DRAFT DOCUMENT

Proposed Policy on Cyber Risk Mitigation v17

PREAMBLE

Cyber Risks to the University are proliferating and our community faces an expanding array of threats to information security from an increasingly connected world. Cyber security incidents and threats demonstrate a growing technical sophistication and acceleration that have substantially raised the risk profile of essential University information and technology systems. These risks are particularly significant since cyber attacks come increasingly from organized criminal enterprises, corporate interests, or government agencies. Escalation of these risks seems likely as networks connect more types of devices that make more desirable targets for malicious activities.

This rise in cyber security risks joins the physical risks to information security – machine failure, loss of connectivity, power loss, damage to data centres, human-error. Loss of irreplaceable data from these risks or long system recovery times may cause highly detrimental consequences to the work of faculty, students and staff.

Computing devices – such as servers that are a primary target for cyber attacks, or mobile devices that are transient, easy to lose, and have capacity to readily access and store University data – increase Cyber Risk as they add potential entry points and vulnerabilities to the University's networks, applications and data. Applications, hosted on mainframes or servers, internally or externally, and that run on personal computers and mobile devices, owned by the University or individuals in our community, constitute additional channels for cyber security risk as they may be compromised through phishing, viruses, and other forms of malicious activity.

All these windows into the University's information ecosystem must be physically secured, patched, maintained, and monitored to limit or prevent malicious activity. Compromised devices or applications may be used for malicious activity inside the institution's network in ways that may disrupt the work of other units or be leveraged to propagate attacks. Actions that reduce exposure to risk by implementing standards for securing devices, and reducing the overall target footprint, physical and logical, are important objectives of the Cyber Risk Mitigation policy.

This policy aims to ensure that the University community recognizes and acts to protect against Cyber Risks when procuring and implementing information technologies. The policy prompts for the development of procedures to formally review and document units' Cyber Risk mitigation approaches and responsibilities. It ensures that the collective risks for information technology are understood, mitigated, and managed. When fully implemented, this policy will ensure that

For Discussion

DRAFT DOCUMENT

appropriate leaders within the University have reviewed and approved the balance between Cyber Risk mitigation and residual risk for every unit of the institution.

The University has made substantial investments within the CIO portfolio and across the institution to establish physically and logically secured facilities (e.g., data centres), with virtual servers and storage clusters, backup and recovery services, business continuity capabilities and processes, and professional staff with expertise in cyber security to support the community's common IT needs. These services and resources are key instruments in the University's response to the cyber risks we collectively face.

For Discussion

DRAFT DOCUMENT

DRAFT PROPOSED POLICY

The University of Toronto adopts this Cyber Risk Mitigation policy as a measure to protect the confidentiality, integrity, availability and accountability for institutional data as well as the information systems that store, process or transmit institutional data. This policy applies to all academic and administrative units, and 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 organizational units, will deploy and use IT systems and services in ways that vigilantly mitigate cyber security risks to IT devices and data during creation, storage, transit, use and disposal. It is the obligation of all community members to protect information created by its members and stored by the University and its authorized delegates to its defined standards.

1. *As the senior officer charged with the responsibility for the university's facilities, information technology, and ongoing operations, the Vice-President, University Operations (VPUO) shall have the responsibility for protection of the institution's digital information assets and systems. The VPUO is authorized to establish appropriate guidelines and procedures to achieve that goal.*
2. *Unit heads (vice-presidents/deans/chairs/department heads) shall be responsible for cyber risk mitigation within their units in accordance with institutional guidelines.*
3. *Under the direction of the Chief Information Officer, Information and Technology Services shall implement initiatives to manage cyber security risks for digital information assets and systems; operate facilities and offer services that maximize security; and provide guidance and develop university standards for protecting data, devices and facilities in use across the University. Information Technology committees, with senior representation from the University's academic and administrative divisions, shall provide advice to the CIO with respect to the University's protection of digital information assets and systems.*
4. *Across the University, those charged with managing and securing data shall operate in a manner that reduces and mitigates Cyber Risk vulnerabilities by using secure facilities and standardized procedures for protecting the University's digital assets and systems. Facilities and services that operate at university-wide, divisional and departmental levels shall meet institutional standards.*

For Discussion

DRAFT DOCUMENT

Proposed Implementation

The Cyber Risk Mitigation policy requires Information & Technology Services to develop and implement standards and procedures to manage security risks to digital information assets and systems. The plan for implementation of the policy will be developed with advice from IT service providers distributed across the University. The implementation plan will acknowledge the diversity of objectives, activities, and infrastructure that exist across divisions and departments.

The Cyber Risk Mitigation policy implementation plan will:

1. Establish a set of common standards and processes for managing cyber risks.
2. Establish a process, common across University divisions and departments, for identifying risks, developing an appropriate risk management plan, and implementing that plan at the divisional or departmental level.

Each risk management plan will include risk identification and assessment, and plans for risk mitigation, implementation, and demonstration of compliance.

As the risks associated with data, information services and infrastructure found in academic and administrative units vary greatly, it is recognized that requirements will reflect that diversity; one risk management solution will not fit all. However, to ensure a rigorous investigation of and response to cyber risk across the University, it is expected that all departments and divisions will complete a common process. ITS' Information Security group (ISEA) and the faculties of Law and Medicine have recently completed risk analysis exercises that will contribute to development of a standard model.

It is anticipated that the common process will include the following standards and procedures for identifying and managing risk:

1. Units will inventory their existing IT hardware, software, networks, technology management and business processes to establish a risk inventory.

2. As not all data and services are equally sensitive, units will align security efforts to a data sensitivity assessment.

3. Units will align their efforts to meet or exceed the minimum expectations of the information security guidelines published by ISEA.

4. Units will document the physical and logical location of sensitive data assets to aid in incident response.

5. Identify opportunities to meet requirements through use of secure resources and services provided by ITS.

For Discussion

DRAFT DOCUMENT

6. Identify appropriately secure solutions, in compliance with university standards, that are or would be implemented for resources retained at the local level.

7. Identify a timeline for implementation of the plan.

8. A process will be identified so that as new services and systems are planned, they will be evaluated for privacy and security risks using the common standards. Units will ensure sensitive information solutions are managed post-selection, to ensure that risk is not introduced in the development, implementation, operation, administration, and retirement phases of the solution lifecycle.

In support of these distributed efforts, ITS and ISEA will:

- Operate facilities and offer services to divisions and departments that maximize security and support their required information technology requirements. Where it is necessary to pass specific costs to an organizational unit, the rates will reflect the lesser of (a) the actual, scaled cost for the provided service or (b) the full cost of a highly comparable service in the marketplace.
- Develop institutional risk management standards in consultation with distributed IT services providers across the University, and review and revise them as required to address changes in threats, technology, and best practices in risk management.
- Provide guidance and support to divisions and departments in the development of their local risk management plans.
- Broadly and continually engage with organizational units to enhance the evolution of facilities, systems, and services that best protect the University's digital information assets.

ISEA will solicit broad input from the University community to update its current information security baseline, and to revise the data classification schema to create a classification defining sensitive or 'protected' data that requires enhanced risk management.

Within one year of the publication of the common standards and process, all units will be expected to develop their initial local risk assessment and mitigation plan. The plan will be discussed and requires joint approval by the unit head (e.g., Principal, Dean, Chair or Vice-President) and the Chief Information Officer. The plan will identify those risks that are to be addressed through subscription to secure services offered by ITS. Where unique academic activity or other factors are present, unit heads may formally accept responsibility to meet university Cyber Risk mitigation standards through locally managed solutions, provided the plan

For Discussion

demonstrates establishment and maintenance of appropriate and adequate resources and expertise for risk mitigation, policy compliance, and quality management of IT services that remain at a campus, divisional or departmental level.

DRAFT DOCUMENT

For Discussion