FOR APPROVAL **PUBLIC** **CLOSED SESSION**

TO: Governing Council

SPONSOR: Professor Scott Mabury, Vice-President, University Operations
CONTACT INFO: 416.978.2031, scott.mabury@utoronto.ca

PRESENTER: see above
CONTACT INFO:

DATE: February 9, 2016 for February 25, 2016

AGENDA ITEM: 5 (a.)

ITEM IDENTIFICATION:

Policy on Information Security and the Protection of Digital Assets

JURISDICTIONAL INFORMATION:

Section 4 of the Terms of Reference for the Academic Board states:

> *The Academic Board is responsible for consideration of policy in the academic area and for monitoring matters with its area of responsibility. In general, the Board is concerned with matters affecting the teaching, learning, and research functions of the University, the establishment of University objectives and priorities, the development of long-term and short-term plans and the effective use of resources in the course of these pursuits.*

GOVERNANCE PATH:

1. Planning & Budget Committee [for recommendation] – January 13, 2016
2. Academic Board [for recommendation] – January 28, 2016
3. Executive Committee [for endorsement and forwarding] – February 9, 2016
4. **Governing Council [for approval] – February 25, 2016**
5. Audit Committee [for information] – March 3, 2016

PREVIOUS ACTION TAKEN:

The *Policy on Information Technology* was approved by the Governing Council on February 1, 2007, replacing the *Policy on the Use and Development of Computing Facilities* (1984) and the *Computing Services Financial Policy and Accounting Practice in Respect of Major Computer Mainframe Acquisitions* (1978). The *Policy* states: "The Vice-President and Provost is authorized to establish guidelines and procedures related to the use of information technologies."

The Audit Committee has been provided with periodic updates in the development of the proposed *Policy on Information Security and the Protection of Digital Assets*. The *Policy* was presented for information and discussion at the Planning & Budget Committee meeting of May 13, 2015.

HIGHLIGHTS:

Background

This *Policy* is designed to enhance the level of security protecting the information that is generated, processed, used and stored electronically at the University. Such "Digital Assets" (defined in the proposed *Policy*) exist in widely distributed electronic information systems that address University-wide, divisional and local needs.

The *Policy* is intended to provide a framework within which central Information Technology Services (ITS) and central and academic divisions will develop and implement their own plans for information security and the protection of Digital Assets. The proposed *Policy* addresses the establishment of Standards, as well as Procedures and Guidelines to ensure those Standards are maintained. The *Policy* will not impinge on divisional discretion when it comes to Information Technology (IT) services and activities, provided such Standards are met. In addition, it explicitly acknowledges that some of the information generated, processed, used and stored is protected by academic freedom, is personal information, is proprietary information, is confidential, or that otherwise has elements that, pursuant to other University policies and agreements, may require special treatment.

Current Risk and Need

U of T's decentralized IT structure offers flexibility to its faculty members and units in designing their own IT solutions to fit local research and teaching needs. Given the nature of University work, its network is very open, with the potential of presenting 393,000 publicly addressable devices to the world, whereas most private sector institutions might present only a handful. Information and Digital Assets generated by the University's faculty, staff, and students are housed in many places – for example, on the University's networks and servers and on University systems like Blackboard and ROSI; as well as on cloud platforms like Dropbox, on mobile devices, on individual personal computers, and elsewhere.

Information and Digital Assets at U of T are subject to risk on many fronts – for example, an unencrypted personal computer or tablet with research data that is lost on the subway could lead to a major data breach, or a hacker intentionally targeting one of the University's servers could expose personal student information. Risks of this nature are not merely hypothetical. Because of its extensive research and teaching activity, the University faces persistent attacks against our networks. There have been data vulnerabilities at the University that could have had serious ramifications in terms of exposure of personal information and private data had they not been controlled and secured quickly.

The risk currently faced by the University is similar to that which is faced by other public-sector and private-sector organizations, but it has an added dimension – resulting in the potential for additional risk – in the highly distributed nature of the University's computing resources. Many peer institutions have policies like the proposed one in order to deal with securing information, including personal and private information, and to help prevent data breaches. In formulating this *Policy*, the University has drawn on the experience of these peer institutions. This rapidly evolving and technical area has been identified – both internally at the University through the Audit Committee and elsewhere, and by external entities such as the Ontario Information and Privacy Commissioner – as being extremely important if privacy and security are to be maintained.

Highlights

Some key elements of the *Policy* are as follows:

- A statement of the importance of protection of the University's Digital Assets
- The requirement that every academic and administrative unit develop a risk management plan to promote information security and the protection of Digital Assets.
- The establishment of a consultative framework for continuous improvement in identifying minimum security Standards and related Procedures for University-wide application
- A stated commitment to academic freedom
- Provision for limited emergency authority, subject to review
- Naming of the President or designate as the institutional authority for information security
- Affirmation that information security requirements shall align with all relevant University policies
- The establishment of an Information Security Council (ISC) to recommend University-wide Standards and Procedures, to be co-chaired a faculty member with academic expertise and the Director of the ITS Information Security department
- Reporting to governance through the Planning & Budget and Audit Committees

Consultation

The administration has engaged in eighteen months of broad consultation across the academic, administrative and IT staff communities of the University. Consultation included discussion with the Principals and Deans group, with standing IT committees such as the divisionally representative IT Leaders Forum, at various departmental meetings, in individual meetings with faculty members and departments, and at other venues. In addition, various drafts of the *Policy* were shared with the broader University community through the ITS Web site and the Info-Tech listserv.

The CIO assembled a Working Group on Information Risk Management Practice to set the foundation for the *Policy*'s implementation alongside development and finalization of the *Policy* itself. The Working Group, co-chaired by Professor Ron Deibert and the Director of ITS Information Security, is developing recommendations for information risk management Procedures, Standards and Guidelines, and will also provide recommendations on the establishment of its successor, the ISC.

In spring 2015, the administration heard from faculty members and department Chairs in the Faculty of Arts & Science (FAS) and the Faculty of Applied Science and Engineering (FASE) with some concerns about the proposed *Policy*. Themes of the feedback primarily focused on:

- A desire for the University's commitment to academic freedom to be reflected in the *Policy*, particularly with regard to information and data related to research and teaching activities,
- The potential for increased centralization of IT resources and costs of implementation, and
- Questions about the membership and Terms of Reference of the ISC.

Over the course of summer 2015, the Provost, Vice-President, University Operations, and Vice-President, Research & Innovation met with faculty and staff from academic divisions to hear and respond to these concerns. A smaller *ad hoc* group was assembled, co-chaired by the Vice-President, University Operations and Vice-President, Research & Innovation, with membership from FAS, FASE, the Faculty of Information, the University of Toronto Mississauga, and other divisions, to offer further feedback on the *Policy* and its eventual implementation.

A letter from the University of Toronto Faculty Association (UTFA), dated October 20, 2015, also raised some concerns about aspects of the *Policy*, in line with other feedback received. The Provost has indicated that a joint working group with UTFA has been formed to examine the separate but related issue of privacy related to the electronic records of faculty and librarians.

The proposed *Policy* has been revised on several occasions in response to feedback received from these various sources. After significant revision to account for these community concerns, the administration believes that the proposed *Policy* addresses the important security and risk mitigation required for the protection of the University's essential research and teaching mission in a manner that is responsive to local academic and administrative needs, as well as to the various elements of University Policies and Agreements that may intersect.

Oversight

The *Policy* gives oversight for the *Policy* to Governing Council, requiring an annual report by the President or designate to its Planning and Budget Committee and the Audit Committee. Supporting the implementation of the *Policy* is a cascading set of responsibilities:

- The President or designate is responsible for information security and the protection of Digital Assets under the *Policy* and the establishment of Procedures and Standards to give effect to the *Policy*.
- The ISC recommends the Procedures and Standards to the President as well as gives input into the operation of the *Policy*, and in turn receives feedback and regular reports from the President regarding these matters. This feedback loop will enhance both effectiveness and transparency when it comes to assessing metrics of the *Policy*'s implementation and actions related to security vulnerabilities and remediation.
- The ISC will be chaired jointly by a faculty member and the director of the ITS Information Security department, and will be advisory to the President. This reflects the

desire for broad input from all relevant stakeholders as Standards and Procedures are developed.

The *Policy* acknowledges the President or designate's authority to take emergency steps to protect Digital Assets in the event of data breaches and similar emergency situations, but ensures transparency in requiring notification to those affected, and reporting in a variety of ways.

The *Policy* is explicit in stating that Procedures, Standards and Guidelines must be consistent with the University's mission and purpose, as well as all relevant University Policies and Agreements, including those dealing with the protection of academic freedom. These would include policies that confirm the University's obligations under *Freedom of Information and Protection of Privacy Act* (FIPPA) and other relevant legislation, as well as the *Memorandum of Agreement between The Governing Council of the University of Toronto and The University of Toronto Faculty Association*.

Implementation

After the *Policy* is approved by the Governing Council, an implementation phase will begin. The *Policy* requires that academic and administrative department heads remain responsible for assuring the protection of Digital Assets within their units. Each unit will be expected to develop its own Information Risk Management program that is appropriate to its own needs. (An example of a divisional implementation plan and Information Risk Management program from the Faculty of Medicine is attached.) The ITS Information Security department has indicated that it is pleased to assist units in this process and in the development of various training resources and compliance programs, as it did with the Faculty of Medicine.

A major element of the *Policy*'s implementation is the establishment of the ISC and the setting of its terms of reference. The composition of the ISC will be appropriately representative of the various central and academic divisions as well as faculty, staff, and librarian stakeholders. There will be robust academic participation and consultation in the ongoing deliberations and work of the ISC.

The importance of divisional and local roles in exercising their own continuing discretion is emphasized in the *Policy*'s requirements. The implementation of the *Policy* will preserve the flexibility that makes U of T's IT structure so distinctive while adding appropriate accountability mechanisms.

FINANCIAL IMPLICATIONS:

There are no direct implications for the University's operating budget at this time. Specific implications will become known as the *Policy* is implemented across the University.

RECOMMENDATION:

Be It Resolved

THAT the proposed *Policy on Information Security and the Protection of Digital Assets,* dated December 21, 2015, be approved effective February 26, 2016.

DOCUMENTATION PROVIDED:

Policy on Information Security and the Protection of Digital Assets

Faculty of Medicine Implementation Plan

University of Toronto *Policy on Information Security and the Protection of Digital Assets*

Revision: December 21, 2015

Statement of Intent

The University of Toronto adopts this ***Policy on Information Security and the Protection of Digital Assets*** as a measure to protect the privacy, confidentiality, integrity, and availability of Digital Assets, including information systems that store, process or transmit data. This *Policy* applies to all academic and administrative units, third-party agents of the University, as well as any other University affiliate that is authorized to access institutional data, services and systems.

All University of Toronto campuses, divisions, departments and other administrative or academic organizational units shall deploy and use IT systems and services in a manner consistent with the University's research and teaching mission, while vigilantly mitigating security risks to Digital Assets, including data during storage, transit, use and disposal. It is the obligation of all University community members to protect information that is created by them and stored by the University and its authorized delegates to its defined principles and standards.

Across the University, those charged with managing and securing Digital Assets shall operate in a manner that reduces and mitigates vulnerabilities by following Standards, Guidelines and Procedures for protecting the University's Digital Assets. Facilities, services, and systems that operate at University-wide, divisional and departmental levels will meet these requirements.

Administrative Authority

The President or designate shall have overarching responsibility for the protection of the University's Digital Assets. The President or designate is authorized to approve Procedures and Standards and to promote Guidelines for the protection of the University's Digital Assets.

Academic and administrative unit heads shall be responsible for assuring the protection of Digital Assets within their units in accordance with this *Policy* and associated Procedures and Standards.

In order to ensure broad consultation in planning and decision-making processes, an **Information Security Council** (ISC) will be established by the President or designate. The ISC will: assist in the review of envisioned and unanticipated risks to the University's Digital Assets; collaborate with the President or designate to initiate information security initiatives; educate the University community on digital security best practices; and develop and recommend Procedures, Standards and Guidelines for the protection of the University's Digital Assets.

In support of these shared responsibilities, each unit shall in consultation with the ITS Information Security department, and others as appropriate, develop an Information Risk Management Program appropriate to the circumstances of the unit, to be approved by the unit head. The President or designate, in collaboration with the ISC, will review such programs to ensure compliance with this *Policy* and associated Procedures and Standards.

Procedures, Standards and Guidelines must be consistent with the University's mission and purpose, as well as all relevant University Policies and Agreements, including those dealing with the protection of academic freedom. The President or designate will provide regular updates to the ISC about progress in developing and implementing Procedures, Standards and Guidelines in support of this *Policy*.

Governance Oversight

The President or designate shall report annually to Governing Council via the Audit Committee and the Planning and Budget Committee.

Emergency Authority

In the event of an emergency situation that threatens the University's Digital Assets, the President or designate shall have full authority to enact emergency response measures that shut down the risk or mitigate further damage to Digital Assets and protect the University community. Actions taken by the President or designate under this Emergency Authority shall be reported to the Information Security Council and in the President or designate's annual report to Governing Council via the Audit Committee. Those affected by such actions under this Emergency Authority shall be notified as soon as practicable before or after such actions are taken.

Publication

Procedures, Standards and Guidelines will be published and be readily available to members of the University community.

Definitions

Digital Assets – Meant here as the collection of data, information systems, applications, and equipment that contain and process the intellectual property of the University and of the members of its community, and the mechanisms for storage, information processing, and distribution of these data. Digital Assets can include, among other things, information protected by academic freedom, personal information, proprietary information, and confidential information.

Information Security Council (ISC) – The Information Security Council (ISC) is a committee established by the President or designate. The ISC will be co-chaired by a senior faculty member and the director of the ITS Information Security Department. The ISC will be comprised of technical, administrative and academic experts.

Guidelines – Best practises and approaches to protecting Digital Assets. These are not mandated or prescriptive, but are meant to provide guidance to the community for implementing practises that mitigate risks. (For example, Guidelines on accessing U of T resources from an airport or other public Internet connection.) Guidelines will evolve over time.

Procedures – Required practises for protecting Digital Assets as developed through input from the Information Security Council and approved by the President or designate. (For example, Procedures to be followed when disposing of computing devices.) Procedures will be developed and revised as appropriate over time.

Standards – Standards set a baseline for Digital Asset protection. These Standards, developed through input from the Information Security Council and approved by the President or designate, are conceptual and may allow the deployment of different technologies and approaches to meet the Standard. (For example, "Encrypted files must minimally deploy a 256-bit key." The encryption protocol is not mandated, just the level of protection.) Standards will be set and revised as appropriate over time.

UNIVERSITY OF TORONTO
FACULTY OF MEDICINE

Faculty of Medicine
Information Risk Management Program

Table of Contents

A. Introduction

The Information Risk Management Program at the Faculty of Medicine has been established under the authority of the Dean of the Faculty of Medicine, in coordination with the University's Chief Information Officer (CIO), and in accordance with the Faculty's *Information Technology Security Principles* (see Appendix A).

The Faculty of Medicine recognizes and accepts that it has a responsibility to the University in the management of risks associated with information solutions (both products and services). The goal of the Information Risk Management Program (IRMP) is to ensure that risks to the Faculty and the University, arising from mis-handling or mis-identification of information, are managed as an integral component of information solutions throughout their lifecycle, and in full accordance with the policies and guidelines of the University.

This document outlines a proactive framework for identifying and managing information risk, and opportunities to take advantage of existing enterprise infrastructure, at all points in the information solution lifecycle. This framework will form the basis for locally defined roles, practices and procedures designed to support the ongoing awareness and management of information risk.

B. Context and Scope

Since the University became subject to Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) in June 2006, there have been significant increases in the size and frequency of data breaches, the cost of mitigating them, the public attention paid to them, and the sophistication of cyber criminals. Just this year, high-profile breaches at retailers Target and Home Depot have resulted in the exposure of millions of credit card numbers, and in July a "highly sophisticated Chinese state-sponsored actor" hacked into the computer systems at Canada's National Research Council[1], forcing the NRC to rebuild its computer infrastructure from the ground up. In addition, a recent report[2] sponsored by IBM shows that both the probability and the cost of data breaches in education to be among the highest of any sector.

In this context, the Faculty is working with the University to establish a more coordinated, proactive, and thorough approach to information security to protect the information technology (computers, networks, and applications) and information created by its members and stored by the University—no matter where it might be hosted or geographically located. Of particular concern is the protection of Confidential Data, and more specifically, of Protected Data (a higher-risk category of Confidential Data), which is defined below.

An information solution is any combination of hardware or software (no matter by what arrangement it is procured or licensed), designed and built for a specific work-related purpose, usually for multi-user or network-based access. Examples include (but are not limited to) a database on a shared drive, a website or a web application, or a cloud-based service. The IRMP process, as outlined in the Roles & Responsibilities section of this document, applies to anyone with a faculty or staff appointment in the Faculty of Medicine who has a role in the lifecycle of an information solution.

C. What is Protected Data?

Protected Data (PD) is data that includes the following types of Confidential information:

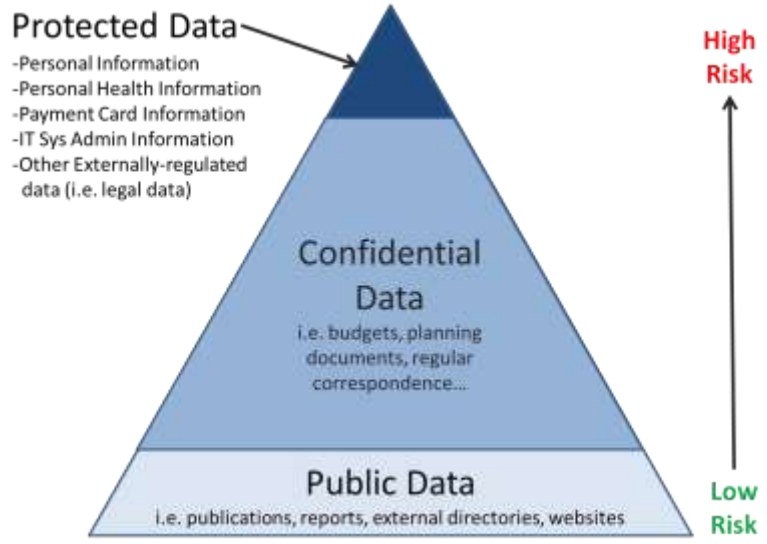
- Personal Information
- Personal Health Information
- Payment Card Information
- IT System Administrator access to information and information solutions / infrastructure (such as root or administrator passwords)
- Other data with externally-regulated protection requirements (such as legal data)

This list may be subject to revision as additional sensitive data classes are identified.

Protected Data is currently the highest data sensitivity classification at the University of Toronto, the others being "Public" (data that is made available without requiring authentication) and "Confidential"

[1] http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241
[2] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

(data that is neither Public nor Protected, and makes up the majority of the data held by the University). This structure can be visualized as a pyramid, in which data at the base (Public data) is of low risk, while data at the apex (Protected data) is high risk.



Personal information is information about an identifiable individual, and its handling is regulated by the Ontario Freedom of Information and Protection of Privacy Act (FIPPA). For more information about FIPPA and personal information, visit the FIPP Office website at http://www.fippa.utoronto.ca/.

The higher the risk, the greater the need for information security controls, records retention policies and practices, and business continuity plans. External requirements may complement or guide the practical implementation of legislation, as determined by professional or authoritative bodies. In all cases, the more stringent data protection requirements–internal, external, or a combination–must be followed.

D. The IRMP Committee

An IRMP committee has been struck for the ongoing execution and oversight of the IRMP, with a permanent membership that includes the following:

- The Faculty's Chief Administrative Officer (CAO)
- The Faculty's Director of Information Technology
- The University's Director of Information Security

The IRMP committee will meet as often as is required for the timely assessment of new information solutions. The IRMP committee is responsible for:

1. Regularly informing the Dean about information security and risk issues, as well as the development, implementation, and operation of risk management activities and controls.

2. Reviewing the division's processes, guidelines, and standards (proactive and reactive) relating to information risk management, approving them for use, and evaluating their performance.
3. Requiring from all organizational units within the division an annually-updated inventory of existing information solutions that contain Protected Data.
4. Assessing all Information Risk and Risk Management (IRRM) questionnaires completed for new information solutions that contain Protected Data or that introduce new risks, whether hosted locally within the University or hosted externally (including in the "cloud").
5. Ensuring that all identified risks are either managed to be equivalent to or better than current University best practice, and/or as required by legislation, contract, or agreement.
6. Ensuring that University-approved and provided IT infrastructure and services are used and leveraged to the greatest extent possible.
7. Defining and tracking information risk management metrics, and providing an annual report to the Dean based on these metrics and on the activities of the IRMP Committee.

Approval by the IRMP Committee must be received prior to an information system being put into production, and ideally before it has been procured or developed.

It is essential that proposed new information solutions be evaluated prior to the Faculty committing to the solution. To that end, solutions must be evaluated for the anticipated presence of Protected Data, and the solution proposal must receive risk management oversight adequate to the technical context in which the solution is expected to operate.

In addition, the committee will meet, as required, in the event of information-security related incidents.

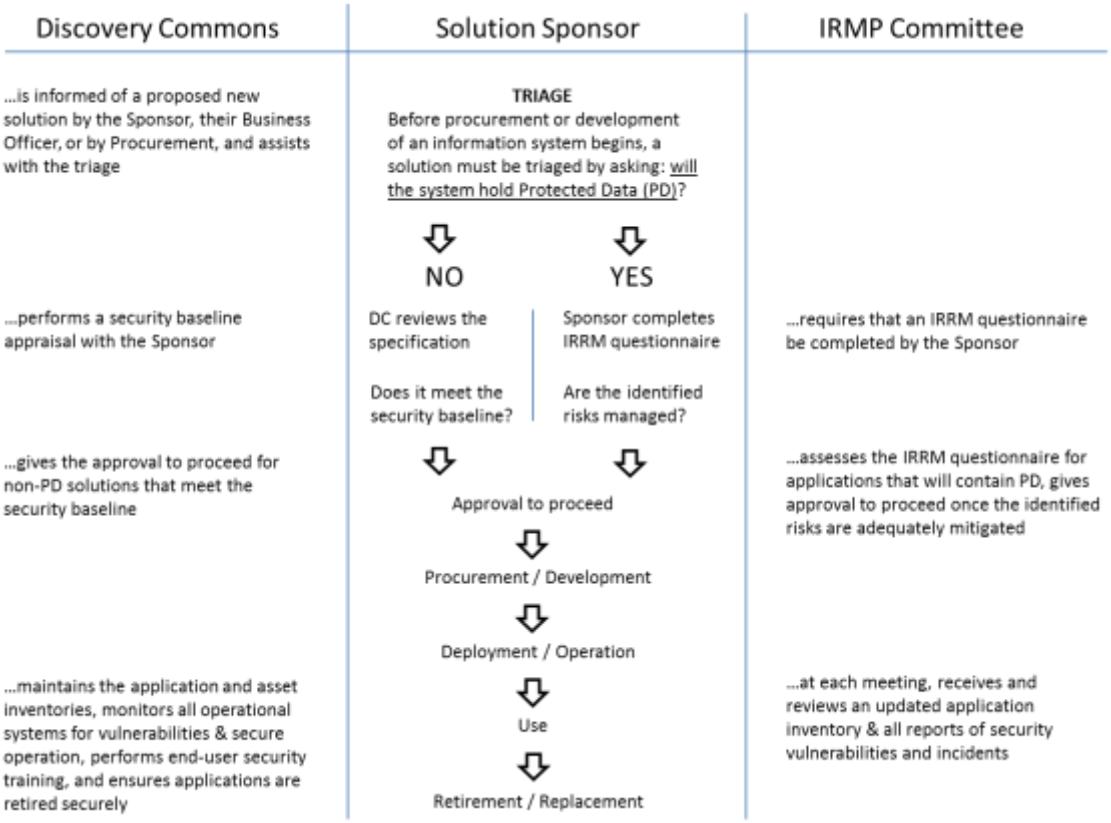
E. Roles & Responsibilities

A number of roles must be defined for every new (and existing) information solution:

- SPONSOR - The Sponsor is the business process owner; holds final accountability for management or acceptance of all security and risk issues related to the solution; is responsible for articulating how the information solution satisfies business needs, development and operational budget, and integration with existing business processes and information systems; and is responsible for defining business rules associated with the use of the information solution.
- STEWARD - During procurement or development, and once the solution is in operation, the Steward is responsible for ensuring, from the business (non-technical) perspective, that the information solution is compliant with Information Risk Management processes, and is accountable to the Sponsor for the ongoing management of information risk.
- CUSTODIAN - The Custodian is the IT unit or vendor responsible for providing technical services related to the deployment and operation of the solution, and executing the technical aspects of the solution's business continuity plan. The Custodian is accountable to the Sponsor/Steward for meeting the documented requirements for the application.

In some cases the Sponsor and Steward may be the same person (and in a very few cases may even be the Custodian as well), but in most cases at the Faculty these roles are played by different people.

The Sponsor (or Steward) of a solution, the IRMP Committee, and the Faculty's IT support unit (the Discovery Commons) have different responsibilities for information risk management during the information system lifecycle, as outlined below:



These hypothetical examples will help to show how this process will work:

1. NO PROTECTED DATA - A faculty member, in her role as a Principal Investigator (PI) in a research lab, wishes to implement a web-based system to keep track of the usage schedules for high-demand laboratory equipment. A graduate student has offered to develop the system using open source technologies. The PI (the Sponsor) discusses the project with the department's business officer (the Steward), and they determine that this system will not contain any Protected Data. (**Answer = NO to the triage question on the chart.**) The business officer then sends the project proposal to Discovery Commons, who provide feedback on how the proposed solution can, with a few changes, be made fully consistent with the University's information security baseline. The graduate student (the Custodian) agrees that the proposed changes are possible, so the PI gives approval to proceed with development.

2. PROTECTED DATA - A professional staff member who organizes a number of academic conferences every year wishes to create a web-based system to support event registration and fee payment. He has talked to a local software development company, which has provided a quote for developing and

hosting such a system, but then realizes that this system will contain Protected Data, such as personal information and payment card information. (**Answer = YES to the triage question on the chart.**) So, the staff member (the Steward) completes an IRRM questionnaire, gets the Chair's approval (the Sponsor), and submits it to the IRMP Committee. Due to the very high level of risk posed by setting up a new online payment system, the IRMP Committee recommends that an existing event registration system be used instead—either a Faculty or a commercial service (the Custodian). The staff member opts for a well-known Canada-based commercial service, completes an IRRM questionnaire for it, and receives the approval of the IRMP Committee to proceed.

F. The Information System Lifecycle

The Information System Lifecycle consists of four discreet stages through which an information solution passes: procurement/development, deployment/operation, use, and retirement/replacement. At each stage there are a number of applicable controls and risk management strategies which can be applied to ensure that information security risks are adequately mitigated.

1. Procurement / Development

Risk Management and Business Continuity requirements must be defined in advance of solution procurement or development, as they inform the core functional risk-management requirements that the solution must satisfy. The Faculty will work to find ways to identify and analyze new information solutions as early as possible, through coordination with business officers and with Central Procurement.

The first question that should be asked regarding a new information solution – including information risk management solutions – is whether the solution already exists within the University environment. Business units are strongly encouraged to take advantage of existing, sufficiently secure options before acquiring or developing new solutions.

Before undertaking the process of solution procurement or development, the Sensitivity of information within the solution must be articulated (Protected, Confidential, or Public). Data sensitivity and business continuity requirements define the measures over and above the University's Information Security Baseline necessary to acceptably manage risk.

A Records Retention Schedule based on business needs and data sensitivity must also be established in advance of solution procurement or development, as must be the assignment of roles and responsibilities for information security and risk management. The Records Retention Schedule will define how long data within the solution (including, but not limited to: 'live' data, data backups, metadata, and log data) must be retained and how it must be disposed of.

Solutions must be evaluated for their ability to minimize the introduction of risk into the University environment. To that end, an Information Risk and Risk Management assessment questionnaire (IRRM) must be completed by the Solution Sponsor, or their designate, and assessed by the IRMP Committee, for any solution that will hold Protected Data, or that has the

potential to introduce previously un-evaluated risks (i.e. new threats, new vulnerabilities / technologies, contractual terms / terms of use, or asset types) into the University environment. The IRRM process involves identifying new risks to be introduced, and applying risk management practices and controls appropriate to the type of information solution proposed, drawing on the University's Information Security Baseline as a starting point.

When committing to use external ("cloud" or otherwise externally hosted) information services, matters of data custodianship must be clearly stated in the contract, including, but not limited to: use of data; ownership of data; ability to terminate services and extract University data at will; corporate branding, representation, and advertising based on University data / relationship with the University. Proposed contracts must be vetted as part of the IRRM process, as the contract will serve as a record of the vendor's commitment to protect the University's data.

2. Deployment / Operation

Information solutions must be deployed and operated so that they do not introduce risk into the University environment either through misconfiguration, insecure operation, failure to prepare for recovery from incidents, or failure to protect data when hardware is disposed of / hosting agreements are terminated.

Business Continuity Practices (BCP) must integrate with deployment and daily operation practices in order to prepare responses to known accepted risks, and unknown risks. Part of the BCP process must include a review of incident response so that solution risk assessments can be updated to reflect previously unknown risks, and BCP processes can be improved upon by lessons learned during incident response.

Deployment and operation of information solutions must be done in such a way as to keep 'live' or 'production' data separate from test and development environments. Test and development environments, which are typically less secure than full production environments, must use synthesized data for pre-production work as even data believed to be fully anonymized can reveal personal information. As well, all changes must be successfully tested in an isolated environment before being promoted to production. Deployment of solutions to production and other major changes to information solutions must involve the creation / update of BCP documentation and test practices.

Information solutions must be subject to fitness testing performed annually, and after a major changes / upgrades of key components. This fitness testing must include practice of BCP measures (including, but not limited to system restore / recovery from backup, and operation from geographically remote sites, if applicable) and external functional security control testing to ensure the accuracy / effectiveness of BCP and risk management services and procedures.

3. Use

Use of information solutions must include risk-reduction guidelines for end-users beyond the Provost's guideline for Appropriate Use of Information and Communication Technology as required. This may include the introduction of formalized access control procedures, end-user education programs, improvements to the security of end-user computing equipment (including, but not limited to: device encryption and remote device management), network and remote access controls, and other such risk-management techniques.

4. Retirement / Replacement

As information solutions typically represent multiple repositories of sensitive information (including, but not limited to: 'live' data, backup data, databases, metadata, and log data), care must be taken in the disposal of such solutions to ensure that this data is preserved only in controlled backups, and only for the duration specified by the records retention schedule.

Data stored within old solutions must be consciously and deliberately destroyed if solution components are re-used, recycled, or leave the Faculty's possession.

The selection of a solution replacement must go through the same process as that for solution procurement / development, and must focus on meeting or exceeding current threat techniques and technology, reflecting current threats, vulnerabilities, and existing enterprise solutions.

As risks and risk management strategies evolve with time, it is expected that solutions being replaced were acquired under less stringent risk management conditions; as such, it is anticipated that new solutions will always represent an advance in risk management practices and technologies over older, less robust, solutions.

G. University Guidelines

The Information Security and Enterprise Architecture (ISEA) office maintains a website on which it publishes the University's current Information Risk Management guidelines. These guidelines include tools and processes to evaluate new information services and solutions for risk exposure; to guide their selection or development so as to deliberately manage risk; to deploy, operate and use these services and solutions so as to manage the risk they may introduce to the University environment; and to retire or replace these services and / or solutions in such a way as to manage the University's exposure to risk.

In particular, on this site can be found the current Information Risk and Risk Management assessment questionnaire, or IRRM (entitled the "Privacy and Risk Assessment Questionnaire" on the page) and the University's Security Baseline (part of the Information Security Guidelines document).

http://main.its.utoronto.ca/its-units/isea/practices-guidelines/

Discovery Commons maintains a website primarily containing IT security materials for end users.

http://dc.med.utoronto.ca/

Appendix A – Information Technology Security Principles

Faculty of Medicine
Information Technology Security Principles

Goals and Expectations

The Faculty of Medicine (the Faculty) recognizes and accepts that it has a responsibility to ensure the security of the information technology (computers, networks, and applications) and information that is under its direct care and control, with a particular responsibility for the protection of confidential information. The Faculty's goal is to ensure that the security measures in place are consistent, auditable, current, reasonable, and aligned with its business objectives.

The Faculty also recognizes that in any information technology there will always be vulnerabilities and the potential for outages or breaches. We cannot eliminate vulnerabilities, but we can ensure there is a process in place to consciously and proactively identify them, and that we have plans to address them.

To this end, the Faculty is establishing an Information Risk Management Program (IRMP), so that its information assets, and their supporting environment, may be protected from threats to their confidentiality, integrity, and availability. The IRMP includes a governance framework for managing how the Faculty identifies and responds to risk, for applying risk management strategies at each stage of the information solution lifecycle, and for establishing procedures for resolving outages, breaches, and new vulnerabilities in a responsible and timely manner.

Responsibilities

Information security at the University of Toronto is the responsibility of the Information Security and Enterprise Architecture (ISEA) group of the central Information and Technology Services (ITS) portfolio. Information technology security within the Faculty is primarily the responsibility of its IT support unit, the Discovery Commons, under the direct management of the Director of Information Technology, and within the portfolio of the Chief Administrative Officer (CAO).

All staff, faculty members, and students in the Faculty have a responsibility to comply with all relevant end-user IT security guidelines and recommended security practices. This information can be found on the Discovery Commons website. The Faculty is committed to continuing its program of user education regarding IT security issues.

More specifically, IT staff within Discovery Commons or elsewhere in the Faculty are required to comply with all applicable University IT security policies and guidelines, as documented on the Information Security and Enterprise Architecture (ISEA) office website.

The Faculty retains accountability for the confidentiality, integrity, and availability of its information. The Information Risk Management Program will, therefore, involve business owners, as well as Discovery Commons and ISEA, in the identification and management of information risk.

Page 1 August 2014

Information Risk Management Program

The Faculty of Medicine is partnering with ITS to create an Information Risk Management Program for the Faculty that will: identify the sensitivity of information assets within the Faculty, create physical and online environments to securely accommodate those assets in proportion to their sensitivity, establish metrics for the measurement of asset security, and establish governance processes and a governance body to ensure asset security remains current and effective throughout the information systems lifecycle, and across the Faculty. The IRMP is described in more detail in the document entitled *Faculty of Medicine Information Risk Management Program*.

Types of Information

The Information Risk Management Program is focused on those systems and applications containing "Protected Data" (PD), which is defined as including the following Confidential information: Personal Information (PI), Personal Health Information (PHI), Payment Card Information (PCI), IT-administrator level access to information and information solutions / infrastructure (IT-ADMIN), and externally regulated data. This list may be subject to revision as sensitive data classes are identified. Protected Data is currently the highest data sensitivity classification at the University of Toronto, the others being "Public" (data that is made available without requiring authentication) and "Confidential" (data that is neither Public nor Protected, and makes up the majority of data held by the University).

Specifically regarding the storage and use of Personal Information, the Faculty will comply with the Freedom of Information and Protection of Privacy Act (FIPPA), including limiting collection, and use and disclosure of personal information for necessary legally authorized purposes. The management of personal information by the University is performed under the terms of the University's Notice of Collection, available on the Freedom of Information and Protection Of Privacy (FIPP) Office website.

Specifically regarding the storage and use of Personal Health Information, the Faculty's position is that PHI must not be stored on or transferred through any of the computers, networks, or applications that are under its care and control, even in encrypted form. Because alternative clinically-secure systems are available to learners and faculty members, the Faculty disclaims any responsibility for an individual's unauthorized storage of PHI on a University or Faculty system.

Specifically regarding the storage and use of Payment Card Information or IT-Administrator level access to information and information solutions / infrastructure, the Faculty will comply with the technical requirements set out in the 'Information Security Baseline' document on the ISEA web site.

Contacts

For more information about the Faculty of Medicine's IT Security Principles or IRMP, please contact the Director of IT at 416-946-8625, or by email at discovery.commons@utoronto.ca. For more information about the University's IT security policies and programs, contact the Director, Information Security and Enterprise Architecture, at 416-978-7092, or by email at security.admin@utoronto.ca.