FOR INFORMATION **OPEN SESSION**

TO:	Planning and Budget Committee
SPONSOR:	Professor Scott Mabury, Vice-President, University Operations
CONTACT INFO:	416.978.2031, scott.mabury@utoronto.ca
PRESENTER:	As above
CONTACT INFO:	
DATE:	February 18, 2020 for February 25, 2020
AGENDA ITEM:	5

ITEM IDENTIFICATION:

Update to the Policy on Information Security and the Protection of Digital Assets.

JURISDICTIONAL INFORMATION:

The Committee is responsible for policy on a broad range of planning issue and priorities and the use of University resources. The is a proposed update to the *Policy on Information Security and the Protection of Digital Assets* reflecting the formation of the Information Security Council as informed by the Policy, and the appointment of an institutional Chief Information Security Officer (CISO).

GOVERNANCE PATH:

1. **Planning & Budget Committee [for information] – February 25, 2020.**
2. Audit Committee [for information] – March 4, 2020.
3. Academic Board [for information] – March 12, 2020
4. Executive Committee [for information] – March 24, 2020.
5. Governing Council [for information] – April 2, 2020.

PREVIOUS ACTION TAKEN:

The *Policy on Information Security and the Protection of Digital Assets* was approved by Governing Council on February 25, 2016.

HIGHLIGHTS:

Background
The *Policy on Information Security and the Protection of Digital Assets* was to be followed with the implementation of its recommendations, key among them, from the *Policy*:

> 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.

Further, the role of the ISC was intended to:

> [A]ssist in the review of envisioned and unanticipated risks to the University's Digital Assets; collaborate with the President or designate to initiate information security initiatives; educate the University community on digital security best practices; and develop and recommend Procedures, Standards and Guidelines for the protection of the University's Digital Assets.

The *Policy* referred to the President or Designate throughout. At the time, there was no clearly defined senior leadership role focused on Information Security and as such, the word "Designate" provided a placeholder until the appropriate role was created.

Pursuant to the *Policy*:

- The Information Security Council was founded and commenced operation on 5 February 2018;
- The University appointed its first Chief Information Security Officer in December 2018.

As a result, the following changes to the *Policy* are appropriate to reflect the changes in the organisation:

1. Where the phrase "*President or Designate*" appears in the *Policy*, it is to replaced with "*President or Designate (normally, the Chief Information Security Officer)*, or (normally, the CISO);
2. In the Definitions section, the *Policy* refers to to the Information Security Council co-chairs as follows:

   > The ISC will be co-chaired by a senior faculty member and the director of the ITS Information Security Department. The ISC will be comprised of technical, administrative and academic experts.

   Reflecting the appointment of the institutional Chief Information Security Officer:

   > "… the *director of the ITS Information Security Department*" is to be replaced with "*... the Chief Information Security Officer*"

FINANCIAL IMPLICATIONS:

There are no direct implications for the University's operating budget at this time. Specific implications will become known as the *Policy* is implemented across the University.

RECOMMENDATION:

For Information only.

DOCUMENTATION PROVIDED:

Policy on Information Security and the Protection of Digital Assets with proposed changes highlighted.

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

Revision: *March xx, 2020*

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 privacy, confidentiality, authenticity and 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 a manner consistent with 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 following Standards, Guidelines and Procedures for protecting the University's Digital Assets. Facilities, services, and systems that operate at University-wide, divisional and departmental levels will meet these requirements.

Administrative Authority

The President or designate *(normally, the Chief Information Security Officer, CISO)* shall have overarching responsibility for the protection of the University's Digital Assets. The President or designate *(normally, the CISO)* 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 *(normally, the CISO)*. The ISC will: assist in the review of envisioned and unanticipated risks to the University's Digital Assets; collaborate with the President or designate *(normally, the CISO)* to initiate information security initiatives; educate the University community on digital security best practices; and develop and recommend Procedures, Standards and Guidelines for the protection of the University's Digital Assets.

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 *(normally, the CISO)*, in collaboration with the ISC, will review such programs to ensure compliance with this Policy and associated Procedures and Standards.

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. The President or designate *(normally, the CISO)* will provide regular updates to the ISC about progress in developing and implementing Procedures, Standards and Guidelines in support of this Policy.

Governance Oversight

The President or designate *(normally, the CISO)* 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 *(normally, the CISO)* 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 *(normally, the CISO)* under this Emergency Authority shall be reported to the Information Security Council and in the President or designate's *(normally, the CISO)* 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.

Information Security Council (ISC) – The Information Security Council (ISC) is a committee established by the President or designate *(normally, the CISO)*. The ISC will be co-chaired by a senior faculty member and the *Chief Information Security Officer* ~~director of the ITS Information Security Department~~. The ISC will be comprised of technical, administrative and academic experts.

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 (normally, the CISO). (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 (normally, the CISO), 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.

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

Revision: *March xx, 2020*

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 privacy, confidentiality, authenticity and 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 a manner consistent with 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 following Standards, Guidelines and Procedures for protecting the University's Digital Assets. Facilities, services, and systems that operate at University-wide, divisional and departmental levels will meet these requirements.

Administrative Authority

The President or designate *(normally, the Chief Information Security Officer, CISO)* shall have overarching responsibility for the protection of the University's Digital Assets. The President or designate (*normally, the CISO)* 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 *(normally, the CISO)*. The ISC will: assist in the review of envisioned and unanticipated risks to the University's Digital Assets; collaborate with the President or designate *(normally, the CISO)* to initiate information security initiatives; educate the University community on digital security best practices; and develop and recommend Procedures, Standards and Guidelines for the protection of the University's Digital Assets.

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 *(normally, the CISO),* in collaboration with the ISC, will review such programs to ensure compliance with this Policy and associated Procedures and Standards.

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. The President or designate *(normally, the CISO)* will provide regular updates to the ISC about progress in developing and implementing Procedures, Standards and Guidelines in support of this Policy.

Governance Oversight

The President or designate *(normally, the CISO)* 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 *(normally, the CISO)* 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 *(normally, the CISO)* under this Emergency Authority shall be reported to the Information Security Council and in the President or designate's (*normally, the CISO*) 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.

Information Security Council (ISC) – The Information Security Council (ISC) is a committee established by the President or designate *(normally, the CISO).* The ISC will be co-chaired by a senior faculty member and the *Chief Information Security Officer.* The ISC will be comprised of technical, administrative and academic experts.

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 (normally, the CISO). (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 (normally, the CISO), 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.