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

Revision: November 10, 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 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 promote the University's research and teaching mission while vigilantly mitigating security risks to Digital Assets, including data during storage, transit, use and disposal. It is the obligation of all University community members to protect information that is created by them 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, Guidelines and Procedures for protecting the University's Digital Assets. Facilities, services, and systems that operate at University-wide, divisional and departmental levels shall meet these requirements.

Administrative Authority

The President or designate shall have overarching responsibility for the protection of the University's Digital Assets. The President or designate is authorized to approve Procedures and Standards and to promote Guidelines for the protection of the University's Digital Assets.

Academic and administrative unit heads shall be responsible for assuring the protection of Digital Assets within their units in accordance with this Policy and associated Procedures and Standards.

In order to ensure broad consultation in planning and decision making processes, an **Information Security Council** (ISC) will be established by the President or designate. The ISC is chartered to regularly review threats to the University's Digital Assets; to collaborate with the President or designate to initiate information security initiatives; and to recommend Procedures, Standards and Guidelines for the protection of the University's Digital Assets. The ISC will assist in the review of envisioned and unanticipated risks to information security and protection of Digital Assets. The composition of the ISC will be comprised of technical, administrative, and academic experts. The ISC will be chaired jointly by a senior faculty member and the director of the ITS Information Security department.

In support of these shared responsibilities, each unit shall in consultation with the ITS Information Security department, and others as appropriate, develop an Information Risk Management Program appropriate to the circumstances of the unit, to be approved by the unit head. The President or designate will review such plans to ensure compliance with this Policy and associated Procedures and Standards, each of which shall respect relevant University Policies and Agreements.

The Procedures, Standards and Guidelines shall ensure that the protection of Digital Assets is accomplished in a manner that is consistent with all relevant University Policies and Agreements, including those dealing with the protection of academic freedom.

The President 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 President or designate shall report annually to Governing Council via the Audit Committee and the Planning and Budget Committee.

Emergency Authority

In the event of an emergency situation that threatens the University's Digital Assets, the President or designate shall have full authority to enact emergency response measures that shut down the risk or mitigate further damage to Digital Assets and protect the University community. Actions taken by the President or designate under this Emergency Authority shall be reported to the Information Security Council and in the President or designate's annual report to Governing Council via the Audit Committee. Those affected by such actions under this Emergency Authority shall be notified as soon as practicable before or after such actions are taken.

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. Digital Assets can include, among other things, information protected by academic freedom, personal information, proprietary information, and confidential information.

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