5163 Duke Street
Halifax, Nova Scotia, Canada B3J 3J6
902 444 9600 tel, https://nscad.ca

Policy Name:	Enterprise Password Policy		
Policy No:	6.11	**Approval Authority:**	Senior Management Team
Volume:	6, Computer Services	**Responsible Executive:**	Director, Computer Services
Chapter:	11, Enterprise Password	**Responsible Office:**	Computer Services
Originally issued:	September 2014	**Revisions:**	September 2017; March 2019

Policy Statement

All Faculty, Staff, Students and Administrators of NSCAD University have access to systems and services that are password protected. All users with active credentials must follow the directives and guidelines in this policy.

Reason for Policy

Many computer systems, applications and services at NSCAD University require a login ID and password in order to identify and authenticate users. As the university has adopted a single sign-on environment, where the same login ID and password authenticates a user to multiple systems, a robust password policy provides a major defense against unauthorized use of our systems.

When creating a password, the object is to make it as difficult as possible for others to guess or programmatically "crack". Best practice to protect files and University resources is to choose a "strong" password, change it regularly, and never sharing it with others.

Policy Applies to

- This policy applies to all information technology systems and processes at NSCAD University that create, modify, or use information that is private/confidential or of significant institutional value. All such systems will adhere to the minimum acceptable standards, as described below.

Who Should Read this Policy?

- All Faculty, Staff, Students and Administrators.

Contacts

Please direct any question on policy meaning or application to the Director, Computer Services, 902-444-7203 or computer@nscad.ca.

Definitions

ERP: Enterprise Resource Planning system. Currently a vendor-provided product called Colleague, it is a large integrated database that helps direct administration of the University through established best practices.

The Policy

Requirements

1. **Minimum Password/Passphrase Standards (for all University accounts):**
   - A unique user identifier and password is issued for each user of the system. User-initiated password changes must be supported.
   - Sharing individual account is prohibited. Passwords must be changed if they have been used, obtained, or suspected to have been obtained, by anyone other than the account owner.
   - Passwords must be changed at least once annually (every 365 days).
   - Passwords must be stored in a hashed/encrypted format, and will be transmitted over open networks in an encrypted format.
   - Passwords must pass all of the following composition rules:
     a) a combination of alphabetic, numeric and special characters that does not match previous passwords
     b) a minimum of 8 characters - no character string matches from previous passwords
     c) no consecutive, repeated, or serial characters (e.g., aaaa1111, abcd1234)
     d) no single dictionary words

2. **Elevated Privilege System Accounts:**
   - Elevated privilege system accounts are those accounts that have the rights required to maintain a system or application – such as operating system, application, or database administrator accounts, or to operate a scientific instrument.
   - Administrators should not use their personal account as an elevated privilege system account.
   - Where possible these accounts should use a managed authentication service such as Active Directory, LDAP or RADIUS.
   - Elevated privilege system account passwords/passphrases must:
     a) comply with the minimum password standards
     b) be changed at least semi-annually or every 180 days
     c) be at least 12 characters in length when possible

3. **Enterprise User Accounts (Colleague Users):**
   - Enterprise user accounts are those accounts that have the rights required to use and maintain our University Enterprise Resource Planning system.
   - Where possible these accounts should use a managed authentication service such as Active Directory, LDAP or RADIUS.
   - Enterprise user account passwords/passphrases must:
     a) comply with the minimum password standards
     b) be changed at least semi-annually or every 180 days

Procedures

1. Assisted Password Resets: User account passwords will not be reset if the password administrator cannot identify the user requesting the password change/reset with one of the following:
   - A secret key or satisfactory answers about personal information held in central database records
   - A supervisor or technology support person's personal identification
   - A clearly identifiable photo ID
   - Satisfactory challenge-responses in a self-service application

2. Self-service password resets can be performed at https://pass.nscad.ca

Forms and Tools:

N/A

Enterprise Password Policy: https://nscad.ca/site-nscad/media/nscad/6.11EnterprisePasswordPolicy.pdf