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:

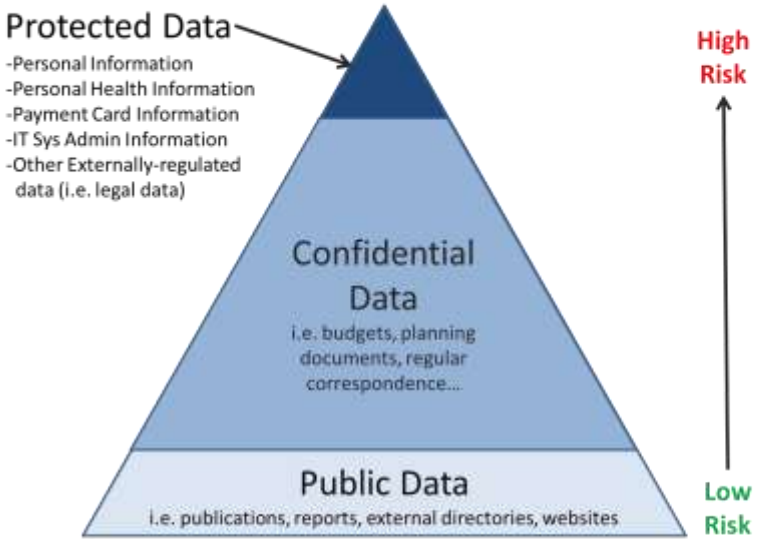
- Personal Information
- Personal Health Information
- Payment Card Information
- IT System Administrator access to information and information solutions / infrastructure (such as root or administrator passwords)
- Other data with externally-regulated protection requirements (such as legal data)

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.


Protected Data
-Personal Information
-Personal Health Information
-Payment Card Information
-IT Sys Admin Information
-Other Externally-regulated data (i.e. legal data)
Confidential Data
i.e. budgets, planning documents, regular correspondence...
Public Data
i.e. publications, reports, external directories, websites
High Risk
Low 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.

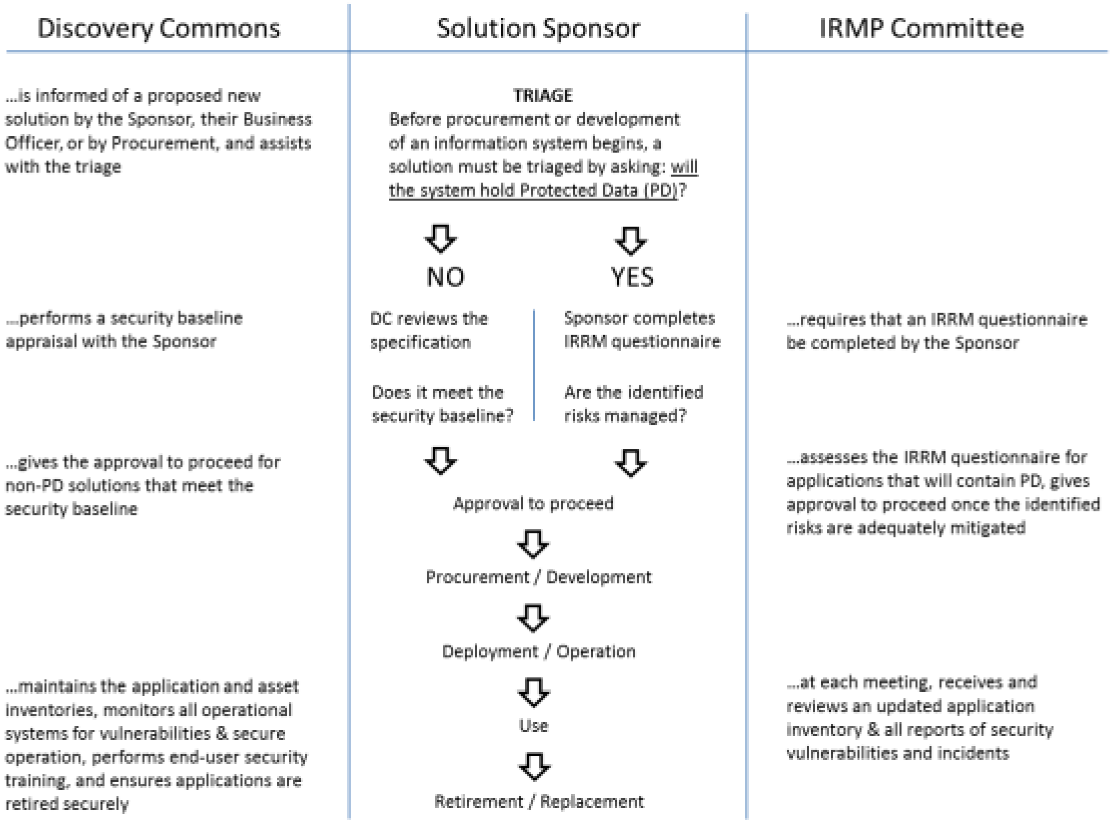
E. Roles & Responsibilities

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:



Discovery Commons
Solution Sponsor
IRMP Committee
...is informed of a proposed new solution by the Sponsor, their Business Officer, or by Procurement, and assists with the triage
TRIAGE
Before procurement or development of an information system begins, a solution must be triaged by asking: will the system hold Protected Data (PD)?
NO
YES
...performs a security baseline appraisal with the Sponsor
DC reviews the specification
Does it meet the security baseline?
Sponsor completes IRRM questionnaire
Are the identified risks managed?
...requires that an IRRM questionnaire be completed by the Sponsor
...gives the approval to proceed for non-PD solutions that meet the security baseline
Approval to proceed
...assesses the IRRM questionnaire for applications that will contain PD, gives approval to proceed once the identified risks are adequately mitigated
Procurement / Development
Deployment / Operation
...maintains the application and asset inventories, monitors all operational systems for vulnerabilities & secure operation, performs end-user security training, and ensures applications are retired securely
Use
...at each meeting, receives and reviews an updated application inventory & all reports of security vulnerabilities and incidents
Retirement / Replacement

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).

Best Practices & Guidelines

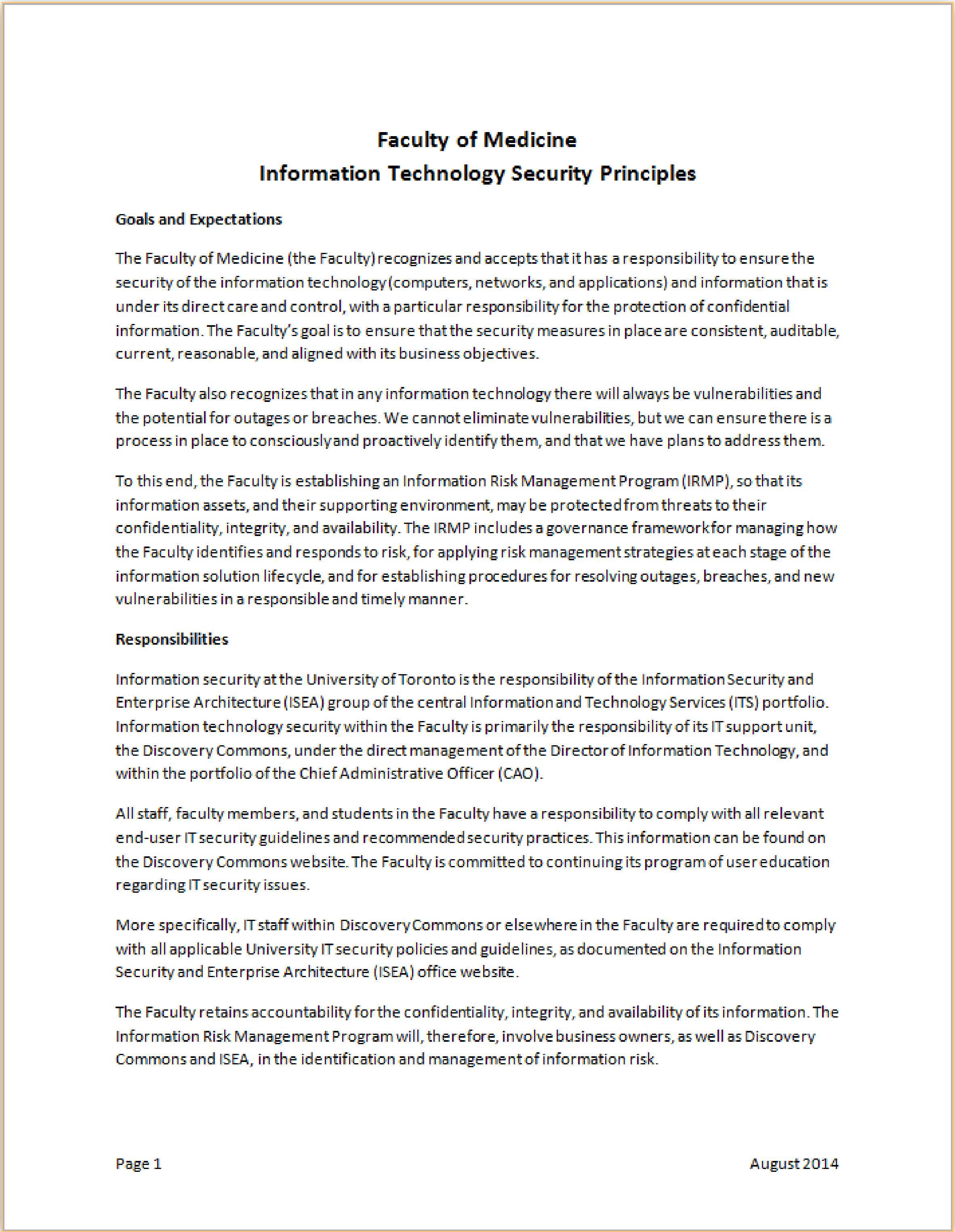
- Information Security Guidelines
- Security Guidelines for Printers and Photocopiers
- Guidelines for Securing Smart Phones & Tablets
- IT Security Incident Reporting Protocol
- Best practices for Phishing Prevention
- Information Risk and Risk Management Assessment Template
- Privacy and Risk Assessment Questionnaire (UofT)

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

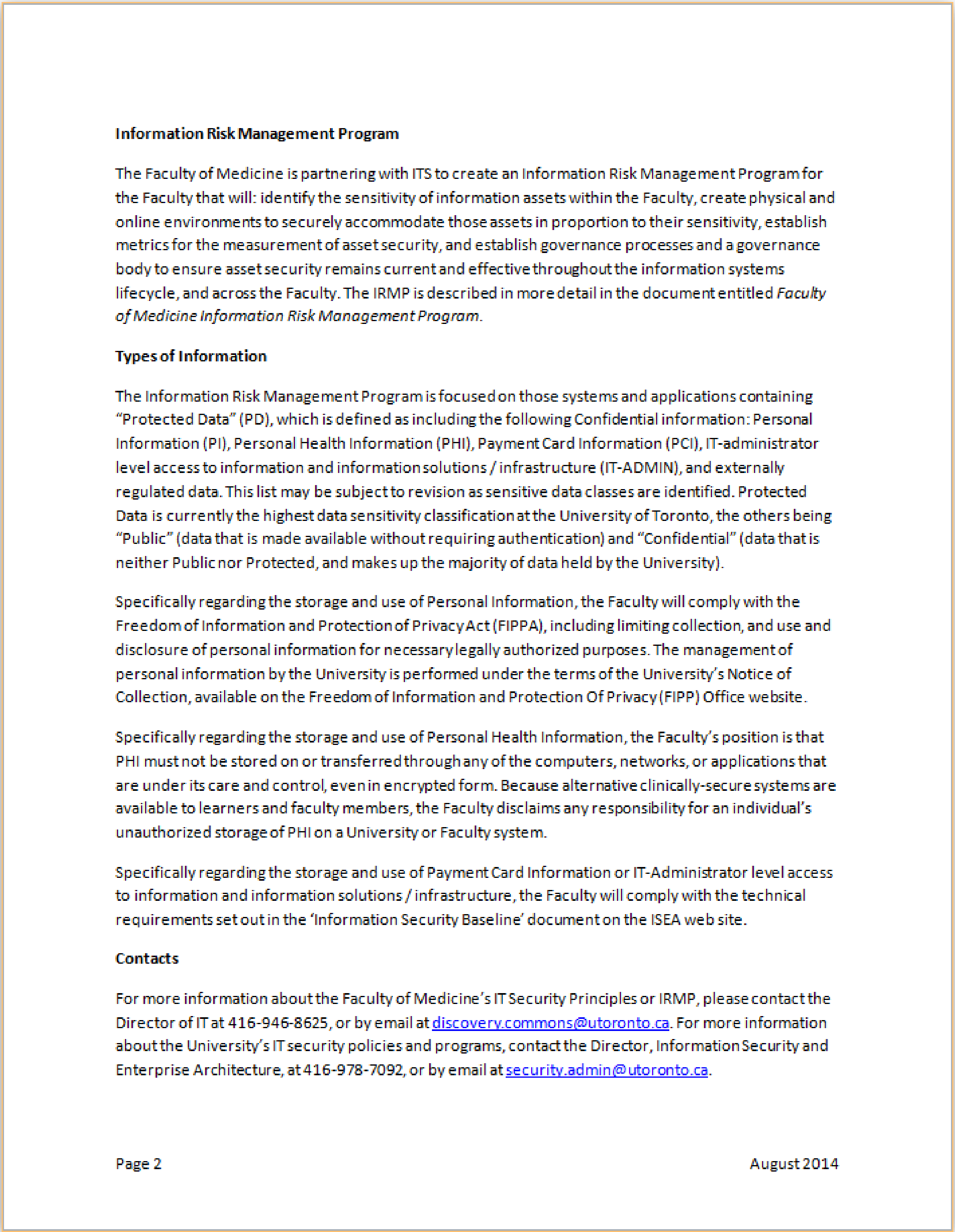
Information security at the University of Toronto is the responsibility of the Information Security and Enterprise Architecture (ISEA) group of the central Information and Technology Services (ITS) portfolio. Information technology security within the Faculty is primarily the responsibility of its IT 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.