CONESTOGA
Connect Life and Learning

PASSWORD POLICY

Authorizer: Chief Information Officer, Information Technology Systems

Version: V1

Effective Date: 2/1/2022

POLICY STATEMENT:
Passwords are and remain a solid foundation of most information technology systems. This policy will outline the approach to and use of passwords in the Conestoga College information technology ecosystem.

A password or passphrase method of authentication for users to access systems or information sources. Conestoga College uses passwords where applicable to provide authentication services to various information technology resources.

In all cases where a password or passphrase is used for authentication the following standards will be adhered to:

- Each user will have a unique password to each authentication system and will not reuse passwords across multiple systems. The required minimums for passwords are in the Password Technical Standards document.
- Passwords will go through periodic expiries as defined in the Password Technical Standards document.
    - An exception to this would be if a password has been flagged for compromise or identified in a known password leak, a password would be forced to be reset at that time.
- No user shall request a reset of another user's password under any situation, nor shall passwords be shared among any users.
- Multifactor authentication methods will be enforced and used where applicable for multiple layers of authentication.

POLICY ELABORATION:
Where a password is required by use of a system or information source, the creation or modification of said password shall adhere to all guidelines in this document as well as any other applicable documents including, but not limited to, the following:

Student Rights and Responsibilities Policy
Acceptable Use of Technology Policy

Violations of this policy may trigger consequences set out in other policies.

General Guidelines for all passwords in use at Conestoga College are as follows:
a. Passwords shall be unique
b. Passwords shall not be reused
c. Passwords shall not be shared among users
d. Passwords shall not be in use by more than one user
e. Passwords shall be reset according to required standards
f. Passwords shall meet or exceed all technical requirements
g. Passwords shall be used in conjunction with multifactor authentication were possible

If a password is discovered to not adhere to the guidelines or other applicable standards, then that password shall be changed to match the requirements in such a manner that does not cause undue operational impact but on as short a time frame as possible.

SCOPE:
This policy applies to all users of Conestoga College's technology and information resources.

DEFINITIONS:
Information Technology (IT) Resources
Services, facilities, and equipment including, but not limited to: computer systems; networks; data storage media and content/data; software applications; hardware or; any other electronic, telecommunications or portable device used for the digital transmission of information, on campus or remotely, through which Conestoga provides access or is connected.

Multifactor Authentication (MFA)
MFA is the use of additional verification and authentication steps to provide access to Conestoga College's systems. This may be triggered by accessing a system with sensitive data, by elevating access to a higher than normal level, or by logging in with a higher than average risk-based sign by either user or system metrics.

Passphrase
A passphrase is a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage but is generally longer and more complex for added security.

Password
A type of authenticator comprised of a character string intended to be memorized or memorable by the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process.

REFERENCES:
- NIST Digital Identity Guidelines
- Acceptable Use of Technology Policy
- Student Rights and Responsibilities Policy

REVISION LOG:

December 15, 2021	Academic Forum
January 19, 2022	Academic Coordinating Committee