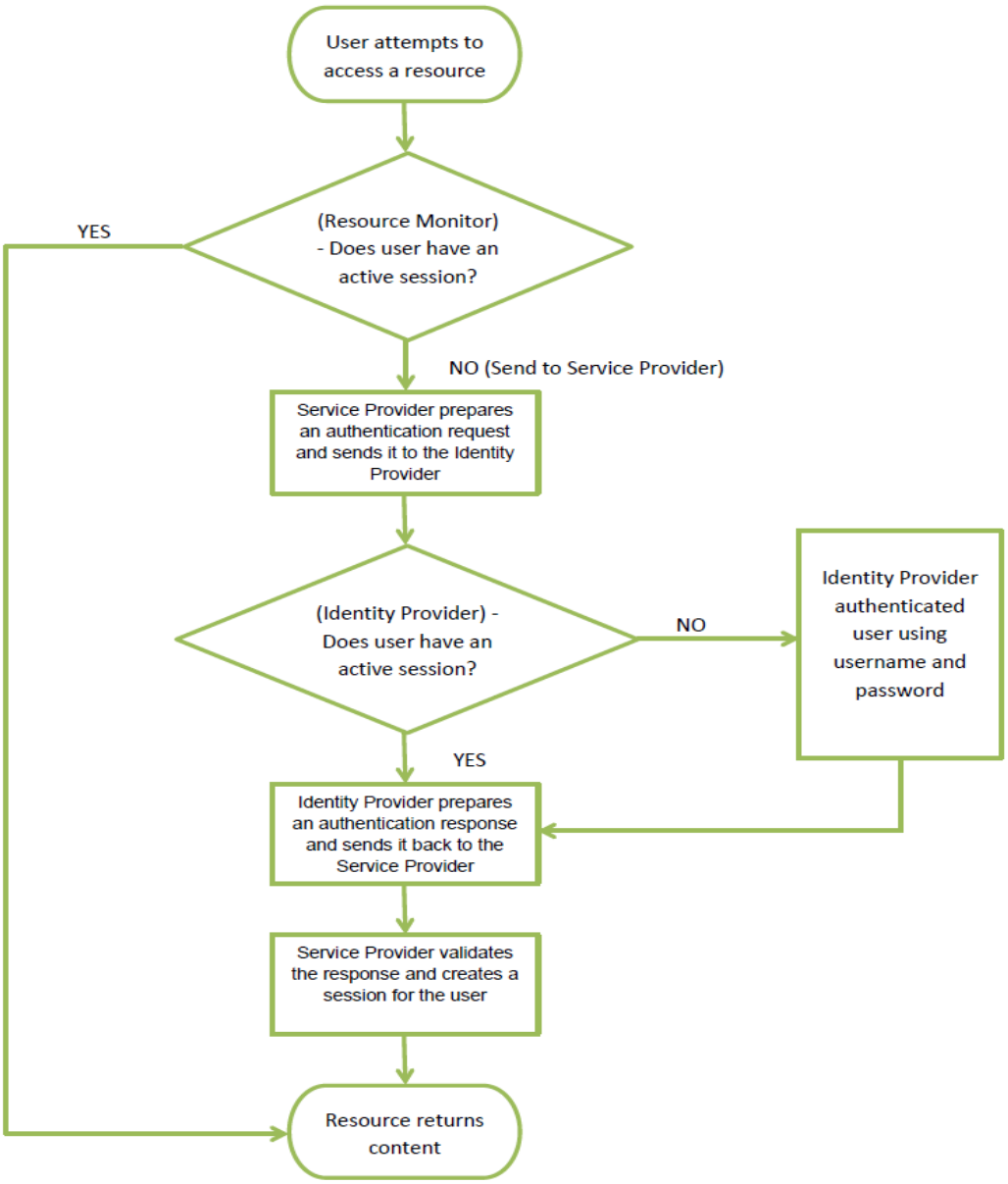

Figure 6: Single Sign-On Solution

In this configuration, users do not have a password within the Google system by default, and are redirected to the University of Guelph IDP server if they do not have a valid session when they connect to the Google application site. In this configuration, all user authentication is provided by the University, and there is a trusted session established between Google and the University to ensure that it is not possible to bypass the authentication system. However, direct access via IMAP or POP3, for example (such as

[5] http://shibboleth.net/about/basic.html

using the mail application in a mobile phone), require a user password to be set within Google to provide this access as SAML authentication is not supported. This can be done using the standard Google password settings, or by using a passkey generated by Google, similar to the process used for device access when using Google's two factor authentication (in this case, Google generates a 16 character passcode to be entered into the email client).

2.5 Safeguards and Controls provided by Google

The Google Apps for Education Agreement contains an exhibit titled Security Standards which details the security and safeguards that Google undertakes as part of the services it provides. This exhibit is summarized in the following sub-sections:

2.5.1 Physical Security

All data centres are equipped with a number of safety features to ensure proper protection. There is a round-the-clock security operation with Closed-circuit television (CCTV) monitoring and both internal and external patrol of the premises. Access is regulated through electronic key access and biometric access control systems and alarms are installed to detect any unauthorized access. Formal procedures are laid out for key card requests. All such requests have to be made through email and must be approved by the requestor's manager and data centre director. Only authorized Google employees, contractors and visitors are allowed to enter the data centre. Every electronic key card used is monitored and recorded each time perimeter doors, shipping and receiving and other critical areas are accessed. All unauthorized and failed access attempts are logged and investigated. Access authorization is restricted based on zones and an individual's job responsibilities. Fire doors at the data centre are equipped with alarms.

2.5.2 Network Security

All customer data is transferred through standard internet protocols and data centers are connected through high speed private links for fast and secure data transfer. Multiple layers of network devices and intrusion detection systems are used to protect Google's network and appropriate purpose built technologies are incorporated into external facing systems. Google's approach to intrusion detection and prevention involves tightly controlling the size and make-up of Google's attack surface through preventative measures, employing intelligent detection controls at data entry points and employing technologies that automatically remedy certain dangerous situations.

2.5.3 Logical Controls

Administrators and End Users must authenticate themselves through a central authentication system or through a customer's single sign-on (SSO) system in order to use the services. Each application checks credentials in order to allow the display of data to an authorized end user or authorized administrator. Internally, Google employs a centralized access management system to restrict personnel access to production servers and access is granted only to a limited number of authorized personnel. LDAP, Kerberos and a Google proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. Approvals are managed by workflow tools that maintain audit records of all changes. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. Where passwords are employed for authentication at Google (e.g., login to workstations), password policies are followed that employ industry standard practices. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., Credit Card data), Google uses hardware tokens.

2.5.4 Data Security Controls

Customer data is stored in a multi-tenant environment on Google-owned servers and replicated between geographically distributed data centres. Data of various end users is logically isolated at the application layer as well as on a per customer account basis. Disks containing customer data that are decommissioned (due to errors or hardware failure) are subject to a series of data destruction processes before being reused or destroyed. The data destruction process consists of a multi-step erase process

that is verified by at least two independent validators. The erase results are then logged by the disk's serial number. If the disk cannot be erased, then it is stored securely until it can be destroyed.

2.5.5 Other Controls

The infrastructure systems are designed to prevent single points of failure by incorporating measures such as dual circuits, switches and networks that help provide redundancy. Preventative and corrective maintenance of the data centre equipment is scheduled through a standard change process according to documented procedures. Data centres are provided with sufficient backup power mechanisms. Uninterruptible power supply (UPS) batteries can provide up to 10 minutes of power supply during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. The standby diesel generator can take over if backup power is required for a longer duration. Google servers use a Linux based implementation customized for the Google application environment and customer data is stored using Google proprietary algorithms to augment data security and redundancy.

3 Statement of sensitivity

The sensitivity analysis provides the foundation for the TRA. Assets with higher sensitivities typically require more safeguarding. Sensitivity ratings fall into three different categories:

- **Confidentiality:** Protection typically involves safeguarding sensitive data from being read by people without a need to know or appropriate security clearance;
- **Integrity:** Protection typically involves safeguarding data from unwanted changes; and
- **Availability:** Protection involves protecting assets to ensure there are no single points of failure and that they are available as and when required to support business objectives.

The following ratings were assessed herein and reflect the notable ratings encountered across all components and information under consideration for the Google Apps for Education email and calendaring initiative and related environments:

- **Confidentiality** was rated at **Medium.** While some sensitive information is sent and received via email, the risk of a disclosure of information is not likely to cause harm to individuals or damage to systems.
- **Integrity** was rated at **High.** The University considers email from students via their provided email account to be equivalent to a signed document for certain University business. As a result, it is important that information is not corrupted or modified.
- **Availability** was rated at **High.** Communications with students are primarily done via email, so it is important that the students are able to access email, and that the mail transport systems are available to transfer email between systems.

For further details concerning sensitivity ratings for people, processes, hardware, software and facilities please refer to **Appendix 3 – Sensitivity injury tables**.

4 Threat assessment

The threat landscape for the University has been derived from threats identified from interviews and documentation that has been provided by the University. This information was synthesized and taken into consideration for the University environment.

Accidental and Deliberate threats to the University, the Google Apps for Education email and calendaring initiative and related systems could include one or more of the following:

- Users (Faculty, Staff and Students)
- Administrators (System Administrators, Network Administrators, IT Security)
- Vendors (Google)

Deliberate threats to the University, the Google Apps for Education email and calendaring initiative and related systems could include the following:

- Hackers and criminals
- Third parties

For the most part, threats to the University email system could be considered similar to other organizations. One area where a higher threat exists with respect to students is the threat of “known attackers”, or other students, roommates, friends who may deliberately access student email by guessing the password or using a computer that has saved passwords to access email. For the Google solution, natural disasters are not considered a large threat because of the distributed nature of the Google platform and multiple access methods available to connect.

Threat rating tables were populated while taking into consideration the above threat landscape and are included in **Appendix 4 – Threat Agent Ratings.**

5 Vulnerabilities and safeguards

Vulnerabilities are "*an attribute of an asset or the environment in which it is located that increases the likelihood of a threat event, the probability of compromise, or the severity of the outcome. Vulnerabilities are inversely proportional to safeguard effectiveness*[6]."

Safeguards are "*assets or external controls that reduce overall risk to employees, other assets or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats or vulnerabilities*[7]."

A detailed identification of safeguards and vulnerabilities is provided in **Appendix 5 – Vulnerability Assessment Tables**. For the purposes of streamlining this assessment, safeguards and vulnerabilities were assessed in a cumulative manner based on the identified threats to assets.

The vulnerabilities and safeguards were considered in the context of the email and supporting environments, so are not an exhaustive list of all systems within the University. For the most part, vulnerabilities are centered around the policies and procedures in dealing with Google for administration of email, contract provisions with Google, and the security of the Cisco IronPort gateway and supporting systems, as the gateway is a critical component in the successful operation of the combined email solution.

An explanation of vulnerability ratings (based on the effectiveness of safeguards) are also detailed in Appendix 5 and were used in the development of risk scenarios in Section 6.3.

---

[6] As defined by the Harmonized Threat Risk Assessment (TRA) Methodology Handbook
[7] Ibid.

6 Risk assessment findings

6.1 Risk scenario summary

Based on the approach outlined above, the following risk scenarios were assessed at a moderate to high current risk level. Current risk is defined as the risk associated with the University's currently planned implementation of Google Apps for Education email, taking into consideration both existing safeguards and existing vulnerabilities. Targeted residual risk is the risk associated with the University if the mitigation measures identified in the TRA are implemented.

Risk scenario	Title	Current Risk	Targeted Residual Risk
1	Cisco IronPort Mail Gateway Misconfiguration/Misdirection	High	Low
2	Compromise of the Cisco IronPort Mail Gateway	High	Low
3	Exploitation of passwords/password compromise and opportunity for unauthorized access to email	Moderate	Low
4	Compromise of Google security	Moderate	Low
5	Potential challenges with email security monitoring and compromise detection	High	Low
6	Centrally enforced email security settings vs. end-user security settings	Medium	Low

6.2 Recommendations summary

The recommended mitigation measures to address the risks identified in the risk scenarios are summarized in the table below. The table includes a high-level indication of estimated effort associated with the recommendation activity. This High-Level Effort is identified as High, Moderate and Low (H,M,L).

- **High** effort items would typically require a project setting, involve a team of resources and span an elapsed time greater than a month (greater than 500 hours of effort). High ongoing effort would average greater than 20 hours of effort per week.

- **Moderate** effort items would typically require a smaller project setting involving the several team members over a period of one to four weeks (150-500 hours of effort). Moderate ongoing effort would average 10 to 20 hours of effort per week.

- **Low** effort items would typically not require a project setting, but could be accomplished by an individual, for example, the security administrator, or a very small team in less than a week (less than 150 hours of effort). Low ongoing effort would average less than than 10 hours of effort per week.

Note: the above descriptions should not be confused with the ranks assigned under the "relative priority" column.

Recommendations specific to the Google Apps for Education email and calendaring initiative

Relative Priority	Recommendation	Scenarios Mitigated	Level of Effort Notes
1	**Recommendation #1:** Implement well documented processes (and automated processes if possible) to handle provisioning, modification and de-provisioning of email accounts to reduce the likelihood of email gateway misconfiguration.	RS-1	**High** one-time effort to implement well documented/automated processes to handle provisioning, modification and de-provisioning of email accounts. **Low** ongoing effort to handle provisioning, modification and de-provisioning of email accounts if well documented processes are easily adhered to or automated processes are regularly inspected for effectiveness.
2	**Recommendation #2:** The University should incorporate a process to ensure there is central monitoring of system, network and application logs to help detect any misdirection/ misconfiguration issues relating to the IronPort so they can be rectified in a timely manner. Security Incident and Event Management (SIEM) systems should be considered as part of this to enable automated correlation and alerting of events and reduced manual monitoring of data.	RS-1 RS-2	**High** one-time effort to implement and centralize monitoring of system, network and applications logs and optionally implement SIEM. **Moderate** ongoing effort to monitor central logging of system, network and application activities, or **Low** for SIEM, as many manual processes can be automated.
3	**Recommendation #3:** The University should implement regular vulnerability testing on externally facing systems such as the IronPort as a verification that all know vulnerabilities are patched or otherwise mitigated for these systems.	RS-2	**Moderate** – Selection and implementation of a VA assessment tool or service, as well as training if implemented as a tool rather than an external service.
4	**Recommendation #4:** At a minimum, there should be a requirement to enforce both the use of alphanumeric passwords and enforcing regular password changes.	RS-3	**Low** one-time effort to implement alphanumeric and change requirements for password. **Low** ongoing effort to make any changes/adjustments to alphanumeric and change requirements for password.
5	**Recommendation #5:** The University should insist that Google include contract provisions on how security incidents should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.	RS-4	**High** one-time effort to draft and negotiate contract provisions to handle security incidents and associated processes. **Moderate** ongoing effort to monitor that contract provisions relating to handling security incidents and associated processes are adhered to.
6	**Recommendation #6:** The University should insist that Google include contract provisions on how the monitoring and detection of compromised email accounts should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.	RS-5	**High** one-time effort to draft and negotiate contract provisions to handle monitoring and detection of compromised email accounts and associated processes. **Moderate** ongoing effort to monitor that contract provisions relating to monitoring and detection of compromised email accounts and associated processes are adhered to.

Relative Priority	Recommendation	Scenarios Mitigated	Level of Effort Notes
7	**Recommendation #7**: The University should work with Google to ensure that centrally set email security settings cannot be overridden by end users/students.	RS-6	**High** one-time effort to work with Google to ensure that centrally set email security settings cannot be overridden by students. **Low** ongoing effort to monitor that email security settings cannot be overridden by students based on centrally set email security settings.

6.3 Risk scenario's

Risk scenario 1 – Cisco IronPort Mail Gateway Misconfiguration/Misdirection

Current Risk: High (36)

Assets affected: Students, email administrators, security processes, system configuration information, email data, Cisco IronPort Gateway, mail routing software (Cisco IronPort), Zimbra email system, Google Apps for Education - Gmail

Description of risk, vulnerability and impact: If the University decides to go with its single domain option, the IronPort gateway will have to be configured to look up every email address in the University LDAP directory. Required maintenance to ensure all active uoguelph.ca student mail addresses are in the directory with the correct email routing option set will be high. In addition, the IronPort will take on a significantly higher load for its involvement in mail routing and having to perform a lookup of every email address inbound and outbound, and all email from Google will need to be routed through the gateway as well. There is an increased risk of email being misrouted if uoguelph.ca mail addresses are not entered correctly in the LDAP directory. Misrouted email containing sensitive information going to the incorrect student could compromise confidentiality of student information.

.

Asset Rating (from Appendix 3): **High (4)**

Critical Asset ID	Critical Asset Name	Type	Confidentiality (C) / Integrity (I) / Availability (A)
CA-01	Students	People	C=High, I=N/A, A=N/A
CA-02	Email Administrators	People	C=N/A, I=N/A, A=H
CA-04	Security Processes	Processes	C=M, I=H, A=H
CA-06	System configuration information	Information	C=H, I=H, A=H
CA-07	Email data	Information	C=H, I=H, A=H
CA-10	Cisco IronPort Gateway	Hardware	C=L, I=H, A=H
CA-11	Mail routing software (Cisco IronPort)	Software	C=L, I=H, A=H
CA-12	Zimbra email system	Software	C=L, I=H, A=H
CA-13	Google Apps for Education email and calendaring suite	Software	C=L, I=H, A=H

Threat Rating (from Appendix 4): **Moderate (3)**

Threat Agent Identifier	Threat Agent Title	Type	Threat Impact/Gravity	Threat Likelihood

TA.02	Administrators	Accident	Moderate	Moderate
TA.05	Administrators	Deliberate	Moderate	Low
TA.07	Hackers & Criminals	Deliberate	High	Low

Vulnerability Rating (from Appendix 5): **Moderate (3)**

SG# / VN#	Safeguard / Vulnerability Description
SG-02	The Cisco IronPort mail gateway is used to secure email
SG-03	There is proactive monitoring of the Cisco IronPort mail gateway
VN-01	The Cisco IronPort mail gateway could be misconfigured increasing the risk that emails could be misdirected
VN-03	There is no central monitoring of logs, increasing the risk that malicious events could go undetected

Probability of Compromise	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex / Fragile/Portable
Severity of Outcome	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex/Fragile

Risk =		Asset Rating	X	Threat Rating X	Vulnerability Rating
	=	4		3	3
	=	**36**		**High**	

Recommendations

Recommendation #1: Implement well documented processes (and automated processes if possible) to handle provisioning, modification and de-provisioning of email accounts to reduce the likelihood of email gateway misconfiguration.

Recommendation #2: The University should incorporate a process to ensure there is central monitoring of system, network and application logs to help detect any misdirection/misconfiguration issues relating to the IronPort so they can be rectified in a timely manner. Security Incident and Event Management (SIEM) systems should be considered as part of this to enable automated correlation and alerting of events and reduced manual monitoring of data.

Targeted residual risk after recommendation is implemented: Low

Risk scenario 2 – Compromise of the Cisco IronPort Mail Gateway

Current Risk: High (36)

Assets affected: Email administrators, security processes, system configuration information, Cisco IronPort Gateway, mail routing software (Cisco IronPort).

Description of risk, vulnerability and impact: Based on Common Vulnerabilities and Exposures (CVE) and other compromised data, 4 data exploits were reported for the Cisco IronPort devices in 2013. Of these, 2 were denial of service vulnerabilities, and 2 were remote code execution vulnerabilities. Denial of service vulnerabilities affect the availability of the gateway, so would impact the ability of students using email to send and receive email outside of the Google infrastructure and could result in confusion (they could send/receive to other students, but emails to and from Staff or Faculty or emails to non-University email accounts would not go through as they are routed via the IronPort gateway). Remote code

execution would allow an attacker to change configuration of the gateway, obtain information about email users, and/or utilize the gateway to compromise internal systems.

.

Asset Rating (from Appendix 3): **High (4)**

Critical Asset ID	Critical Asset Name	Type	Confidentiality (C) / Integrity (I) / Availability (A)
CA-02	Email Administrators	People	C=N/A, I=N/A, A=H
CA-04	Security Processes	Processes	C=M, I=H, A=H
CA-06	System configuration information	Information	C=H, I=H, A=H
CA-10	Cisco IronPort Gateway	Hardware	C=L, I=H, A=H
CA-11	Mail routing software (Cisco IronPort)	Software	C=L, I=H, A=H

Threat Rating (from Appendix 4): **Moderate (3)**

Threat Agent Identifier	Threat Agent Title	Type	Threat Impact/Gravity	Threat Likelihood
TA.02	Administrators	Accident	Moderate	Moderate
TA.05	Administrators	Deliberate	Moderate	Low
TA.07	Hackers & Criminals	Deliberate	High	Low

Vulnerability Rating (from Appendix 5): **Medium (3)**

SG# / VN#	Safeguard / Vulnerability Description
SG-03	There is proactive monitoring of the Cisco IronPort mail gateway
VN-01	The Cisco IronPort mail gateway could be misconfigured increasing the risk that emails could be misdirected
VN-03	There is no central monitoring of logs, increasing the risk that malicious events could go undetected

Probability of Compromise	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex / Fragile/Portable
Severity of Outcome	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex/Fragile

Risk =		Asset Rating X	Threat Rating X	Vulnerability Rating
	=	4	3	3
	=	**36**	**High**	

Recommendations

Recommendation #2: The University should incorporate a process to ensure there is central monitoring of system, network and application logs to help detect any misdirection/misconfiguration issues relating to the IronPort so they can be rectified in a timely manner. Security Incident and Event Management (SIEM) systems should be considered as part of this to enable automated correlation and alerting of events and reduced manual monitoring of data.

Recommendation #3: The University should implement regular vulnerability testing on externally facing systems such as the IronPort as a verification that all know vulnerabilities are patched or otherwise mitigated for these systems.

Targeted residual risk after recommendation is implemented: Low

Risk scenario 3 – Exploitation of passwords/password compromise and opportunity for unauthorized access to email

Current Risk: Medium (24)

Assets affected: Email data, system user authentication credentials, Zimbra email system, Google Apps for Education email and calendaring suite.

Description of risk, vulnerability and impact: The University currently does not enforce password complexity for users. Users could use commonly used passwords (e.g., "password" or "admin"), default passwords (e.g., "Guest,", "1234," or blank passwords), consecutive numbers/letters or common keyboard sequences (e.g. "1111," 1234," or "qwerty"), or ones that are vulnerable to logical deduction based on knowledge about a user (e.g. names, birthdates, addresses, etc.). Similarly, there is no enforcement that initially set passwords are to be changed during the first login or subsequent logins and there is no enforcement of any password change requirement. Many legacy systems are used by the University and they cannot handle strong password controls. There is a risk that University user's credentials can be guessed by an attacker using manual or automated techniques, resulting in unauthorized access to University systems, such as email.

Asset Rating (from Appendix 3): **High (4)**

Critical Asset ID	Critical Asset Name	Type	Confidentiality (C) / Integrity (I) / Availability (A)
CA-07	Email data	Information	C=H, I=H, A=H
CA-08	System User Authentication Credentials	Information	C=H, I=H, A=H
CA-12	Zimbra email system	Software	C=L, I=H, A=H
CA-13	Google Apps for Education email and calendaring suite	Software	C=L, I=H, A=H

Threat Rating (from Appendix 4): **Moderate (3)**

Threat Agent Identifier	Threat Agent Title	Type	Threat Impact/Gravity	Threat Likelihood
TA.04	Users	Deliberate	Moderate	Low
TA.05	Administrators	Deliberate	Moderate	Low
TA.07	Hackers & Criminals	Deliberate	High	Low

Vulnerability Rating (from Appendix 5): **Low (2)**

SG# / VN#	Safeguard / Vulnerability Description
SG-01	Identity Management and Single Sign-On (SSO) is used to help authenticate users
VN-04	There is no enforcement of password complexity or change requirements

	Probability of Compromise	Moderate
	Safeguard effectiveness	Safeguard Moderately Effective
	Associated vulnerabilities	Assets Fairly Complex / Fragile/Portable
	Severity of Outcome	Moderate
	Safeguard effectiveness	Safeguard Moderately Effective
	Associated vulnerabilities	Assets Fairly Complex/Fragile

Risk =		Asset Rating	X	Threat Rating	X	Vulnerability Rating
	=	4		3		2
	=	**24**		**Medium**		

Recommendations

Recommendation #4: At a minimum, there should be a requirement to enforce both the use of alphanumeric passwords and enforcing regular password changes.

Targeted residual risk after recommendation is implemented: Low

Risk scenario 4 – Compromise of Google security

Current Risk: Medium (24)

Assets affected: Security processes, vendor processes, email data, user documents, Google Apps for Education email and calendaring suite, Google offsite premises/Data Centres.

Description of risk, vulnerability and impact: According to the Google Apps contract, Google provides access to a "console" application that can be used by the University to produce usage/licensing reports, but it was observed that mechanisms that would be available to the University, namely the Google Console and the Google Apps Status Dashboard, do not provide enough details to be used for security-related reports. Moreover, if a security incident has occurred or is expected to have occurred, the University must request an incident report from Google; Google does not actively provide such reports and there is no clarity on what processes Google will follow to report security incidents. There is also a lack of security reports that can be run to provide details such as number of viruses received in email attachments and number of security incidents. This reduces the University's ability to track and analyze the effectiveness of the Google Apps security controls. There is also increased risk that security incidents affecting Google Apps may go undetected if there are no security incident reporting processes.

Asset Rating (from Appendix 3): **High (4)**

Critical Asset ID	Critical Asset Name	Type	Confidentiality (C) / Integrity (I) / Availability (A)
CA-04	Security Processes	Processes	C=M, I=H, A=H
CA-05	Vendor Processes	Processes	C=M, I=H, A=H
CA-07	Email data	Information	C=H, I=H, A=H
CA-09	User documents	Information	C=H, I=H, A=H
CA-13	Google Apps for Education email and calendaring suite	Software	C=L, I=H, A=H
CA-15	Google offsite premises/Data Centres	Facility	C=L, I=H, A=H

Threat Rating (from Appendix 4): **Moderate (3)**

Threat Agent Identifier	Threat Agent Title	Type	Threat Impact/Gravity	Threat Likelihood
TA.03	Vendors	Accident	Moderate	Low
TA.06	Vendors	Deliberate	High	Low
TA.07	Hackers & Criminals	Deliberate	High	Low

Vulnerability Rating (from Appendix 5): **Low (2)**

SG# / VN#	Safeguard / Vulnerability Description
SG-01	Identity Management and Single Sign-On (SSO) is used to help authenticate users
SG-04	Contract provisions with Google are in place to protect the University
VN-02	The University has no control on confidential data that is stored outside its premises / by Google

Probability of Compromise	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex / Fragile/Portable
Severity of Outcome	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex/Fragile

Risk =		Asset Rating	X	Threat Rating	X	Vulnerability Rating
	=	4		3		2
	=	**24**		**Medium**		

Recommendations:

Recommendation #5: The University should insist that Google include contract provisions on how security incidents should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.

Targeted residual risk after recommendation is implemented: Low

Risk scenario 5 – Potential challenges with email security monitoring and compromise detection

Current Risk: High (36)

Assets affected: Email administrators, help desk processes, security processes, vendor processes, system configuration information, email data, Zimbra email system, Google Apps for Education email and calendaring suite.

Description of risk, vulnerability and impact: The University currently has the ability to monitor and detect Faculty, Staff and student email accounts that are compromised. There is concern that when Google Apps for Education email and calendaring suite is introduced for use by students, the University may no longer have the ability to monitor and detect compromised student email accounts. In addition, there is uncertainty if Google has a clear defined process to report compromised email accounts based on its monitoring and detection efforts.

.

Asset Rating (from Appendix 3): **High (4)**

Critical Asset ID	Critical Asset Name	Type	Confidentiality (C) / Integrity (I) / Availability (A)
CA-02	Email Administrators	People	C=N/A, I=N/A, A=H
CA-03	Help Desk Processes	Processes	C=M, I=H, A=H
CA-04	Security Processes	Processes	C=M, I=H, A=H
CA-05	Vendor Processes	Processes	C=M, I=H, A=H
CA-06	System configuration information	Information	C=H, I=H, A=H
CA-07	Email data	Information	C=H, I=H, A=H
CA-12	Zimbra email system	Software	C=L, I=H, A=H
CA-13	Google Apps for Education email and calendaring suite	Software	C=L, I=H, A=H

Threat Rating (from Appendix 4): **Moderate (3)**

Threat Agent Identifier	Threat Agent Title	Type	Threat Impact/Gravity	Threat Likelihood
TA.02	Administrators	Accident	Moderate	Moderate
TA.03	Vendors	Accident	Moderate	Low
TA.06	Administrators	Deliberate	Moderate	Low
TA.06	Vendors	Deliberate	High	Low
TA.07	Hackers & Criminals	Deliberate	High	Low

Vulnerability Rating (from Appendix 5): **Moderate (3)**

SG# / VN#	Safeguard / Vulnerability Description
SG-06	There is regular monitoring of email to detect security incidents/compromises
VN-06	There is no requirement for Google to report any email security incidents/compromises

Probability of Compromise	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex / Fragile/Portable
Severity of Outcome	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex/Fragile

Risk =		Asset Rating	X	Threat Rating X	Vulnerability Rating
	=	4		3	3
	=	**36**		**High**	

Recommendations:

Recommendation #6: The University should insist that Google include contract provisions on how the monitoring and detection of compromised email accounts should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.

Targeted residual risk after recommendation is implemented: Low

Risk scenario 6 – Centrally enforced email security settings vs. end-user security settings

Current Risk: Medium (24)

Assets affected: Students, email administrators, security processes, Google Apps for Education email and calendaring suite.

Description of risk, vulnerability and impact: There is currently uncertainty on what security settings can be centrally enforced once Google Apps for Education email and calendaring suite is introduced for students. The Google Apps administration console/interface has security settings that can be set. What is not clear at the moment is if these security settings can be centrally enforced on all student email accounts. There is also uncertainty if students may have the ability to override any centrally set security settings. The potential for inconsistent email security settings amongst students increases the risk that their email accounts could get compromised.

.

Asset Rating (from Appendix 3): **High (4)**

Critical Asset ID	Critical Asset Name	Type	Confidentiality (C) / Integrity (I) / Availability (A)
CA-01	Students	People	C=M/H, I=N/A. A=N/A
CA-02	Email Administrators	People	C=N/A, I=N/A, A=H
CA-04	Security Processes	Processes	C=M, I=H, A=H
CA-13	Google Apps for Education email and calendaring suite	Software	C=L, I=H, A=H

Threat Rating (from Appendix 4): **Moderate (3)**

Threat Agent Identifier	Threat Agent Title	Type	Threat Impact/Gravity	Threat Likelihood
TA.01	Users	Accident	Low	Low
TA.02	Administrators	Accident	Moderate	Moderate
TA.04	Users	Deliberate	Moderate	Low
TA.05	Administrators	Deliberate	Moderate	Low

Vulnerability Rating (from Appendix 5): **Low (2)**

SG# / VN#	Safeguard / Vulnerability Description
SG-07	This is central enforcement of critical email security settings
VN-07	End users have the ability to modify their email security settings

Probability of Compromise	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex / Fragile/Portable
Severity of Outcome	Moderate
Safeguard effectiveness	Safeguard Moderately Effective
Associated vulnerabilities	Assets Fairly Complex/Fragile

Risk =	Asset Rating	X	Threat Rating	X	Vulnerability Rating
=	4		3		2
=	**24**		**Medium**		

Recommendations:

CONFIDENTIAL – NOT FOR DISTRIBUTION

Recommendation #7: The University should work with Google to ensure that centrally set email security settings cannot be overridden by end users/students.

Targeted residual risk after recommendation is implemented: Low

Appendix 1 – TRA interview list

The following individuals participated in the information gathering sessions for the TRA:

Last	First	Area	Primary Role
Rasheed	Fazil	Project Manager for Student Email Initiative	Manager of Applications and Integration
Whiteside	Brenda	Student Services/Central Students Association	Associate Vice-President: Student Affairs
Thibodeau	Shannon	Student Services/Central Students Association	Leadership Education & Development (LEAD) Advisor, Student Life
Archibald	Chris	Student Services/Central Students Association	President, Students Association
Forrester	Julia	Student Services/Central Students Association	Member, Students Association
Graham	Rebecca	Senior IT	Chief Information Officer
Gray	Gayleen	Senior IT	Associate Director, IT Strategy and Partnerships
Gautier	Gen	Privacy Officer	Assistant University Secretary
Bos	Gerrit	Data Retention and Destruction/Access Control	IT Security Officer
Thomson	Brian	Help Desk	Manager, Client Productivity
Hogg	Jill	Help Desk	Client Solutions
Tan	Vince	Help Desk	Client Solutions
Herr	Tom	Access Control	Manager, Network Infrastructure
West	Julie	Student Housing/Hospitality Services	Co-ordinator, Research & Special Projects, Student Housing
Griff	Nathan	Student Housing/Hospitality Services	IS Manager, Student Housing
Virani	Altaf	Student Housing/Hospitality Services	Assistant Director, Information Technology
Pettigrew	Brian	Registrar	Assistant Vice-President (Institutional Research & Planning) and Registrar
Anthony	Sharon	Registrar	Assistant Registrar – Enrollment Services
McQuarrie	Deanna	Registrar	Associate Registrar – Admission Services
Sheehy	Manuela	Registrar	Associate Registrar – Student Financial Services
Smith	Hugh	Identity Management/User Authentication	Campus Services, CCS
Nejedly	Zdenek	Identity Management/User Authentication	Systems Analyst
Begin	Robin	Campus Police	Director, Campus Community Police, Fire Prevention and Parking Services

Appendix 2 – Source documents list

Google Agreements

- Apps for Education v10022011 RL (February 2011)
- University of Guelph - Addendum (March 2012)

Documents Related to University of Guelph Policies and Procedures

- Protection of Privacy and Access to Information at Guelph: http://www.uoguelph.ca/info/privacyguidelines/ProtectionofPrivacyandAccesstoInformation.pdf
- Acceptable Use Policy and Guidelines: http://www.uoguelph.ca/web/aupg/
- Software as a Service Enterprise Guidelines: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/Software-as-a-ServiceEnterpriseGuidelines.pdf
- Policy on Release of Student Information: http://www.uoguelph.ca/policies/pdf/ORSInfoReleasePolicy060610.pdf
- Record Retention and Disposition Policy: http://www.uoguelph.ca/policies/pdf/Record%20Retention%20and%20Disposition%20Policy.pdf
- Departmental Privacy Policies: https://www.uoguelph.ca/secretariat/offices/bog/privacy-policies
- Mass Electronic Mail Policy: http://www.uoguelph.ca/info/massemail/
- Guidelines on making an Information Request under FIPPA: https://www.uoguelph.ca/secretariat/offices/bog/how-make-information-request-under-fippa
- Guidelines on making a privacy complaint: https://www.uoguelph.ca/secretariat/offices/bog/how-make-privacy-complaint
- End-Point Encryption Policy: http://www.uoguelph.ca/cio/content/end-point-encryption-policy
- Academic Calendar: http://www.uoguelph.ca/registrar/calendars/
- Information Technology Security Policy Framework: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-ITSecurity-00-PolicyFramework-2009Approved_0.pdf
- Information Technology Security Program: https://www.uoguelph.ca/cio/content/it-security-program
- Major IT Security Management Policy: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-ITSecurity-09.1-MajorIncidents-Approved-2011MAY_0.pdf
- IT Contracting Guidelines: https://www.uoguelph.ca/cio/content/it-contracting-guidelines

- External Contracting Guideline and sample: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-Guidelines-ContractGuidelines.pdf

Documents Related to University of Guelph Deployment

- Project Plan

Google Apps Acceptable Use Policy

Use of the Services is subject to this acceptable use policy ("AUP").

If not defined here, capitalized terms have the meaning stated in the applicable contract ("Agreement") between customer, reseller or other authorized user ("You") and Google.

You agree not to, and not to allow third parties or Your End Users, to use the Services:

- *to generate or facilitate unsolicited bulk commercial email;*
- *to violate, or encourage the violation of, the legal rights of others;*
- *for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;*
- *to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;*
- *to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;*
- *to alter, disable, interfere with or circumvent any aspect of the Services;*
- *to test or reverse-engineer the Services in order to find limitations, vulnerabilities or evade filtering capabilities;*

Your failure to comply with the AUP may result in suspension or termination, or both, of the Services pursuant to the Agreement.

University of Guelph Acceptable Use Policy for Information Technology

1. Purpose and Jurisdiction

The purpose of this policy is to define the acceptable use of Information Technology (IT) Resources in support of the mission of the University of Guelph. It builds on the principles of accountability, transparency, privacy, and fairness, to support a functional environment for work and study in which these resources are protected. This policy applies to anyone who uses or accesses any IT Resource belonging to, under the control or in the custody of, the University of Guelph.

2. Definitions

For the purposes of this policy, the following terms are defined as follows:
Account – includes any username, access code, password, PIN, token, credential, or other authentication which has been assigned to Authorized Users to use any University IT Resource.
Authorized – means specific access rights granted in accordance with University governance or policies.
Authorized User – means a member of the University of Guelph community, who is an employee, student, alumni, associate, or other individual who has been granted specific rights by a University signing officer, or someone delegated in accordance with University governance or policies to use any University IT Resource.
Community Standards – means behaviour or material which the average member of the University Community would reasonably tolerate.
Information Technology (IT) Resource – means any information, data, software, hardware, system, or network belonging to, under the control or in the custody of the University, regardless of who administers it.
Information Technology (IT) Security Officer – means the University employee or designate who is responsible for enforcing the Acceptable Use Policy

Personal Information – means recorded information about an identifiable individual, and as defined in federal and provincial privacy legislation
System Administrator – means an individual responsible and authorized to establish or maintain and provide technical support for a University IT Resource.

3. Acceptable Use

The University of Guelph authorizes the University community to use its Information Technology Resources to fulfill and advance the University's teaching, learning, research, service, administrative, and community development missions.

In addition, the University permits limited personal use of these resources, provided this use does not violate any law, statute, or University policy. Users who require a private means of computing and sending electronic communications should utilize a personal device unconnected to the University's IT network**.**

The University respects the privacy of all users of its IT Resources, and uses reasonable efforts to maintain confidentiality of Personal Information. Circumstances may arise in which such privacy cannot be maintained. Such circumstances include, but are not limited to:

1. Access to Personal Information may be granted to an Authorized User, System Administrator or agent to meet legitimate University business needs and operational requirements, or in the event that an Authorized User is unavailable, or has his or her access revoked.
2. The University may audit, access or restore any IT resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

Such access will be subject to the authorization of the appropriate Vice-President (or designate) in consultation with the Provost.

Authorized Users must exercise good judgment in determining what is acceptable use of IT Resources with due regard to this policy, other University policies and Community Standards. Some activities may be appropriate in a specific context (e.g. for authorized academic and research purposes), while some are not appropriate in any context.
Authorized Users have an obligation to take all reasonable steps (e.g. password protection and strengthening) to protect the confidentiality, integrity, and availability of IT Resources and report encountered vulnerabilities to the Information Technology Security Officer. Failure to do so may constitute a breach of this policy.

Examples of a Breach of Acceptable Use

Unless explicitly authorized, a breach of acceptable use includes, but is not limited to:

1. Allowing others to access your assigned personal Account
2. Failure to exercise reasonable care in safeguarding Accounts and information
3. Accessing someone else's personal Account
4. Seeking information on passwords or information belonging to others
5. Breaking or attempting to circumvent licensing or copyright provisions
6. Copying, deleting, intercepting, or examining someone else's files, programs, or information
7. Attempting to collect, use, or disclose, the Personal Information of others
8. Using IT resources to harass or bully others
9. Attempting to circumvent information security provisions or exploit vulnerabilities
10. Using IT Resources (e.g. University computing account or workstation) for unauthorized commercial purposes
11. Any interference with the ability of others to use IT Resources whether it is disruptive or not
12. Falsifying or misrepresenting your identity
13. Viewing or using pornographic or offensive material in a work, study, or public location
14. Distributing or disseminating pornographic or offensive material in any location

4. Outcomes

If the integrity or security of an IT Resource is compromised or at risk the Information Technology (IT) Security Officer may direct the locking or quarantining of an Account or resource at his or her sole discretion. Upon reasonable belief by the IT Security Officer that a violation of this policy (AUP) may have occurred, the IT Security Officer or designate will conduct an investigation.

If access to any Personal Information is required, authorization will be requested of the appropriate Vice-President (or designate) in consultation with the Provost.

If insufficient evidence of a violation of the AUP is found, the investigation will be closed and involved parties notified where appropriate.

The IT Security Officer will issue a written decision regarding the alleged policy violation within a reasonable timeframe, normally 30 days. Actions noted below may be initiated upon determination of a violation of this policy.

An Authorized User affected by this decision may file an appeal to the Chief Information Officer (CIO). The Authorized User will have 10 calendar days from the issuance of a written decision to file an appeal with the CIO. The CIO may confirm, rescind, or modify the decision. The decision of the CIO is considered final**.**

If a violation is determined to have occurred, the following actions may be initiated by the IT Security Officer:

Class or severity	**Possible outcomes**
Minor violation of the AUP	Warning
Serious or repeated violation of the AUP	Escalation to appropriate authority or disciplinary process and/or restrictions on access or use
Possible violation of another University policy or regulation	Forward for investigation by applicable process under the applicable policy or regulation
Possible violation of federal, provincial, or municipal law or statute	Forward for investigation to Campus Community Police

5. Related University Policies

This Acceptable Use Policy prohibits any use of IT Resources which potentially violates any other University of Guelph policy, code or agreement, constitutes academic or non-academic misconduct, or which violates federal, provincial, or municipal laws or regulations.

In addition to outcomes under the AUP, such violations may be prosecuted under those laws and policies. Any information resulting from an investigation under the AUP may be shared for the purposes of such prosecutions.

Some of these policies include:

- Human Rights Policy
- Graphics Standards Guide
- Mass Electronic Mail Policy
- Protection of Privacy and Access to Information
- Release of Student Information
- Residence Community Living Standards
- Student Rights and Responsibilities
- University Undergraduate or Graduate Calendars
- Human Resources Policies
- Collective Agreements or other Employment Agreements

A more comprehensive list of applicable University policies is maintained by the University Secretariat at http://www.uoguelph.ca/policies/.

6. Departmental AUPs

Departments may have Departmental Acceptable Use Policies to meet their specific operational requirements. An Authorized User using Departmental IT Resources is bound by the Departmental AUP. In the event of a conflict between the Departmental AUP and this policy, this policy prevails.

Essential Components of Departmental AUPs are:

1. A copy of the Departmental AUP must be available to all employees of that department
2. Definition or description of Departmental IT Resources which the Departmental AUP applies to
3. One or more locations where the current University and departmental AUPs may be found.
4. List of user responsibilities and expectations specific to the use of Departmental IT Resources with clear examples of unacceptable actions of activities
5. An indication of actions and examinations considered routine with regard to Departmental IT Resources
6. How suspected violations of the Departmental AUP are handled
    a. Department Chair for violations specific to the Departmental AUP
    b. IT Security Officer for issues related to the University AUP
7. The circumstances under which accounts or access to Departmental IT Resources is terminated or restricted

Any Departmental AUP will be submitted for review to the Chief Information Officer or designate prior to implementation. Review will be completed within a reasonable timeframe, normally 30 days.

For additional information regarding Google Apps for Education, please visit the following website: http://www.google.com/apps/intl/en/edu/University.html.

Appendix 3 – Sensitivity injury tables

Injury tables 1 and 2 below were used to assign confidentiality, integrity and availability ratings to critical assets identified in table 3.

Confidentiality and integrity

Confidentiality refers to the disclosure of information for legitimate purposes only to those who are authorized. This considers how sensitive to unauthorized disclosure the information or data is under normal conditions.

Integrity refers to authenticity and assurance that information is not altered, except as authorized for legitimate reasons. This considers how sensitive to corruption or unauthorized change the information or data is under normal conditions.

Level of injury	Injury Description		
	Individual	Financial	Reputation
Very High *(Catastrophic)*	Very large scale sensitive information disclosure (more than 500 users affected)	More than $5M	Severing of relationship with partner / stakeholder
High *(Critical)*	Large scale sensitive information disclosure (more than 25 users affected)	$1M < $5M	Relationship damaged with partner / stakeholder
Medium *(Moderate)*	Small scale sensitive information disclosure (less than 25 users affected)	$25K < $1M	Damage to rapport with partner / stakeholder
Low *(Minor)*	Name, address disclosure	Less than $25K	No reputation damage

Table 1: Confidentiality and Integrity Injury test

Availability

Availability refers to reliable access to information by authorized users for legitimate purposes. This considers how important timely access to the information or data for users is under normal conditions.

Level of Injury	Description
Very High	Required for continuous operations
High	Required 7 days a week, 5% scheduled down time is acceptable
Medium	Required daily during regular business hours
Low	Required weekly (or less frequently) for a defined period

Table 2: Availability Test

Asset ratings

Critical Asset ID	Critical Asset Name	Type	Confidentiality	Integrity	Availability
People[8]					
CA-01	Students	People	Medium/High	N/A	N/A
CA-02	Email Administrators	People	N/A	N/A	High
Processes					
CA-03	Help Desk Processes	Processes	Medium	High	High
CA-04	Security Processes	Processes	Medium	High	High
CA-05	Vendor Processes	Processes	Medium	High	High
Information					
CA-06	System configuration information	Information	High	High	High
CA-07	Email data	Information	High	High	High
CA-08	System User Authentication Credentials	Information	High	High	High
CA-09	User documents	Information	High	High	Medium
Hardware					
CA-10	Cisco IronPort Gateway	Hardware	Low	High	High
Software					
CA-11	Mail routing software (Cisco IronPort)	Software	Low	High	High
CA-12	Zimbra email system	Software	Low	High	High
CA-13	Google Apps for Education email and calendaring suite	Software	Low	High	High
Facilities					
CA-14	University of Guelph Data Centre	Facility	Low	High	High
CA-15	Google offsite premises/Data Centres	Facility	Low	High	High

Table 3: Critically Identified Assets

[8] All people have a high intrinsic value. Only operational availability values are depicted.

Appendix 4 – Threat agent ratings

Table 3 - Threat Likelihood

Past frequency	Same location Similar assets	Remote location but similar assets or Same location but different assets	Remote location other assets
Daily	High	High	High
1-10 Days	High	High	Moderate
10-100 Days	High	Moderate	Low
100-1,000 Days	Moderate	Low	Very Low
1,000-10,000 Days	Low	Very Low	Very Low
Over 10,000 Days	Very Low	Very Low	Very Low

Table 4 - Threat Gravity

Deliberate threat agent capabilities	Magnitude of accidents or natural hazards	Threat impact or gravity
Extensive Knowledge/Skill Extensive Resources	Highly Destructive Extremely Grave Error Widespread Misuse	High
Limited Knowledge/Skill Extensive Resources or Extensive Knowledge/Skill Limited Resources or Moderate Knowledge/Skill Moderate Resources	Moderately Destructive Serious Error Significant Misuse	Moderate
Limited Knowledge/Skill Limited Resources	Modestly Destructive Minor Error Limited Misuse	Low

Table 5 – Threat Rating

Threat Impact/Gravity	Threat likelihood			
	Very Low	**Low**	**Medium**	**High**
High	Low	Moderate	High	Very High
Medium	Very Low	Low	Moderate	High
Low	Very Low	Very Low	Low	Moderate

Threat Agent Identifier	Threat Agent Title	Description	Type	Knowledge / Skill	Resources	Magnitude	Impact/ Gravity
TA.01	Users	Faculty, Staff, students or insiders not having system access privileges, who could pose a threat to information and information systems. The typical users have limited physical access to the internal system core components. They have logical access to the information held within the system and have considerable knowledge of the internal system operations.	Accident	N/A	N/A	Moderately Destructive	Low
TA.02	Administrators	Individuals with privileged access to the internal systems. The privileged user/employee has been granted highly trusted logical and physical access to internal system and has in-depth knowledge of the infrastructure. This user may inadvertently introduce errors. Errors made at this level could easily affect the internal system as a whole. This Threat Agent may inadvertently introduce errors or misuse the processes. These are employees having privileges over and above that of a regular employee. They are likely to work in areas such as IT, helpdesk, network support, etc.	Accident	N/A	N/A	Serious Error	Moderate
TA.03	Vendors	Service providers who do not have appropriate security considerations included in their Service Level Agreements.	Accident	Moderate	Limited	Serious Error	Moderate
TA.04	Users	Faculty, Staff, students or insiders not having system access privileges, who could pose a threat to information and information systems. The typical users have limited physical access to the internal system core components. They have logical access to the information held within the system and have considerable knowledge of the internal system operations.	Deliberate	Limited	Moderate	Significant Misuse	Moderate
TA.05	Administrators	Individuals with privileged access to the internal systems. The privileged user/employee has been granted highly trusted logical and physical access to internal system and has in-depth knowledge of the infrastructure. This user may inadvertently introduce errors. Errors made at this level could easily affect the internal system as a whole. This Threat Agent may inadvertently introduce errors or misuse the processes. These are employees having privileges over and above that of a regular employee. They are likely to work in areas such as IT, helpdesk, network support, etc.	Deliberate	Extensive	Extensive	Serious Error	High
TA.06	Vendors	Service providers who do not have appropriate security considerations included in their Service Level Agreements.	Deliberate	Extensive	Moderate	Widespread Misuse	High
TA.07	Hackers & Criminals	A group or individuals who attack networks and systems seeking to exploit the vulnerabilities or other flaws.	Deliberate	Moderate	Extensive	Highly Destructive	High

Appendix 5 – Vulnerability assessment tables

Table 6 - Vulnerability Impact or Probability of Compromise (Prevention)

Safeguard effectiveness	Associated vulnerabilities	Probability of compromise
No Safeguard Safeguard Largely Ineffective Probability of Compromise > 75%	Easily Exploited Needs Little Knowledge/Skill/Resources Assets Highly Accessible Assets Very Complex/Fragile/Portable Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Probability of Compromise 25-75%	Not Easily Exploited Needs Some Knowledge/Skill/Resources Assets Moderately Accessible Assets Fairly Complex/Fragile/Portable Moderate Employee Awareness/Training	Moderate
Safeguard Very Effective Probability of Compromise < 25% (Safeguard Performs Only Detection, Response or Recovery Functions)	Difficult to Exploit Needs Extensive Knowledge/Skill/Resources Assets Highly Accessible Assets Very Simple/Robust/Static Employees Well-Informed/Trained	Low (Not Applicable)

Table 7 - Vulnerability Impact on Severity of Outcome (Detection, Response, Recovery)

Safeguard effectiveness	Associated vulnerabilities	Severity of Outcome
No Safeguard Safeguards Largely Ineffective Assets Exposed to Extensive Injury	Unlikely to Detect Compromise Damage Difficult to Contain Prolonged Recovery Times/Poor Service Levels Assets Very Complex/Fragile Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Assets Exposed to Moderate Injury	Compromise Probably Detected Over Time Damage Partially Contained Moderate Recovery Times/Service Levels Assets Fairly Complex/Fragile Moderate Employee Awareness/Training	Moderate
Safeguard Very Effective Assets Exposed to Limited Injury (Safeguard Performs Only a Prevention Function)	Compromise Almost Certainly Detected Quickly Damage Tightly Contained Quick and Complete Recovery Assets Very Simple/Robust Employees Well-Informed/Trained	Low (Not Applicable)

Table 8 - Vulnerability Levels

Vulnerability impact on severity of the outcome(detection, response & recovery)	Vulnerability impact on probability of compromise (prevention)		
	Low (N/A)	**Medium**	**High**
High	Moderate	High	Very High
Moderate	Low	Moderate	High
Low (N/A)	Very Low	Low	Moderate

Identified safeguards

SG#	Safeguard Description
SG-01	Identity Management and Single Sign-On (SSO) is used to help authenticate users
SG-02	The Cisco IronPort mail gateway is used to secure email
SG-03	There is proactive monitoring of the Cisco IronPort mail gateway
SG-04	Contract provisions with Google are in place to protect the University
SG-05	The Cisco IronPort mail gateway is regularly patched
SG-06	There is regular monitoring of email to detect security incidents/compromises
SG-07	This is central enforcement of critical email security settings

Identified vulnerabilities

VN#	Vulnerability Description
VN-01	The Cisco IronPort mail gateway could be misconfigured increasing the risk that emails could be misdirected
VN-02	The University has no control on confidential data that is stored outside its premises / by Google
VN-03	There is no central monitoring of logs, increasing the risk that malicious events could go undetected
VN-04	There is no enforcement of password complexity or change requirements
VN-05	The Cisco IronPort mail gateway is not regularly maintained/updated
VN-06	There is no requirement for Google to report any email security incidents/compromises
VN-07	End users have the ability to modify their email security settings

Appendix 6 – Risk level tables

Table 9 - Numeric Scores for Asset Value, Threat and Vulnerability Levels

Asset Value, Threat and Vulnerability Levels	Very Low	Low	Medium	High	Very High
Scores for Risk Computation	**1**	**2**	**3**	**4**	**5**

Table 10 - Risk Levels and Ranges

Targeted residual Risk	Very Low	Low	Medium	High	Very High
Risk Score (R* in Appendix G)	1 - 4	5 - 12	13 - 32	33 - 75	76 - 125
Remedial Action Required?	No	Probably Not	Possibly	Probably	Definitely

Appendix 7 – University action plans on recommendations

Recommendation	Scenarios Mitigated	Management comments on action plans	Responsible party and timing
Recommendation #1: Implement well documented processes (and automated processes if possible) to handle provisioning, modification and de-provisioning of email accounts to reduce the likelihood of email gateway misconfiguration.	RS-1		**Responsible party:** [to be filled in] **Timing:** [to be filled in]
Recommendation #2: The University should incorporate a process to ensure there is central monitoring of system, network and application logs to help detect any misdirection/ misconfiguration issues relating to the IronPort so they can be rectified in a timely manner. Security Incident and Event Management (SIEM) systems should be considered as part of this to enable automated correlation and alerting of events and reduced manual monitoring of data.	RS-1 RS-2		**Responsible party:** [to be filled in] **Timing:** [to be filled in]
Recommendation #3: The University should implement regular vulnerability testing on externally facing systems such as the IronPort as a verification that all know vulnerabilities are patched or otherwise mitigated for these systems.	RS-2		**Responsible party:** [to be filled in] **Timing:** [to be filled in]
Recommendation #4: At a minimum, there should be a requirement to enforce both the use of alphanumeric passwords and enforcing regular password changes.	RS-3		**Responsible party:** [to be filled in] **Timing:** [to be filled in]
Recommendation #5: The University should insist that Google include contract provisions on how security incidents should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.	RS-4		**Responsible party:** [to be filled in] **Timing:** [to be filled in]
Recommendation #6: The University should insist that Google include contract provisions on how the monitoring and detection of compromised email accounts should be handled and what related processes should be followed such that the University is informed and decisions can be made on next steps and action items.	RS-5		**Responsible party:** [to be filled in] **Timing:** [to be filled in]

Recommendation	Scenarios Mitigated	Management comments on action plans	Responsible party and timing
Recommendation #7: The University should work with Google to ensure that centrally set email security settings cannot be overridden by end users/students.	RS-6		**Responsible party:** [to be filled in] **Timing:** [to be filled in]

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte operates in Quebec as Deloitte s.e.n.c.r.l., a Quebec limited liability partnership.