



Purpose

The purpose of the working group is to develop a set of recommendations as outlined in our mandate below and bring them forth to the Information Security Council.

Mandate

1. Review the exiting Incident Response Plan Review current tools and capabilities - ability to prevent, detect, investigate and respond to an incident.
2. Engage the Crisis Management team to ensure alignment
3. Ensure alignment with Business Continuity, Disaster Recovery and Availability Planning
4. Engage with an external consultant to review and provide guidance of our plan
5. Ensure there is a section on crisis communications, including review of legal requirements (external Consultation)
6. Evaluate Cyber Insurance and the alternative for retaining specific skills needed in event of a significant incident
7. Develop a program around a table top exercise(s) and walk-through drill/simulation test (external vendor)
8. Provide input into Information Security Awareness Program
9. Conduct post-hoc reviews of measures taken in response to digital emergencies and / or breaches concerning digital assets and their remediation, and based on these, make recommendations for future responses (Determine root cause and document lessons Learned)

Process

The working group will seek input from key stakeholders and other interested parties (i.e. faculties and divisions, crisis management team, communications team, central and divisional IT units. Its findings will be documented in the form of an interim report and a final report and will be presented to the Information Security Council.

Timing

1. Initial meetings and consultations: March through April 2018
2. Interim report submitted to the Information Security Council: May 2018
3. Final report submitted to the Information Security Council: September 2018



Membership

Alex Tichine (chair) – Associate Director, Information Security and Enterprise Systems, FASE

Patrick Hopewell – Director - Enterprise Information Solutions, ITS

Alan Stojanovic – Information Security Architect, ISEA - ITS

Rafael Eskenazi – FIPP Director, FIPP Office

Luke Barber – Acting Director - IT Solutions & Risk Management, UTM

John Kerr – Director Risk Management and Insurance - Finance

Caroline Rabbat – Director - Critical Incidents, Safety and Mental Health, A&S

Glenn Attwood – Manager - Networking and Telecommunications, UTSC

Mark Britt – Director - Internal Audit

Sotira Chrisanthidis – Acting Director, FAS IIT