ENTERPRISE PASSWORD POLICY

POLICY No.:	315-009
SCOPE:	All Faculty, Staff and Administrators
APPROVAL:	Senior Management Team (Required)
DATE OF ORIGINAL POLICY:	September 1, 2014
LAST UPDATED:	September 1, 2014
SCHEDULED REVISION DATE:	September, 2017
CONTACT:	Director, Computer Services

1 Preamble and Purpose

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 you to multiple systems, a robust password policy provides a major defense against unauthorized use of our systems.

The object when creating a password is to make it as difficult as possible for others to guess or programmatically "crack" what you've chosen. Best practice to protect your own files and University resources requires choosing a "strong" password, changing it regularly, and never sharing it with others.

2 Applicability

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.

System administrators and supervisors may choose to implement these standards with a combination of technological controls and local instruction. Policies and/or standards adopted by an administrative unit must be consistent in principle with this University policy, but may provide additional detail, guidelines or restrictions.

3 Requirements

Part 1: Minimum Password/Passphrase Standards (for all University accounts):

1. **A unique user identifier and password is issued for each user of the system. User-initiated password changes must be supported.**
2. **Sharing of your 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.**
3. **Passwords must be changed at least once annually (every 365 days).**
4. **Passwords must be stored in a hashed/encrypted format, and will be transmitted over open networks in an encrypted format.**
5. **Passwords must pass all of the following composition rules:**
   - **a combination of alphabetic, numeric and special characters that does not match previous passwords**
   - **a minimum of 8 characters**
   - **no character string matches from previous passwords**
   - **no consecutive, repeated, or serial characters (e.g., aaaa1111, abcd1234)**
   - **no single dictionary words**

Part 2: Additional Password/Passphrase Requirements:

Elevated Privilege System Accounts.

1. **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.**
2. **Administrators should not use their personal account as an elevated privilege system account.**
3. **Where possible these accounts should use a managed authentication service such as Active Directory, LDAP or RADIUS.**
4. **Elevated privilege system account passwords/passphrases will:**
    - **comply with the minimum password standards**
    - **be changed at least semi-annually every 180 days**
    - **be at least 12 characters in length when possible**

Enterprise User Accounts (Colleague Users).

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

4 Procedures

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:

1. **A secret key or satisfactory answers about personal information held in central database records**
2. **A supervisor or technology support person's personal identification**
3. **A clearly identifiable photo ID**
4. **Satisfactory challenge-responses in a self-service application**

5 Questions

Any questions regarding this policy should be directed to the Computer Services department.