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

Background

Risks to the University's Digital Assets 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 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 digital 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 attack, or mobile devices that are transient, easy to lose, and have capacity to readily access and store University data – increase risk to information security, 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 Policy on Information Security and the Protection of Digital Assets.

This policy aims to ensure that the University community recognizes and acts to protect against information security risks when procuring and implementing information technologies. The policy prompts for the development of procedures to formally review and document units' Digital Asset 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 appropriate leaders within the University have reviewed and approved the balance between Digital Asset 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 in divisions and departments 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 information security to support the community's common IT needs. These services and resources are key instruments in the University's response to the risks to Digital Assets that we collectively face.