IT Security Incident Response Protocol
McGill University

Issued: November 15, 2008
Issued by: Chief Information Officer

November 15, 2008 – applying to IT facilities run by administrative units
March 15, 2009 (projected) – applying to all McGill computer facilities, after consultation and revision

Contents

1. Reasons for this protocol

The goal of this protocol is to:

- Identify accountability for responding to IT security incidents
- Ensure appropriate escalation
- Ensure effective administrative response to IT security incidents
- Streamline the response process

2. Application of this protocol

This protocol applies to IT security incidents that affect McGill IT resources.

" 'McGill IT Resources' means all Data, software, hardware, communications systems, storage systems, networks and devices connected to or making use of the University Network, regardless of who administers them."

- Policy on the Responsible Use of McGill Information Technology Resources, April, 2010

This protocol complements, rather than replaces, other protocols and policies in place at McGill.

3. Definitions

IT security incident

An IT security incident, for the purposes of this protocol, includes events where there is suspicion that:

- Confidentiality or integrity of McGill data has been compromised
- IT systems or infrastructure has been attacked or is vulnerable to attack

Types of Incidents

There are three levels of incident severity:

1. *Ordinary:* Incidents for which there are routine solutions. Sensitive information has not been exposed or accessed by unauthorized parties.
2. *Medium:* Incidents that do not have routine solutions but are limited in scope and consequences.
3. *Severe:* Incidents that involve significant personal data leakage, compromised institutional data, or that impacts a significant number of users, all of which has significant consequences.

Information Security unit

The Information Security unit, led by the Director, Information Security, reports to the Chief Information Officer, and has responsibility for the IT security infrastructure on campus.

Incident Officer

The Incident Officer is part of the Information Security unit, and is charged with managing an incident.

Ad hoc Response Team

An ad hoc Response team is assembled by the Incident Officer, and drawn, as appropriate, from the following group (or their delegates):

- Student or Applicant data: Registrar
- Staff data: Associate Vice-Principal, HR
- Alumni data: Registrar or delegate and Vice-Principal, DAR
- Personal banking data: Controller
- Cheque/Supplier data: Controller
- Procurement data: Director of Purchasing

- Research data: Dean or VP-Research
- Others: such as University Safety

4. Reporting an IT security incident

Any member of the university community must report a suspected IT security incident according to normal practice within their unit. (This could be to their supervisor, or directly to their IT service team for their unit or to ICS Service Desk.) However, if the security incident involves many users, such as a virus outbreak, individual reporting is not required.

All suspected IT security incidents must be reported to Information Security (infosec@mcgill.ca or 514-398-3704) either directly by the individual who has discovered the suspected IT security incident, or in those cases, where they have alerted their unit, by the unit.

Where the IT security incident involves physical security issues in addition to IT security issues the incident may instead be reported to the University Security Services who will in turn alert Information Security.

5. Managing the IT security incident

All incidents

Information Security will:

- Create an incident file
- Assign an Incident Officer
- Identify the scope and type of problem (including classifying as ordinary, medium or severe)
- Take corrective action
- Report to appropriate office for further action or discipline to be taken, as needed (Dean of Students, AVP-HR)
- Close the incident file

Medium and severe incidents

Incident officer will:

- Form an ad hoc Response Team to include the relevant owner(s) of the data or issue, provide regular briefings to the Response Team by e-mail, even if there has been "no change", at least once a day (more often at the outset)
- Write a closing incident report that is shared with the Response Team

Severe incidents

Incident officer will:

- Escalate the incident to the CIO

The CIO will:

- Brief the Provost (or delegate), the VP-Public Affairs (or delegate) and any other relevant senior McGill officials
- Together with the above-mentioned individuals:
    - Receive regular reports on risks from the Response Team and communicate them to the Provost (or delegate), the VP-Public Affairs (or delegate) and any other relevant senior McGill officials
    - Ensure risk is managed in consultation with the Provost (or delegate), the VP-Public Affairs (or delegate) and any other relevant senior McGill officials
    - Determine a suitable communications plan in consultation with the Provost (or delegate), the VP-Public Affairs (or delegate) and any other relevant senior McGill officials
    - Activate McGill University Emergency Management Policy and Plan (EMP) if the situation requires, based on the impact on persons, property, and the environment.
    - Provide a closing incident report to Provost and the other senior McGill officials who assisted in the management of the incident.

6. Closing incident report

A closing incident report shall be prepared by the Incident Officer for medium and severe incidents. The report shall include:

- Chronology of the incident and actions taken
- Scope of risk the university faced during the incident (such as number of records, degree of exposure)
- Description of action taken to mitigate and resolve the issue
- Communications that were taken
- Brief explanation of basis for key decisions
- Evaluation of whether response protocol was followed
- Identification of internal improvements to infrastructure, systems, the incident response protocol, and any other actions that are recommended

7. Director, Information Security responsibility

Annual report

The Director, Information Security, shall provide the CIO and the Provost on an annual basis a report summarizing all IT security incidents organized by a taxonomy that describes the incident and its resolution. This report shall include the level of response required to manage the incident.

This report will consist of aggregate data which shall preserve the confidentiality of individuals and units.

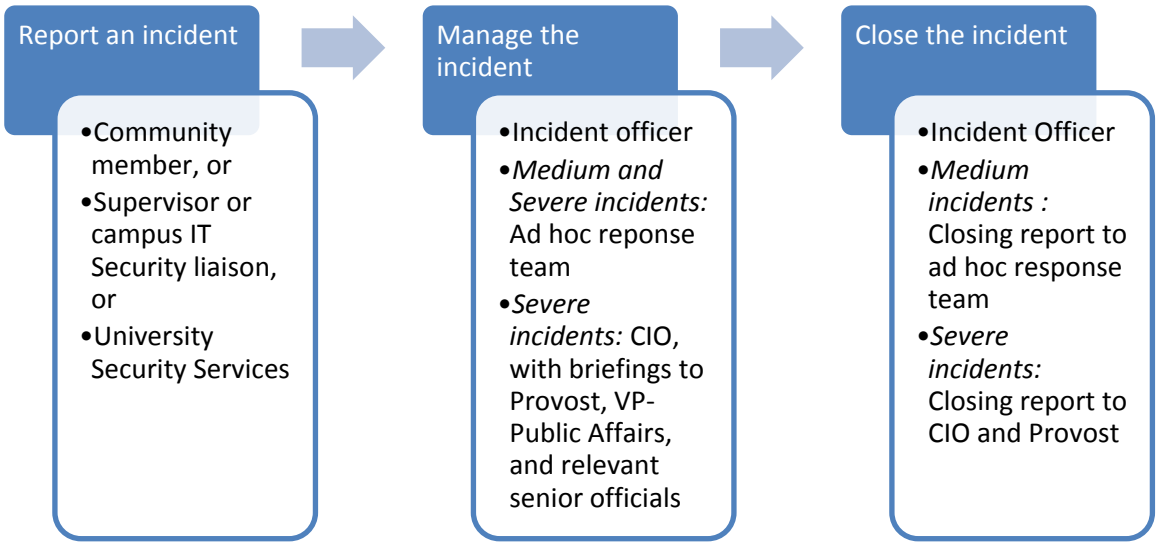
Campus IT security liaison

The Director, Information Security, shall maintain a current list of individuals designated by units that operate McGill computing facilities to act as liaison on matters related to the administration of this protocol.

Examples of IT security incidents

The Director, Information Security, will periodically publish examples of IT security incidents (http://www.mcgill.ca/infosec/) and links to reference material describing IT security incidents, so that the campus will be better informed on the types of incidents that should be reported.

8. Appendix: Summary of Incident Response Protocol



9. Appendix: Process for consultation, discussion and issuing of this protocol

The following will be consulted on drafts of this protocol:

- IT security council (April 4, 2008)
- IT directors (April 9, 2008)
- Associate Vice-Principal, Services (April 2008)
- The Associate Provost, Policies and Procedures (April 21, 2008)
- Academic Planning Group (April 21, 2008)
- Legal Services (April 2008)
- Senior management (July 2008)
- Deans Working Group (Fall 2008)

The document will be revised by and issued by the CIO, after consultation, as outlined above.

Revisions – Jun 18, 2010