Information Security Incident Coordination Process

Introduction: Incident management includes both detecting and responding to security incidents and taking proactive steps to prevent incidents from occurring. A formalized Incident Coordination Team has responsibility for managing and supporting rapid response to major information security incidents.

Purpose: The rationale for chartering a Security Incident Coordination Team is to:

1. Create the capability for planning for major information security incidents in advance.

2. Specify a consistent predetermined course of action for investigations and incident resolution.

3. Identify the individuals and units that need to be involved in investigating and resolving a major information security incident.

4. Facilitate rapid response to major disruptions of IT systems or services.

5. Develop consistent escalation and notification processes for managing major information security incidents.

Goals:

Create a stable cadre of staff who understand both major functional business processes and the general nature of the University’s information technology infrastructure and enterprise systems.

Develop familiarity with the fundamentals of incident handling processes.

Develop standard protocols for classifying, prioritizing, responding to and containing security incidents, and escalation.

Consult with IT experts and appropriate University units with specific technical expertise as required.

Refer incidents and/or findings to appropriate University tribunal and/or grievance processes consistent with relevant University policies.

Analyze incidents after resolution to identify weaknesses in response processes, applications and infrastructure.

ISICT Charter:

The Chief Information Officer (CIO) is the formal sponsor of the Information Security Incident Coordination Team (ISICT). The CIO will appoint each member of the ISICT in conjunction with their applicable Unit Manager.

The ISICT will be a 'stand-by' team of individuals selected for their institutional knowledge of business processes and the University's technology infrastructure.

An important aspect of the ISICT capability is planning in advance for adverse events. When a major incident (disruption or attack) is in progress, decisions have to be made quickly. The ISICT has a mandate to develop standard protocols and capabilities for timely responses which are appropriate, efficient, and thorough.

The Information Security Manager will chair the ISICT as the CIO's designate, and manage the logistics of arranging immediate response to the applicable incident.

ISICT Activation:

The ISICT will normally be convened when deemed necessary upon the recommendation of the Information Security team, subject to the approval of the CIO (or designate). The applicable supervisors of each ISICT member will be notified (concurrently with the members) when the ISICT is convened. The Charter (above) provides for convening of the ISICT in advance of major incidents for incident response planning and development of standard practices.

Major security incidents which trigger the (recommended) activation of the ISICT can not be fully anticipated or documented herein. ISICT activation would normally be recommended based on a preliminary assessment of the incident's characteristics and operational impact, but could be triggered by any of the following:

- A "**data breach**" (i.e. unauthorized exposure) of sensitive or confidential University data (including *personally identifiable information)*, the source or cause of which is initially unknown or uncertain.
- A serious and **on-going disruption** of an enterprise business system or central technology service/infrastructure, the cause of which is suspected to be security-related.
- A multi-site (or multi-node) security event, affecting **multiple computers** or **many users**.

- An intrusion **in progress** with the potential to seriously damage or disrupt operations.
- A security-related threat, not currently active, but having **campus-wide scope** or involving **enterprise/critical systems** or infrastructure.
- Any security-related incident which involves **external media** (press), or a potential **breach of legislative compliance** (e.g. FIPPA).