DAWSON COLLEGE

No. IST-01

Title:	**IT Security Policy**

CLASSIFICATION: INFORMATION SYSTEMS & TECHNOLOGY
FIRST ADOPTED: May 06, 2014
AMENDED: June 01, 2015, 25 November 2016

Goal

This document outlines your responsibilities, as an employee and user of IT resources, regarding IT security. It complements and gives concrete examples but does not replace existing polices and legislation.

1. Protect your accounts

*(*ref*. IST-00 IT Policy 6: users shall…not allow third parties to use their account and take reasonable measures to prevent such access.* and IST-03 *Password Policy)*

a) Do not share your password. If you need a colleague to access files, emails, contact the helpdesk to make arrangements.

b) Never answer an email that asks for your password or follow a link in an email to change your password.

c) Change your password immediately if you suspect it has been compromised and contact the helpdesk .

d) All computers have a built-in default to lock after 10 minutes of disuse. Lock yours whenever you leave your desk.

2. Protect the systems

(ref:. IST-00 IT Policy 2.c: users shall… take no action which could compromise the integrity or normal operations of these resources.)

a) Anti-virus is installed on all computers and laptops provided by the College. If you have reason to believe yours is not functioning or updating properly, contact the helpdesk.

b) Exercise caution when using your computer or laptop, especially when surfing, as you could be the target of malware.

c) Do not use Dawson email for purposes other than your work or Dawson life, as you could be the target of spam and phishing.

3. Protect the information

*(*ref*: RSQ cA-2.1: An Act respecting access to documents held by public bodies and the Protection of personal information* and *Office 365 Terms of Use)*

a) The College has a legal obligation to protect personal information, that is, information concerning and allowing a natural person to be identified. If you have access to such information, you must preserve its confidentiality and only use it for the purposes of your function.

b) Do not store documents containing personal information on a laptop, tablet, or personally-owned equipment, unless encrypted. College laptops are encrypted with BitLocker.

c) Documents containing personal information must be deleted once they no longer serve their purpose, with the exception of archival procedures.

d) If you use our wireless network, choose dawson_secure so that the communication is encrypted.

e) Choose storage for your documents that is adequate for your needs but does not compromise information security. For storage in the Cloud, Office 365/OneDrive should be used. Before choosing a cloud service, notably for surveys or web hosting, check with IST that the College cannot meet your needs.

f) You are given access to systems and information pertinent to your role. If you believe your access privileges need modification or are no longer needed, for example after changing a position, contact the helpdesk.

4. Report an IT security incident

If you believe there has been a breach or risk of a breach of security, contact the helpdesk. Should you lose a College laptop, tablet or phone, contact the helpdesk immediately. All cases are assessed according to risk and possible impact.

When no routine solution exist, or if a breach of information is confirmed, the case is escalated to the Director of Information Systems and Technology or designate, who will ensure:

- An ad hoc response team is formed to address the issue
- If applicable, the IT policy is applied, including referral to the proper jurisdiction
- The particulars of the case are recorded in the incidents file