Passwords Policy

PASSWORDS			
Effective Date	June 1, 2023	**Policy Type**	Administrative
Responsibility	Director, IT	**Related Policies**	IT Governance Policy IT Acceptable Use Policy IT Security Policy
Approval Authority	Executive Council	**Review Schedule**	June 1, 2028

1. **Policy Statement:**

Passwords are a critical component of information security. Passwords serve to protect access to user accounts, data, and systems. However, a poorly constructed or easily guessed password can compromise the strongest defenses. This guideline provides best practices for creating strong passwords.

2. **Scope:**

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local network equipment logins.

3. **Reason for Policy:**

The purpose of this policy is to establish a standard for the secure use and protection of all work-related passwords and provide best practices for the creation of strong passwords.

4. **Guiding Principles – Password Protection**

Users must always protect passwords against disclosure or unauthorized use, including when generated, distributed, used, and stored.

Passwords must follow a minimum set of security requirements including password length, complexity, reuse, age, and account lockout after unsuccessful authentication(s).

Passwords for Privileged Accounts must follow stronger requirements than regular user passwords.

5. The Policy:

5.1. Passwords

Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of 12 characters in all work-related passwords. In addition, we encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type yet meet the strength requirements.

Personal identification numbers (PIN) must be a minimum of 6 characters, alphanumeric.

Two-factor Authentication is required for authentication off-site and when accessing critical systems.

Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet the strong password requirement.

Password cracking or guessing may be performed on a periodic or random basis by the IT Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change.

5.2 Password Creation and Use

All user-level and system-level passwords must conform to the Password Construction Guidelines.

Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

Staff are allowed to use authorized, approved password managers to securely store and manage all their work-related passwords.

User accounts that have system-level privileges granted through group memberships or programs such as administrators must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

5.3 Password Protection

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential <Company Name> information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

Passwords may be stored only in password managers authorized by the organization.

Any individual suspecting that their password may have been compromised must report the incident and change all relevant passwords.

5.4 Single Sign-On (SSO)

Single Sign-On will be the default and preferred method for accessing all authorized systems, applications, and resources. The use of SSO will be mandatory unless specifically exempted due to technical or operational constraints. User accounts are provisioned and managed through the central SSO system, thereby improving the overall security of systems and services.

6. Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Executive Council	• Approve and formally support this policy.
Vice-President, Administration	• Review and formally support this policy.
Director, Information Technology	• Develop and maintain this policy. • Review and approve any exceptions to the requirements of this policy. • Take proactive steps to reinforce compliance for all stakeholders.
Human Resources	• Present each new employee or contractor with the existing NWP policies, upon the first day of commencing work with NWP. • Support all employees and students in the understanding of the requirements of this policy.
Supervisors or Institution Representative	• Support all employees and students in understanding the requirements of this policy. • Immediately assess and report to the IT Help Desk any non-compliance instance with this policy.
Contract Administrators	• Ensure that the password responsibilities and obligations of each party to the contractual relationship are outlined in the contract between the Institution and the contractor/sub-contractor.
All users (Employees and contractors, Students, Visitors and/or Volunteers)	• Comply with the requirements of this policy. • Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible.

7. **Definitions:** This section defines terms specific to this policy.

"Account Lockout Duration" refers to a period an account cannot be used after the account lockout threshold has been met.

"Account Lockout Threshold" refers to how many times an incorrect password can be used before account is automatically disabled.

"Maximum Password Age" refers to the period since a password was set before it is required to be changed.

"Minimum Password Age" refers to the period after changing a password before it can be changed again.

"Minimum Password Length" refers to the smallest quantity of characters a password can contain to be considered valid.

"Multi-factor authentication" (MFA) is an identity and access management security method that requires multiple forms of identification to access resources and data.

"Password" is a code, which, when associated with a user account, provides access to an IT system or application, through an authentication mechanism or a login page.

"Password History" refers to a user's previous passwords for the specified system.

"Password Vault" is software used to store and manage passwords securely. The most popular at the time of writing are LastPass, 1Password, Bitwarden, and Dashlane.

"Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.

"Single Sign-On" (SSO) is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

"Security Tokens" are logical codes or physical items that must be used in conjunction with a password to successfully authenticate to an IT system.

"System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.

"Two-factor Authentication" (2FA) is an identity and access management security method that requires two forms of identification to access resources and data.

"Users" are students, employees, consultants, contractors, agents and authorized persons accessing NWP IT systems and applications.

Revision history: This section records the changes made to the policy over time.

Amendments to this policy will be published from time to time and circulated to the Polytechnic community.

Post-Implementation Review: Approved May 15, 2018

Reviewed and Approved: March 5, 2019

Updated: March 30, 2023

Minor edits: August 25, 2023

References:

NIST SP800-63.3

SANS Password Construction Guidelines

SANS Password Protection Policy Template