Policy Name: Information Security Incident Response
Originating/Responsible Department: Information Technology Services (ITS)
Approval Authority: Senior Management Committee
Date of Original Policy: June 2018
Last Updated: May 2020
Mandatory Revision Date: May 2021
Contact: AVP (ITS) & Chief Information Officer

Policy:
The University must have the capabilities to respond to, and handle information security incidents in a timely manner to limit the potential impact of information security incidents to its information assets and reputation.

Purpose:
This policy identifies requirements for responding to information security incidents that threaten the confidentiality, integrity, and availability of Carleton University's information assets and outlines the responsibilities of the university community in respect of reporting and managing incidents.

Scope:
This Policy applies to all members of the Carleton community including faculty, staff, students, alumni, guests, and contractors that use or access Carleton University provided information technology resources.

Procedures:

Governance
The University must have an Incident Response Committee to oversee the University’s incident response capabilities.

Reporting
Any member of the Carleton University community or individual who uses the university systems must report suspected information security incidents to the ITS service desk. Examples of potential incidents include:

- Ineffective security controls;
- Breach of information confidentiality, integrity or availability expectations;
- Non-compliance with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware;
- Access violations.

Malfunctions or other anomalous system behaviour may be an indicator of a security attack or an actual security breach and should therefore be reported as an information security event.

Identification of Incidents
Information security incidents must be categorized based on their severity and impact on the university’s operations.
Incident response process
The university must publish and follow detailed procedures for responding to suspected information security incidents. These procedures will be posted online and must be reviewed annually.

Institutional Decision Capability
The impact and risk to Carleton will be assessed and triaged procedurally. This assessment will include provision and criteria for engaging Carleton’s institutional decision capability and crisis management process.

Documentation
Information security incidents must be fully documented, including detailed tracking of each step taken to solve the incident, with specific times and actions recorded.

Communication
The University must communicate the Incident effectively to appropriate personnel and maintain open communication, for the purposes of updating and/or providing instruction, for the duration of the information security Incident.

Training
Members of the university’s Incident Handling Team must receive annual training to keep them updated and aligned with current incident response technologies and management.

Roles and Responsibilities
All members of the Carleton University community have a responsibility to report information security incidents to ITS.

The Cyber Incident Response Steering Committee is responsible for:
- Annual review and approval of the University’s incident response procedures
- Oversight of information security incidents that have the potential for loss of confidentiality, integrity or availability of confidential or sensitive information
- Categorisation of incident severity and associated response
- Recommendations to enhance the incident response steps, communications, and resources that includes head count, tools, and training

The Director of Information Security (ITS) or their delegate is responsible for:
- The development and maintenance of the Terms of Reference for the Cyber Incident Response Steering Committee
- Posting and maintaining Carleton’s institutional Incident Response process.
- Coordination of ITS related incident response as per documented procedures.

ITS is responsible for:
- The receipt of reported incidents, categorization, and assignment of severity
- The completion of the required incident documentation
- Coordination of incident response where there is a risk of brand damage or compromise of sensitive information such as Personally Identifiable Information
- Coordination with the Cyber Incident Response Committee during incidents

Department of University Communications is responsible for:
- Communication handling during major incidents

Privacy Office is responsible for:
• Informing the Information Privacy Commissioner of Ontario for Incidents that include a breach of privacy

Department Chairs, Directors, and management in all departments are responsible for:
• Reporting of information security incidents to ITS
• Cooperating with ITS in any investigation including the provision of relevant information system logs (event logs, syslogs, etc)

Compliance
Non-compliance to this Policy may result in disciplinary action.

Contacts:
Assistant Vice-President (ITS) & Chief Information Officer

Links to Related Policies:
http://www.carleton.ca.secretariat/policies/
• Acceptable Use Policy for Information Technology
• Password Policy for Information Systems
• Remote Network Access
• Carleton’s Privacy Policies