

Information Security: Reporting of Information Security Incidents

Resource reference: **VPS-33-D02**

Status: **Approved**

Last revision: **2023-11-01**

Introduction

This directive defines a standard for all members of the Concordia community to report any suspicious incidents relating to the security of Concordia's information systems. IT Support Staff are responsible for handling security incidents in coordination with Concordia's cybersecurity operations team in alignment with Concordia's Incident Response Plan (IRP) and the Quebec governments act respecting the governance and management of the information resources of public bodies and government enterprises.

Concordia's Chief Information Security Officer has issued this directive under the authority of Policy Number: [VPS-33 - Information Security Policy](#).

Questions about this directive may be referred to: ciso@concordia.ca.

Scope of incidents that must be reported

All acts that may constitute real or suspected breaches of security must be reported promptly to IITS. This includes, but is not limited to:

- unauthorized access
- phishing emails
- theft
- system or networks intrusions
- willful damage
- fraud

The cybersecurity operations team will take charge of the incident and assist with the response to ensure Concordia reacts in a timely appropriate manner and that all legal and regulatory obligations are met including the addition of the incident to the institutional incident register.

How to report incidents

IITS monitors and investigates all IT security incidents. This service includes identifying, responding to, and handling IT security-related incidents such as unauthorized access and intrusions, and any other IT-related security concerns.

Report an IT security incident by phoning the IT Service Desk at 514-848-2424 ext. 7613 or by visiting the IT Service Catalogue at: <http://concordia.ca/it/security/reporting.html>

Accessibility

Community members with accessibility questions or needs related to this directive are asked to contact the appropriate IITS resource person by emailing iits-accessibility@concordia.ca.

Implementation, audit, and review

Concordia's Chief Information Security Officer (CISO) is responsible for the implementation, review, and approval of this directive. Concordia's CISO initiates a review on an annual or as-needed basis to ensure alignment with both internal and external requirements and regulations.