Carleton UNIVERSITY
Canada's Capital University

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 2021**
Mandatory Revision Date:	**May 2022**
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 anyone that uses, accesses or connects to Carleton University provided information technology services or resources.

Procedures:

Governance
The Cyber Incident Response Steering Committee provides guidance and oversight of the University's incident response capabilities.

Reporting
Anyone using or accessing university information technology services or resources 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; and/or
- 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 maintain and follow detailed procedures for responding to suspected information security incidents. The ITS Incident Response Procedures document must be available to staff involved in incident response and must be reviewed annually.

Institutional Decision Capability
The impact and risk to the University will be assessed and triaged procedurally. The assessment will include provisions and criteria for engaging the University's institutional decision capability and crisis management process.

Documentation
Information security incidents must be fully documented. Detailed tracking of each step taken to resolve the incident will include specific and relevant dates, times actions taken, by whom, and the outcomes of each action. Supporting artifacts such as logfiles must also be preserved as part of the incident record.

Communication
The Incident Response Team will communicate details of the incident to appropriate community members and will maintain open, effective communications for the duration of the information security incident.

Training
Members of the University's Incident Response Team will conduct practice security incident exercises to maintain their awareness of current processes and procedures. These exercises must be conducted annually.

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;
- Categorization 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; and
- Coordination of ITS related incident response following documented procedures.

ITS is responsible for:

- The receipt of reported incidents, categorization, and assignment of severity;
- The completion and retention of the required information security incident documentation;
- Coordination of information security incident response where there is a risk of reputational damage or compromise of sensitive information such as Personally Identifiable Information (PII); and
- Coordination with the Cyber Incident Response Committee during incidents.

Department of University Communications is responsible for:

- Communication handling during major information security incidents.

Privacy Office is responsible for:

- Initiating the Privacy Breach Reporting Protocol when personal information is compromised during an Information Security Incident
- Notifying affected individuals, the Information Privacy Commissioner of Ontario, and other external stakeholders as necessary where a privacy breach has been confirmed.

Department Chairs, Directors, and management in all departments are responsible for:

- Reporting of information security incidents to ITS; and
- 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:

- Acceptable Use Policy for Information Technology
- Information Security
- Access to Information and Privacy
- Personal Health Information Processing