**No. IST-03**

| **Title:** | **Password Policy** |
|---|---|

**CLASSIFICATION:** INFORMATION SYSTEMS & TECHNOLOGY
**FIRST ADOPTED:** (V1.1) May 8, 2014
**AMENDED:** (V2.01) April 4, 2016
(V2.02) April 22, 2016

## 1. Scope

All employees, students and other users of the College's IT resources are responsible for taking the appropriate steps, as outlined below, to select and secure their password(s).

## 2. Enforcement

Users must not take any measures to bypass password authentication, for example in attempting to override the automatic time outs. Only use password-saving features, e.g. the password manager in your browser, if you are the sole user of the machine.

## 3. Complexity requirements

Passwords must meet the following requirements:

- Be at least 8 characters long
- Include a mix of uppercase, lowercase, and numbers (or optionally, special characters).
- Cannot reuse an old password
- Cannot include the user's account name, or part of it.

The following are also considered good practice in choosing a good password:

- Do not use the name of a relative or pet
- Do not use the same password(s) for your Dawson account(s) as you do for your personal account(s) outside work.
- Do not use birthdates or other personal dates

A good way to generate complex yet easy to remember passwords is to use an abbreviated passphrase: using the first the letter of a sequence of meaningful words, capitalizing a letter and adding a digit.

## 4. Aging

Passwords must be changed at least one time every year. Some mission critical systems, such as Student Information Systems, finance/purchasing, and payroll, may enforce a shorter expiry period.

## 5. Network password

Your network password will work on most college systems including; email, wireless network, employee MyDawson, Moodle, SharePoint, etc.

The mission critical systems have distinct passwords.

In addition, some critical functions within MyDawson require a super user password, or re-entry of the password.

## 6. Sharing passwords

Passwords must not be shared with colleagues, even with a superior, unless an exception has been granted by IST.

Occurrences where a password or an account may have been compromised must be reported immediately to IST; the password for the account and related accounts must be changed.

When it is necessary to disseminate or store passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access.