UNIVERSITY OF TORONTO

OFFICE OF THE GOVERNING COUNCIL

The following context from the Governing Council Governance cover sheet may be helpful in reviewing the latest version of the draft proposed Policy.

HIGHLIGHTS:

Background

This Policy is designed to enhance the level of security protecting the information that is generated, processed, used and stored electronically at the University. Such "Digital Assets" (defined in the proposed Policy) exist in widely distributed electronic information systems that address University-wide, divisional and local needs.

The Policy is intended to provide a framework within which central Information Technology Services (ITS) and central and academic divisions will develop and implement their own plans for information security and the protection of Digital Assets. The proposed Policy addresses the establishment of Standards, as well as Procedures and Guidelines to ensure those Standards are maintained. The Policy will not impinge on divisional discretion when it comes to Information Technology (IT) services and activities, provided such Standards are met. In addition, it explicitly acknowledges that some of the information generated, processed, used and stored is protected by academic freedom, is personal information, is proprietary information, is confidential, or that otherwise has elements that, pursuant to other University policies and agreements, may require special treatment.

Current Risk and Need

U of T's decentralized IT structure offers flexibility to its faculty members and units in designing their own IT solutions to fit local research and teaching needs. Given the nature of University work, its network is very open, with the potential of presenting 393,000 publicly addressable devices to the world, whereas most private sector institutions might present only a handful. Information and Digital Assets generated by the University's faculty, staff, and students are housed in many places – for example, on the University's networks and servers and on University systems like Blackboard and ROSI; as well as on cloud platforms like Dropbox, on mobile devices, on individual personal computers, and elsewhere.

Information and Digital Assets at U of T are subject to risk on many fronts – for example, an unencrypted personal computer or tablet with research data that is lost on the subway could lead to a major data breach, or a hacker intentionally targeting one of the University's servers could expose personal student information. Risks of this nature are not merely hypothetical. Because of its extensive research and teaching activity, the University faces persistent attacks against our networks. There have been data vulnerabilities at the University that could have had serious ramifications in terms of exposure of personal information and private data had they not been controlled and secured quickly.

The risk currently faced by the University is similar to that which is faced by other public-sector and private-sector organizations, but it has an added dimension – resulting in the potential for additional risk – in the highly distributed nature of the University's computing resources. Many peer institutions have policies like the proposed one in order to deal with securing information, including personal and private information, and to help prevent data breaches. In formulating this Policy, the University has drawn on the experience of these peer institutions. This rapidly evolving and technical area has been identified – both internally at the University through the Audit Committee and elsewhere, and by external entities such as the Ontario Information and Privacy Commissioner – as being extremely important if privacy and security are to be maintained.

Highlights

Some key elements of the Policy are as follows:

- A statement of the importance of protection of the University's Digital Assets
- The requirement that every academic and administrative unit develop a risk management plan to promote information security and the protection of Digital Assets.
- The establishment of a consultative framework for continuous improvement in identifying minimum security Standards and related Procedures for University-wide application
- A stated commitment to academic freedom
- Provision for limited emergency authority, subject to review
- Naming of the President or designate as the institutional authority for information security
- Affirmation that information security requirements shall align with all relevant University policies
- The establishment of an Information Security Council (ISC) to recommend University-wide Standards and Procedures, to be co-chaired a faculty member with academic expertise and the Director of the ITS Information Security department
- Reporting to governance through the Planning & Budget and Audit Committees

Consultation

The administration has engaged in eighteen months of broad consultation across the academic, administrative and IT staff communities of the University. Consultation included discussion with the Principals and Deans group, with standing IT committees such as the divisionally representative IT Leaders Forum, at various departmental meetings, in individual meetings with faculty members and departments, and at other venues. In addition, various drafts of the Policy were shared with the broader University community through the ITS Web site and the Info-Tech listserv.

The CIO assembled a Working Group on Information Risk Management Practice to set the foundation for the Policy's implementation alongside development and finalization of the Policy itself. The Working Group, co-chaired by Professor Ron Deibert and the Director of ITS Information Security, is developing recommendations for information risk management Procedures, Standards and Guidelines, and will also provide recommendations on the establishment of its successor, the ISC.

In spring 2015, the administration heard from faculty members and department Chairs in the Faculty of Arts & Science and the Faculty of Applied Science and Engineering with some concerns about the proposed Policy. Themes of the feedback primarily focused on:

- A desire for the University's commitment to academic freedom to be reflected in the Policy, particularly with regard to information and data related to research and teaching activities,
- The potential for increased centralization of IT resources and costs of implementation, and
- Questions about the membership and Terms of Reference of the ISC.

Over the course of summer 2015, the Provost, Vice-President University Operations, and Vice-President Research & Innovation met with faculty and staff from academic divisions to hear and respond to these concerns. A smaller ad hoc group was assembled, co-chaired by the Vice-President University Operations and Vice-President Research & Innovation, with membership from FAS, FASE, the Faculty of Information, the University of Toronto Mississauga, and other divisions, to offer further feedback on the Policy and its eventual implementation.

A letter from the University of Toronto Faculty Association (UTFA), dated October 20, 2015, also raised some concerns about aspects of the Policy, in line with other feedback received. The Provost has indicated that a joint working group with UTFA has been formed to examine the separate but related issue of privacy related to the electronic records of faculty and librarians.

The proposed Policy has been revised on several occasions in response to feedback received from these various sources. After significant revision to account for these community concerns, the administration believes that the proposed Policy addresses the important security and risk mitigation required for the protection of the University's essential research and teaching mission in a manner that is responsive to local academic and administrative needs, as well as to the various elements of University Policies and Agreements that may intersect.

Oversight

The Policy gives oversight for the Policy to Governing Council, requiring an annual report by the President or designate to its Planning and Budget Committee and the Audit Committee. Supporting the implementation of the Policy is a cascading set of responsibilities:

- The President or designate is responsible for information security and the protection of Digital Assets under the Policy and the establishment of Procedures and Standards to give effect to the Policy.
- The ISC recommends the Procedures and Standards to the President as well as gives input into the operation of the Policy, and in turn receives feedback and regular reports from the President regarding these matters. This feedback loop will enhance both effectiveness and transparency when it comes to assessing metrics of the Policy's implementation and actions related to security vulnerabilities and remediation.
- The ISC will be chaired jointly by a Faculty member and the director of the ITS Information Security department, and will be advisory to the President. This reflects the

desire for broad input from all relevant stakeholders as Standards and Procedures are developed.

The Policy acknowledges the President or designate's authority to take emergency steps to protect Digital Assets in the event of data breaches and similar emergency situations, but ensures transparency in requiring notification to those affected, and reporting in a variety of ways.

The Policy is explicit in stating that Procedures, Standards and Guidelines must be consistent with the University's mission and purpose, as well as all relevant University Policies and Agreements, including those dealing with the protection of academic freedom. These would include policies that confirm the University's obligations under Freedom of Information and Protection of Privacy Act (FIPPA) and other relevant legislation, as well as the Memorandum of Agreement with UTFA.

Implementation

After the Policy is approved by the Governing Council, an implementation phase will begin. The Policy requires that academic and administrative department heads remain responsible for assuring the protection of Digital Assets within their units. Each unit will be expected to develop its own Information Risk Management program that is appropriate to its own needs. (An example of a divisional implementation plan and Information Risk Management program from the Faculty of Medicine is attached.) The ITS Information Security department has indicated that it is pleased to assist units in this process and in the development of various training resources and compliance programs, as it did with the Faculty of Medicine.

A major element of the Policy's implementation is the establishment of the ISC and the setting of its terms of reference. The composition of the ISC will be appropriately representative of the various central and academic divisions as well as faculty, staff, and librarian stakeholders. There will be robust academic participation and consultation in the ongoing deliberations and work of the ISC.

The importance of divisional and local roles in exercising their own continuing discretion is emphasized in the Policy's requirements. The implementation of the Policy will preserve the flexibility that makes U of T's IT structure so distinctive while adding appropriate accountability mechanisms.