Information Security Incident Reporting Instructions

1. Purpose

Provide a **quick reference** for reporting an information security incident and the **immediate steps** to be taken.

2. Scope

These instructions apply to **all the College's individuals and entities**, whether regular, occasional or contractual, regardless of their status, who are using the College's information assets.

3. What to do in the event of an information security incident?

In the event of an information security incident, please follow these guidelines:

- **Report the incident:** contact your local IT Services immediately to report the situation.
- **Gather information:** if possible, gather all relevant information such as date, time, circumstances, and error messages to document the incident.
- **Do not delete data:** avoid deleting items that may serve as evidence or be useful for subsequent analysis.
- **Confidentiality:** only share the incident with those who need to know in order to resolve it.
- **Do not pay a ransom:** if you are asked to pay a ransom, do not do so and contact your local IT Services immediately.
- **Do not shut down your workstation:** it is important not to turn off your workstation as this could result in the loss of evidence used during the analysis.
- **Follow IT recommendations:** follow any recommendations given by the IT staff for an effective incident management process.

4. Who to contact?

- Administrative Services: infosec@crcmail.net
- Lennoxville: IT-Support-Lennox@crcmail.net
- Saint-Lambert: it-support-slam@crcmail.net
- St. Lawrence: ITSupportStlo@crcmail.net