POLICY TITLE:	Major Information Security Incident Management Policy
POLICY #:	CIO-ITSecurity – 09.1
Initial Draft By - Position / Date:	D. D. Badger - Dir. PMO /March-2010
Approved By / Date:	***Initial Draft*** reviewed by ITSC/June 12-2010 ***Final Draft*** reviewed by ITSC/Apr 26-2010 ***Final Draft (revised):*** 2011-May – DDB/GB ***Final Draft (revised):*** 2017-March - SW
Last Revised Date:	***Approved: 2017-June-SW/DW/RG***
Next Review Date:	
BRIEF DESCRIPTION:	This Policy defines a standard University-wide process for managing major information technology security incidents, references related University Policies, outlines preparations in advance of incidents occurring, and specifies a coordinated and managed response and escalation process.

Contents

Introduction

All University of Guelph faculty, staff, students and contractors are guided by the Acceptable Use Policy for Computing and Networking Facilities (AUP). The AUP specifies the responsibilities of individual users, system administrators, information technology (IT) service providers and management with regard to the utilization of University IT services and resources. The AUP also specifies the complaint and resolution process of alleged acceptable use violations. The AUP will generally provide acceptable guidance for minor IT-related security incidents.

This Policy defines a standard University-wide process for managing major information security incidents in advance of their occurrence, and provides guidance in initiating rapid responses and appropriate escalation when a major information security incident does occur (or is suspected).

This Policy charters a 'standby' Information Security Incident Coordination Team (ISICT). The University Chief Information Officer (CIO) is the executive sponsor of the ISICT. The Information Security Incident Coordination Process documents when the ISICT would be activated and may involve University administration, judicial processes, Campus Community Police, and technical resources.

This Policy references the University's Emergency Management Plan which details responsibility for major campus emergency situations or disruptions.

This Policy references the University's policy on roles and responsibilities of groups and individuals for information technology security CIO-ITSecurity-02.1 Roles and Responsibilities.

Scope

This policy applies to all University of Guelph students, staff, faculty and contractors, and all information technology systems, services, data and infrastructure owned by or operated for the University.

Policy Statements

1. This Policy defines major information security incidents, a standard process for managing incidents, and specifies individual responsibilities including the protocol for incident reporting, resolution and follow-up activity.

2. This Policy establishes a 'stand-by' Information Security Incident Coordination Team (ISICT) which will be invoked as required by the CIO (or designate).

3. ISICT will manage and support major incident response activities, including remediation, escalation and closure.

4. ISICT will assign technical resources as required to conduct immediate investigation of the sources or causes of major incidents.

5. When criminal activity is alleged or suspected, Campus Community Police Services must be engaged.

6. When unauthorized disclosure of sensitive/confidential data or personal information (as per *Freedom of Information and Protection of Privacy (FIPPA)* legislation) is alleged or suspected, the University Secretariat must be engaged.

7. This Policy authorizes assigned resources to take necessary measures to prevent the spread of any malware, and lock compromised computing accounts.

Information Security Incidents Defined

As of January 2016, Information Security classifies security incidents into three categories:

Severity	**Description**
Minor Incident	Minor security incidents involve a reported security issue that may impact a single individual, a non-critical system, or a policy violation that does not have a widespread impact and is not criminal in nature. These incidents are managed by the Information Security team following standard operation procedures (SOP). Examples include, but are not limited to: • AUP violations • Copyright complaints

	• Compromised student accounts • Single non-critical system malware or virus infections • Spam/phishing message reports.
Significant Incident	A significant security incident has greater scope than a minor incident, involves multiple parties, critical systems, or teams. Typically these have a larger impact or service level disruption on University services or systems, may involve publically facing systems, or affect an external organization. These incidents are managed by the Information Security team, and may require the assistance from technical support teams from other groups on campus. Examples include, but are not limited to: • Localized denial of service attacks • Compromised administrator credentials • Targeted or high volume spam/phishing • Malware affecting several systems • Malware affecting sensitive/critical systems.
Major Incident	Major information security incidents include, but are not limited to: • Denial-of-service attacks on enterprise application systems or IT infrastructure • Theft or misuse of data • Data breaches • Criminal acts or violations of privacy legislation. A significant service level disruption to the University networking infrastructure or any major application system may be escalated to a major incident if the suspected root cause is security related. Any unauthorized intrusion that impacts the availability or integrity of critical IT services such as email, telephone, administrative systems, Internet access, or that affects large numbers of users will be considered a major security incident. Major security incidents also include enterprise application systems and/or databases that have been compromised by ‘malware’, by unauthorized use of administrative accounts, unauthorized disclosure of personal or sensitive information, and either loss or corruption of data.

Incident Reporting and Management

All members of the University community, including third-party contractors are required to report information security incidents (as defined within this Policy or the AUP). It is recommended that notification be provided to both the applicable Unit Manager/Chair **and** to the University Information Security team (ext. 58006, email: incident@uoguelph.ca).

The process of incident management includes defined accountability and consistent, documented procedures. In addition to rapid response to incidents, important related actions include logging, analysis, reporting, communications, involvement of management, required notification to external parties, and debriefing.

All information security incidents will be categorized and tracked in the centrally managed ticketing system, and reports will be generated on a monthly basis by the Information Security team. These reports will be made available to the CIO and other parties approved by the CIO as necessary.

Responsibilities

All Members of the University Community including faculty, staff, students and contractors are responsible for the following:

1. Report any unusual or suspected improper computer activity (i.e. violations of the AUP) to their applicable supervisor, **and** the University Information Security team (ext. 58006, email: incident@uoguelph.ca).

Designated system support technicians and network administrators are responsible for the following:

1. Report any unusual or suspected improper computer activity, security incident or alleged AUP violation to their applicable Unit Head/Department Chair **and** the University Information Security team. Suspected criminal activity (e.g. child pornography), or theft of IT assets should be reported directly to University of Guelph Community Police Services.

2. Avoid making any modifications to systems/equipment involved (or suspected of involvement) in the security incident until receiving instruction from the University Information Security team. Disconnection from the network is the recommended action, however the system should not be

powered off or rebooted unless instructed to do so by the Information Security team.

Department Chairs/Managers/Unit Heads are responsible for the following:

1. Ensure any unusual or suspected improper computer activity, security incident or alleged AUP violation is reported to the University Information Security team **and** their applicable Dean/Director.

2. Ensure any suspected criminal activity (e.g. child pornography), or theft of IT assets is reported to University of Guelph Community Police Services.

The Information Security Team is responsible for the following:

1. Record/log and document all reports of major IT incidents.
2. Verify the existence (and boundary extent if possible) of reported incidents.
3. Make a preliminary assessment of the incident’s impact and current status (N.B. Refer to Appendix 1: ISICT).
4. Report major incidents to the Chief Information Officer (CIO).
5. Follow the established CCS major incident communications plan.
6. Establish and maintain communication with applicable Department Chairs or Managers of the affected units or systems.
7. Recommend the CIO convene the Information Security Incident Coordination Team (ISICT) when appropriate (see Appendix 1).
8. Advise University of Guelph Community Police Services when criminal activity is alleged.
9. Advise University Secretariat if a data breach involving confidential records or personal information is alleged.
10. Liaise with University of Guelph Community Police Services and external forensic consultants (if required) to gather evidence as may be required.

The Chief Information Officer (CIO) is responsible for the following:

1. Receive notice of major IT incidents from the Information Security team or other source (internal or external to the University).

2. Receive recommendations from the Information Security team to convene the Information Security Incident Coordination Team (see Appendix 1).

3. Authorize the convening of the ISICT when necessary.

4. Ensure senior management is kept apprised of the incident, including members of the Campus Control Group.

5. Coordinate communications with relevant stakeholders and the University community as necessary.

Related Policies and References

1. University of Guelph Emergency Management Plan. The Emergency Management Plan is triggered “when an incident has the potential to interrupt the normal activities of the University for an extended period of time.”

2. Acceptable Use Policy. All University of Guelph faculty, staff, students and contractors are guided by the AUP regarding the use of Computing and Networking Facilities. The purpose of the Acceptable Use Policy (AUP) is to identify situations where unacceptable use of systems or networks affects the teaching, learning, research, services or administrative missions of University or compromises the security of systems or data. It also outlines the complaint and resolution process used to resolve any allegations of inappropriate activity.

3. CIO-ITSecurity-02.1 Roles and Responsibilities for Information Technology Security. This Policy defines the roles and responsibilities of groups and individual members of the University community who are responsible for information technology assets and security processes.

4. University Access and Privacy Policies. Reference the University Secretariat web-pages for detailed information regarding *Freedom of Information and Protection of Privacy (FIPPA)* legislation, and required actions if a privacy breach occurs.

5. Information Security Incident Coordination Process. Documents when the ISICT would be activated and may involve University administration, judicial processes, Campus Community Police, and technical resources.

Definitions

Data Breach: A data breach is an incident in which sensitive, protected or confidential data has been accessed, stolen or altered by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), confidential information or intellectual property.

Denial of Service attacks: A denial of service (DoS) or distributed denial of service (DDoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. The most common kind of DoS attack is simply to send more traffic to a network address than it was designed to receive.

Service Level Disruption: An interruption or degradation of system/service availability or performance. Classification as major would be dependent upon the duration, severity and impact of the disruption (e.g. performance degradation versus lack of availability), the criticality of the application/service, and the suspected source of the disruption (i.e. security related).

Version, Change and Approval History

Approved:	June 21, 2017 – Rebecca Graham, CIO
Final Draft w/revisions:	March 27, 2017 - SW
Final Draft w/revisions:	May 2, 2011 - GB
Final Draft w/revisions:	April 8, 2011 - DDB
Final Draft w/revisions:	Feb. 1, 2011 - DDB
Final Draft Issued:	Dec. 1, 2010 - DDB
Circulation Draft Changes:	Nov. 12, 2010 - DDB
Initial Draft Changes:	June 11, 2010 - DDB
Initial Draft Changes:	May 18, 2010 - DDB
Initial Draft Changes:	April 30, 2010 - DDB
Initial Draft Written:	March, 2010
Authored by:	D. D. Badger, CGA, CISA, CGEIT Director, IT PMO & Systems Assurance