Policy Title	Authentication and Cyber Security Login Measures
Policy Holder	Senior Director – Computer Services and Project Management
Policy Approver(s)	Senior Team
Related Policies	7-1-1 Acceptable Use Policy
Related Procedures	
Appendices	
Storage Location	Website - https://www.confederationcollege.ca/policies-and-procedures
Effective Date	
Next Review Date	January 30, 2026

Purpose

With increased risk of cyber security breaches, measures are required to protect the College and its users.

Scope

This policy applies to all students, staff and stakeholders with access to Confederation College information technology resources through a login account.

Definitions

VPN	Virtual Private Network - an encryption technology to secure transmissions when communicating with the College.
Phishing	A type of social engineering/cyber attack where the perpetrator sends a fraudulent message designed to trick a person into revealing sensitive information or to deploy malicious software on the victim's computer.

Governing Laws and Regulations

Policy Statements

The College implements a variety of technical measures to provide security against electronic based cyber attacks against the College including but not limited to firewalls, e-mail filtering appliances, endpoint detection software, and antimalware packages. Additionally, the following measures that directly impact authorized users of College IT infrastructure are enforced:

1 **College passwords**

All College users authenticate themselves using login accounts and a password known only to them. The College is following industry recommended practice for the format and maintenance: Passwords do not expire unless a related cyber security incident is identified, and must be at least 15 characters long.

2 **Multifactor authentication (MFA) for College employees**

All College employees are required to use a secondary authentication when

- Using their College owned computer.
- Accessing the College VPN.
- Accessing the College portal.

The College uses DUO as the tool for the secondary authentication. The recommended option is to use the DUO app on a smartphone. Other options are available.
The College will not provide mobile phones nor subsidies for employees to complete MFA.

3 **Basic cyber security training**

All College employees must complete a basic training module for identifying common cyber security threats with a focus on phishing. Employees will periodically be tested with simulated attacks to confirm preparedness and skill in identifying threats.

4 **Work at Home requirements for College employees**

Employees who are conducting College business off site, will require use of the College VPN for access to systems containing sensitive data. To use the VPN employees must be granted access rights to the service, and either

- use their College computer or
- use their home computer with newer operating system (ex Windows 10), and install an acceptable antimalware package.

The College VPN will only allow access upon confirming acceptable software on the user's computer

Note that until January 2023, the College is providing Malwarebytes at no charge to any staff requiring an antimalware package.

5 **Multifactor authentication for College students**

Students can optionally use the Microsoft Authenticator app as a method of implementing MFA on their login account. This is a recommended practice for general security and to avoid the inconvenience of an account lockout should Computer Services identify attempts at potential account hacking. (Note the College uses Microsoft's risky login algorithm to lock out accounts where login attempts are out of the ordinary. Ex. From a remote community, at an odd time, etc.)

Non-Compliance

Non compliance will result in an inability to access services by default. Users are also subject to 7-2-3 Non Compliance Penalties.

Revision History

Version	Change	Author	Date of Change
New		Paul Inkila	18/4/2022