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

3rd Consultation Draft – 17 February 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 confidentiality, integrity and availability of Digital Assets including the 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 ways that vigilantly mitigate security risks to Digital Assets, including data during 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 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 using secure facilities, Standards and Procedures for protecting the University's Digital Assets. Facilities and services that operate at University-wide, divisional and departmental levels shall meet these requirements.

Administrative Authority

The Vice-President University Operations shall have overarching operational responsibility for the protection of the University's Digital Assets. The VPUO or designate is authorized to establish, Procedures, Standards and Guidelines for the protection of the University's Digital Assets.

Unit heads (vice-presidents/deans/chairs/department heads) shall be responsible for assuring the protection of Digital Assets within their units in accordance with the Policy and associated Procedures, Standards and Guidelines.

In support of these shared responsibilities, each unit shall develop an Information Risk Management Program appropriate to the circumstances of the unit and jointly approved by the unit head and the VPUO or designate.

In order to ensure broad consultation in planning and decision making processes, an **Information Security Council** with broad representation from divisions and departments will be established by the VPUO or designate. The Council will advise on the development and revision of appropriate Procedures, Standards and Guidelines for protecting the University's Digital Assets. These Procedures, Standards and Guidelines will be reviewed regularly to reflect new and evolving technologies that are deployed across the University, as well as emerging threats to Information Security.

The VPUO or designate will provide regular updates to the Information Security Council on:

- Progress on developing and implementing Procedures, Standards and Guidelines in support of the Policy;
- Metrics demonstrating the effect of Procedures, Standards and Guidelines in support of the Policy;
- Significant security breaches and their remediation.

Governance Oversight

The Vice-President University Operations (VPUO) shall report annually to Governing Council via the Audit Committee.

Emergency Authority

In the event of an emergency situation that threatens the University's Digital Assets, the VPUO shall have full authority to enact emergency response measures that shut down the risk or mitigate further damage to Digital Assets and to protect the University community.

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.

Security of Digital Assets - Their confidentiality, integrity, availability, and accountability for use, in proportion to the University's sensitivity to their unauthorized disclosure, alteration, loss, or unrecorded access.

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 – Mandatory practises for protecting Digital Assets as developed through input from the Information Security Council and approved by the VPUO 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 VPUO 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.

Information Security Council – A group chartered by the VPUO or designate to regularly review threats to the University's Digital Assets, and to collaborate with the VPUO or designate to initiate information security initiatives, and develop Procedures, Standards and Guidelines for the protection of the University's Digital Assets.

Proposed Implementation

The goal of the proposed Policy on Information Security and the Protection of Digital Assets is to enhance security for the University's resources. Its achievement will require collaboration among interested and responsible members of the University community, drawing upon the expertise and experience distributed through campuses, divisions, departments and the shared services of the Information Security and Enterprise Architecture (ISEA) group.

To complement consultation and planning to date, the CIO will immediately commission an ad hoc Working Group on the Implementation of Information Risk Management Practice. Chaired jointly by the director of ISEA and a director of IT drawn from an academic division, and with members expert in information security operations drawn from across the University's campuses, divisions and departments, the Working Group will develop recommendations for the Procedures, Standards and Guidelines anticipated by the Policy. The Working Group will also provided detailed recommendations on the establishment of its successor, the ongoing Information Security Council anticipated by the Policy.

One of the key Procedures to be developed will be a standardized approach to planning Information Risk Management Programs in appropriate unit levels across the university. The Procedure must acknowledge the diversity of objectives, activities, and infrastructure that exist across academic and administrative units, the variety of risks, and the variation in the mitigation approaches that may be appropriate. One risk management program will not fit all units; but the Procedure will require all units to develop a circumstantially appropriate plan that will address risk identification and assessment, plans for risk mitigation, a local implementation plan, and demonstration of compliance.

More specifically, the common Procedure would likely include the following requirements for unit plans:

1. Local inventory of existing IT hardware, software, networks, technology management and business processes to establish a risk inventory.
2. Categorization of data using a sensitivity assessment.
3. Documenting the physical and logical location of sensitive data assets to aid in incident response.
4. An expectation to meet or exceed the minimum expectations of University Standards.
5. Adoption other Procedures and suggested Guidelines where appropriate
6. Identification of appropriately secure solutions, in compliance with University Standards
7. Identification of opportunities to meet requirements through the use of secure resources and services provided by ITS or other qualified providers.
8. Establishing a process to ensure that risk in services involving sensitive information is managed during all stages of the solution lifecycle, including design, development, implementation, operation, administration, and retirement.
9. Periodic reporting to ISEA on implementation of Standards and Procedures. To ensure as high a standard is maintained by centrally provided services, ISEA will periodically report to Internal Audit on ITS' implementation of the same Standards and Procedures.
10. Timeline for implementation of the plan.

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 information technology requirements.

- 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.

- Provide guidance and support to campuses, divisions and departments in the development of their local risk management plans.

Within one year of the publication of the common Standards and Procedures all units will be expected to develop their initial Information Risk Management Program.

The program will be discussed and require joint approval by the unit head (e.g., Principal, Dean, Chair or Vice-President) and the Chief Information Officer, acting as the VPUO's designate. Unit heads may accept responsibility to meet University Standards and Procedures through locally managed solutions that demonstrate adequate arrangements for risk mitigation, Policy compliance, and management of services that remain at the campus, divisional or departmental level. Alternatively, the program will identify those risks that are to be addressed through subscription to secure services offered by ITS or other qualified providers.

Background

Risks to 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.