No. IST-05

Title: IT Incident Management Policy

CLASSIFICATION: INFORMATION SYSTEMS & TECHNOLOGY
FIRST ADOPTED: 26 September 2017
AMENDED:

1. Scope

This policy defines the protocol to report, assess, resolve and follow-up IT incidents.

2. Definitions

IT incidents (also referred to as incidents in this document) are events which affect or compromise the operations of the IT systems and infrastructures, or the information stored within. They include but are not limited to: denial-of-service attacks, outage or major degradation of service, intrusion or unauthorised use of privileged accounts, website defacement, breach or unauthorised disclosure of data, loss or corruption of data, etc.

Outage incidents are incidents that halt or degrade significantly the operation of network or computer systems. **Security incidents** are incidents that compromise the integrity of systems or data, or where the intent was malicious. For example a server crashing due to a high volume of requests is an outage incident. It is deemed a security incident if this status makes the service unsecure, or if the requests were caused by a denial-of-service attack.

Incidents of **government scope** are incidents which either: hinder mission-essential services, have consequences on other government organisations offering essential services, have a real or potential consequence on the security and well-being of citizens, have a consequence on the privacy or protection of personal information, or affect the government image or confidence.

The **CERT/AQ** (Computer Emergency Response Team de l'Administration Québécoise) is the governmental alert network.

The **Information Security Officer** (*Responsable de la Sécurité de l'Information – RSI*) is named by Board to oversee matters regarding information security. S/he names one or more **Incident Coordinators** (*Coordonnateur Sectoriel de la Gestion des Incidents* – CSGI) who participate in the CERT/AQ.

3. Reporting

All users of IT services are required to report security incidents to the Helpdesk, as per the IT Security Policy (IST-01).

Once an incident is acknowledged, a preliminary assessment is conducted and a case opened in the incidents file. Besides the scope and severity of the incident, the preliminary assessment evaluates if there are personal information involved, and if it is of government scope.

Incidents of government scope are reported to the **CERT-AQ** by the Incident Coordinator.

Incidents involving personal information are reported to the Director of Corporate Affairs, who may also report it to the *Commission d'Accès à l'Information*.

4. Resolution

If needed, an ad hoc response team may be formed to address the incident, lead by the Incident Coordinator. The Incident Coordinator also ensures the appropriate level of information is communicated in a timely manner to: the Information Security Officer, the Directors of the College, the Communications Officer, the Management Team, the Dawson Community. S/he also makes sure possible corrective measures are researched before closing the case.

If the IT policy was breached, the Director of Information Systems and Technologies may apply sanctions or bring the case to another jurisdiction as per the IT User Policy (MGMT-IST-00).