ACCEPTABLE PASSWORD AND PASSPHRASE PROCEDURE

Approving Authority: Academic Coordinating Committee

Policy Owner: Vice President, Information Technology & Systems

Policy Lead: Associate Director, Cyber Security

Effective Date: 2024/11/20

Revision Date: N/A

PROCEDURE STATEMENT

This procedure outlines the use of passwords and passphrases for technology at the Conestoga College Institute of Technology and Advanced Learning (Conestoga). Conestoga uses passwords and/or passphrases where applicable to provide authentication services to technology.

DEFINITIONS

Cellular Device: Any electronic device that can connect to a cellular network using the mobile service provider's SIM card installed within it.

Conestoga Business: Activities performed for business and operations purposes on behalf of Conestoga including academic, administrative and research activities and purposes.

Contractor: Any person or entity contracted by Conestoga to provide goods or services on Conestoga-owned or leased property or at Conestoga coordinated off-site programs, functions, or events. A contractor shall be considered an employer and meet or exceed Conestoga's health and safety management system requirements unless otherwise determined to be a constructor.

Data: Individual symbols or pictures that represent raw facts or figures, which on their own do not comprise meaning and have no discernible arrangement. It can be processed by a computer, computer system or application.

Employee: An individual employed by the College, whether employed full-time, part-time, or on a contract basis, and includes, but is not limited to, faculty, researchers, support staff and administrators.

Guest: An individual who is not an employee, contractor, or student and is external to Conestoga, which includes, but is not limited to, Board members, visitors, alumni, and volunteers.

Information: Data that has been given value or meaning through interpretation or analysis and that has been organized to create meaning.

Mobile Device: Any communication device that does not require a physical wire to relay information from one device to another. It is designed or architected product that is able to be moved easily and used at a variety of locations.

Multifactor Authentication (MFA): Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric). MFA is generally considered secondary authentication in addition to a primary authentication method.

Passphrase: A secret consisting of a sequence of words or other characters to authenticate an identity or to authorize access to data. A passphrase is like a password in usage but is generally longer for added security.

Password: A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.

Student: An individual enrolled in a course or courses at Conestoga, including full-time and part-time.

Technology: Any computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data or information. Components can include, but are not limited to, computers and associated peripheral devices, computer operating systems, utility/support software, accounts, and communications hardware and software.

Technology Resource: Any hardware, software, or communication equipment that a user interacts with for data or information management. This includes but is not limited to computers, mobile devices, cellular devices, applications, user accounts, wired and wireless network services that a user uses for tasks such as creating documents, sending messages, or retrieving data or information from repositories. These resources are owned, leased or in the care, custody, or control of Conestoga.

Technology User: An individual or entity that uses technological tools, devices, or systems for various information and data tasks, which includes, but is not limited to, guests, contractors, students, and employees. These users are authorized to use technology resources owned, leased or in the care, custody, or control of Conestoga with proper authentication and/or identification.

RESPONSIBILITIES

Technology Users

All technology users are responsible for safeguarding their password/passphrase and to not share or publicize it. It is the responsibility of the technology user to adhere to all requirements of this procedure, all Conestoga policies, and procedures.

Cyber Security

The Cyber Security team is responsible for ensuring the security of technology resources via the implementation of technical solutions to identify compromised passwords or passphrases, protect passwords or passphrases, remediating technology resources with weak or compromised passwords or passphrases, and providing instructions on setting strong passwords or passphrases.

PROCEDURE

1. In all cases where a password or passphrase is used for authentication, the following standards must be adhered to.

   Each technology user will have a unique password or passphrase for each technology resource and will not reuse a password or passphrase across multiple technology resources.

   The required minimums for passwords or passphrases are in the Password/Passphrase
   Technical Standards document. Information and guidance is available on the IT and S password page.

   1.1. Passwords or passphrases will become expired after a set timeframe as defined in the Password/Passphrase Technical Standards document.

      1.1.1. An exception to this is if a password or passphrase has been flagged for compromise or identified in a known leak. In these instances, a password or passphrase would be forced to be reset at that time.

   1.2. No technology user shall request a reset of another technology user's password or passphrase under any circumstance, nor shall passwords or passphrases be shared among any technology users. A technology user's identity will be confirmed before a reset will be completed.

   1.3. Multifactor authentication will be enforced and used for multiple layers of authentication. The most secure form of multifactor authentication will be used.

   1.4. If and when a technology user knows or suspects their password and/or passphrase has been compromised, they must immediately contact the IT and S department via one of the contact methods listed on the IT Service Desk page.

RELEVANT LEGISLATION AND RELATED DOCUMENTS

- The Criminal Code of Canada
- Canada's Anti-Spam Legislation
- Accessibility for Ontarians with Disabilities Act (AODA)
- The Personal Information Protection and Electronic Documents Act (PIPEDA)
- Employment Standards Act
- Freedom of Information and Protection of Privacy Act (FIPPA)
- Technology Governance Policy
- Acceptable Use of Technology Procedure
- Employee Code of Conduct Policy

- Employee Discipline Procedure
- Protection of Privacy Policy
- Applied Research Policy
- Social Media Guidelines for Conestoga Employees
- Student Rights and Responsibilities Policy
- Technology Lifecycle Management Policy
- Technology Asset Management Procedure
- Wireless and Mobile Device Technology Management Procedure
- Password/Passphrase Technical Standards
- NIST Digital Identity Guidelines

REVISION LOG

2024/03/13	1.0 draft created for policy review
2024/11/20	Academic Coordinating Committee approval