Terms of Reference (Revised)

Working Group on the Implementation of Information Risk Management Practice

1	Committee Name	**Working Group on the Implementation of Information Risk Management Practice**
2	Type	Advisory, Ad Hoc
3	Chairpersons	An expert Faculty member from an academic division, and Director, Information Security & Enterprise Architecture, ITS
4	Authority	Advisory to the CIO
5	Timeframes, Reporting and Deadlines	The Working Group will meet once a month (or at the call of the co-chairs) with the aim of reporting a set of draft deliverables (see below) to the CIO by the end of August, 2015, or as soon thereafter as possible.
6	Composition	Co-Chairs • An expert Faculty member from an academic division (Prof. Ronald Deibert) • Director, Information Security & Enterprise Architecture (Martin Loeffler) Members will be drawn from the ranks of faculty, administrative services, and IT staff involved in the operational implementation of information security practice. See project website for current membership.
7	Goal	To produce, in collaboration between the University's divisions and ITS, a set of information risk management Guidelines, Standards and Procedures that can be used across the University in support of delivering on the mandate of an institutional information security policy, or better manage information risk in anticipation of a policy.
8	Proposed Process	1. Review industry standards of information risk management, at a high level, and identify common and high-priority elements; 2. Review practices and initiatives already underway at the University in the area of information risk, within ISEA and in the divisions; 3. Identify and review successful information risk management initiatives at academic institutions comparable to U of T, as available; and 4. Produce a set of deliverables (see below) that can be adapted and used at the institutional/departmental / divisional levels.
9	Deliverables	The Working Group will produce three main deliverables: 1. A recommended program of Guidelines, Procedures and Standards (see definitions below) that that can be used, or adapted as circumstances dictate, by divisions to manage risk to Digital Assets. 2. Recommendations regarding development of local information risk management programs that can be used by divisions to enhance security of their digital assets. 3. Recommendations regarding the establishment of the standing Information Security Council anticipated by the draft Information

		Security and Protection of Digital Assets policy.
10	Staff Support	PGAC - ITS.
11	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. **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.