NORTHERN LIGHTS COLLEGE

Information Technology Password Policy

Policy Number:	
Category:	Administration
Approval Date:	April 4, 2014
Date Last Amended:	April 4, 2014
Date Last Reviewed:	April 4, 2014

POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Northern Lights College's resources. All users, including contractors and vendors with access to Northern Lights College’s systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

PURPOSE

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

PROCEDURE

- All system-level passwords (e.g., Windows Local Administrator, application administration accounts, service / task accounts, etc.) must be changed on at least a semi-annual basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every four months.
- User accounts that have system-level privileges granted through group memberships such as "Domain Administrator" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

DEFINITIONS

- SNMP
    - Simple Network Management Protocol is a protocol for sending device management information to and from connected devices on IP networks, such as switches.

PROCESS

General Password Construction Guidelines

All users at Northern Lights College should be aware of how to select strong passwords.

- Strong passwords have the following characteristics:
    - Contain at least three of the four following character classes:
        - Lower case characters
        - Upper case characters
        - Numbers
        - Punctuation or “Special” characters (e.g. ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /)
    - Contain at least eight alphanumeric characters.
- Weak passwords have the following characteristics:
    - Contains less than eight characters
    - Words found in a dictionary (English or foreign)
    - Commonly used words such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Northern Lights College", "NLC", "northernlights" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords)

Password Protection Standards

- Always use different passwords for Northern Lights College accounts from other non-Northern Lights College access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various Northern Lights College access needs whenever possible.
- For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share Northern Lights College passwords with anyone, including administrative assistants or support personnel. All passwords are to be treated as sensitive, confidential Northern Lights College information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Technology Services department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, Firefox, etc.).
- If an account or password compromise is suspected, report the incident to the Information Technology Services department.

STAKEHOLDERS

None

AMENDMENT HISTORY

Created: April 4, 2014
Revision:

SCHEDULED REVIEW DATE

April 2019