Proposed Policy on Cyber Risk Mitigation v8

BACKGROUND

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 organised 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.

Every additional physical computing device – particularly servers that are a primary target for cyber attacks – increases Cyber Risk as it adds a potential target and is another device that must be physically secured, powered, cooled, maintained, patched, and monitored for malicious activity. A compromised server in one unit may be used for malicious activity inside the institution's network in ways that may disrupt the work of other units. Reducing the number of physical computing devices while still achieving unit goals is one important approach for mitigating collective Cyber Risks.

The goal of this policy is to ensure that the University community minimizes to the greatest extent practicable the unnecessary creation of Cyber Risks while also enabling the productive work of all units. This requires us to balance actions that (a) create Cyber Risks and (b) can help mitigate them. Both are essential to establish and maintain the diverse IT services required by the university's research, education, and service missions. The policy creates a framework and prompts the development of procedures to formally review and document units' Cyber Risk mitigation approaches and responsibilities.

The University has made substantial institutional investments in secure physical facilities (data centres), virtual processing and storage, backup and business continuity, IT infrastructure, core services, and professional staff with expertise in cyber security to support the community's common IT needs. These investments provide a primary opportunity to reduce cyber threats by having fewer physical devices as targets and fewer devices in less secure facilities. Thus, whenever practicable, establishing physical security for servers in a highly secure, 24 x 7 monitored, protected facility is an essential first step for risk mitigation. By increasing the risk profile, servers that operate outside of the institution's secure data centres increase reputational, financial, and data loss risks for the University and may contribute to other concerns about physical plant failures, inadequate redundancy, suboptimal system maintenance, duplication of services, and energy inefficiencies.

The policy recognises that unique needs for some faculty-led research and teaching (academic uses) or unique administrative uses may not be practicable within the common IT infrastructure and services provisioned by Information Technology Services. The use of robust campus, divisional or departmental IT providers is a secondary means to achieve the goal of this policy.

The policy creates a framework to further the University's organizational partnerships for vigilant efforts to manage and mitigate Cyber Risks for the entire University. It ensures that the collective risks for information technology are understood, mitigated, and managed. When fully implemented, this policy will ensure that appropriate leaders within the University have reviewed and approved the existing balance between Cyber Risk mitigation and residual risk for every unit of the institution.

PROPOSED POLICY

The University of Toronto adopts this Cyber Risk Mitigation policy as a measure to protect the confidentiality, integrity and availability of 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.

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) or other designate of the President, shall have the responsibility for protection of the institution's digital information assets and systems. The Vice-President UO, or other designate of the President, is authorised to establish appropriate guidelines and procedures to achieve that goal.*
2. *In order to ensure broad consultation in planning and decision-making processes, Information Technology committees, with senior representation from the University's academic and administrative divisions, shall provide advice to the VPUO with respect to the University's protection of digital information assets and systems.*
3. *Under the direction of the Chief Information Officer, Information and Technology Services is responsible for minimizing cyber security risks for digital information assets and systems, operating IT facilities that maximize physical security, and providing protection from natural disasters. ITS is also responsible for provisioning a set of information technology infrastructure and services that meet the common, evolving needs of all campuses and units.*
4. *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, maximize physical security for IT systems, and minimize unacceptable risks to IT systems and data (collectively, "Cyber Risks").*

    a. *The optimal approach for reducing and mitigating Cyber Risks is for units to use the secure facilities, common information technology infrastructure, and services provided by ITS to the greatest extent practicable for achieving their work.*

    b. *To the extent that the optimal approach is not practicable for achieving a unit's work, the alternative is for campus, divisional or departmental IT providers to formally assume information security responsibilities, and demonstrate their ability to maintain, on an ongoing basis, security standards established by the ITS Information Security department.*

Proposed Implementation Procedures

Information Technology Services (ITS)

ITS is responsible for maintaining secure facilities; provisioning high-quality, secure, and reliable information technology infrastructure; and providing common services with ample capacity and commensurate technical and user support. In particular ITS will:

- Provide secured facilities and resources to divisions and departments that allow them to achieve 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.
- Provide assistance to units for analysing their information technology requirements, in the context of current and planned ITS common services.
- Provide assistance to units that wish to increase their use of ITS services, or wish to increase the security of divisional or departmental IT services.
- 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.

Campuses, divisions, departments and other organizational units

Within one year of the adoption of this policy, all units will perform an initial, comprehensive evaluation of their information technology needs relative to the requirements of this policy. Following that review, organizational units will:

- Identify any unit-level systems and services that could be served by ITS, and those that must be maintained at a campus, divisional or departmental level.
- Develop a plan for policy compliance with target dates agreed to by the unit head.
- Prepare a formal risk assessment and risk mitigation plan to be discussed and approved jointly by the unit head (e.g., Principal, Dean, Chair or Vice-President) and the Chief Information Officer, including establishment and maintenance of appropriate capacity and expertise for risk mitigation, policy compliance, and quality management of all IT services that remain at a campus, divisional or departmental level.

(Academic uses of systems, software, and services for research and education merit especially broad faculty discretion in how to best achieve these critical parts of the University's mission. In support of this discretion, heads of academic units may formally choose to take responsibility for broad categories of academic uses by providing sufficient resources for divisional or departmental Cyber Risk mitigation vigilance.)