NIPISSING FIRST NATION
A-Kii, Bemaadzijik, E-Niigaanwang
The Land, the People, the Future

Password Policy

Adopted Date	November 16, 2021
Revision Date	April 21, 2026
Revision #	1

NIPISSING FIRST NATION A-Kii, Bemaadzijik, E-Niigaanwang The Land, the People, the Future	**PASSWORD POLICY**	Rev. Approved Date	April 21, 2026
		Previous Approved Rev. Date	November 16, 2021
		Rev. No	1
		No. of Page(s)	5

1. **Policy**
    a. Passwords are a critical component to computer security. They are the first line of protection for user accounts. A poor choice of password could potentially result in compromising NFN's entire network. Therefore, all NFN staff (including contractors and vendors with access to NFN systems) are responsible for taking appropriate steps to secure their password.

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

3. **Scope**
    a. The scope of this policy includes all staff who have access to accounts on any system that resides either on premise or in the cloud, under the control of Nipissing First Nation.

4. **Definitions**
    a. Cloud – refers to any service or system operating on a server off premises.
    b. Plain Text – refers to any form of text that has not been encrypted or secured (such as a password protected file or MD5/SHA256 Hash).
    c. Bad Actor – refers to a cybersecurity adversary that is interested in attacking information technology systems.
    d. MFA – refers to Multi-Factor Authentication where two or more verification factors are required to gain access to a resource such as an application, online account, or a VPN.
    e. Passphrase – a password composed of multiple words or a sentence-like string, typically 14 or more characters, used as an alternative to traditional complex passwords. Passphrases rely on length rather than character complexity for security strength (e.g., threebluetrucksparkedoutside, or Coffee.Before.Anything.Else).

5. **Password Construction Requirements**
    a. Minimum length of fourteen (14) characters on all systems.
    b. Not be a single dictionary word, proper name, common phrase, song lyric, famous quote, or publicly associated personal information. Passphrases

should use four or more unrelated words that do not form a predictable or well-known combination.

c. Not be the same as the User ID.
d. Special characters (e.g. !@#$%^&*), numbers, or uppercase letters are permitted, but not enforced.

6. <u>Transition Clause</u>

a. As of this policy's effective date, staff with existing passwords are not required to change password immediately. However, the new password requirement (including 14 character minimum) applies to future password changes or for newly onboarded accounts.

7. <u>Sharing Passwords</u>

a. Sharing of passwords should never be done unless completely necessary. Never share your passwords with someone outside of the organization that isn't an authorized vendor or contractor. If you need to share a password with a staff member or contractor authorized to receive account access, you must first receive approval from your Department's Director. Following Director's approval, use one of the methods listed below:
    i. Delegated Access – Many online services offer delegated access permissions which allows a user to authorize another user to access their account with limited permissions, without providing their personal login credentials. If you need to share account access and the account in question offers delegated access, this should be the preferred method.
    ii. Password Manager – NFN recommends all staff utilize a password manager for enhanced password security. Password managers can help you generate strong passwords, secure your passwords in a centralized location, audit your passwords for vulnerabilities or leaks to the dark web, safely share passwords with those you trust and revoke password access to those who no longer need access.

    It is recommended that all staff members who use a password manager, utilize the same service. This will make it easier to share passwords within the organization since secure sharing requires both the owner and recipient to utilize the same password manager.
    iii. Password Pusher – When there is no other option available for sharing credentials online, and you need to send your credentials to

someone you can use Password Pusher (https://pwpush.com). Password Pusher links expire after a set amount of time or views, preventing a bad actor from accessing the shared password from a compromised system. Utilizing Password Pusher instead of sending your password in plain text online via email, teams, etc. will greatly enhance security and help protect you in the event your account is compromised.

8. Password Sharing Examples

a. Sharing of passwords should only be done when appropriate. The following is a list of examples for when it is appropriate to share a password. If you are unsure whether it is appropriate to share a password, you should consult NFN IT staff.
   i. Providing a newly onboarded staff member with first time login access.
   ii. Providing a temporary relief worker with account access necessary for them to perform the duties of their position.
   iii. Providing a staff member temporary access to an account for collaboration purposes, when delegated access is not possible.
   iv. In an emergency where account access is time sensitive, but the user who would normally login is unavailable to do so.

9. Retiring Passwords

a. All passwords for accounts that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:
   i. When a user or contractor retires, quits, is reassigned, released, dismissed, etc.
   ii. When temporary access provided to a user is no longer needed.
   iii. Any default or temporary passwords should be changed as soon as possible.
   iv. When a password has been shared with another user and that user no longer needs access.

10. Password Protection Standards

a. Here is a list of best practices to follow, to ensure you are protecting your account:
   i. Always use unique passwords. Do not use the same password across multiple accounts.
   ii. Never reuse a personal account password on an NFN account.

iii. Passwords should meet password construction requirements outlined within this policy.
iv. Never write down a password and leave out in the open (e.g. on a sticky note attached to your monitor).
v. All system-level passwords (e.g. root, network administrator, system administrator, etc.) must be stored securely, either within an encrypted file, a secure password manager (LastPass, 1password, Bitwarden, or Keeper) or be stored physically behind lock and key.
vi. Never send plain text passwords over the internet (e.g. Email, Microsoft Teams, etc.).
vii. Never reveal a password over the phone to anyone.
viii. Don't reveal a password to other staff.
ix. Don't hint at the format of a password (e.g. 'my family name').
x. Don't reveal a password on questionnaires or forms.
xi. Don't share a password with family members.
xii. Don't store passwords in a file on ANY computer system unencrypted.
xiii. If someone demands a password, refer them to this document or have them call the NFN IT Manager.

11. MFA Requirements

a. NFN staff members are recommended to use MFA on all their accounts whenever possible. MFA security practices drastically reduces the likelihood of an account being compromised, even if a bad actor is able to obtain a user's password. NFN will enforce MFA policies on all Microsoft accounts which include:
    i. NFN Email accounts
    ii. Azure Servers and related services where applicable
    iii. Office365 Admin Center
b. NFN requires a minimum secondary authentication via SMS, but highly recommends the use of Time-based One-Time password MFA or Push-Notification MFA. These types of MFA are much more difficult to hack and users will be far more secure compared to SMS based MFA.

12. Compromises

a. If an account or password is suspected to be compromised, including any unusual activity, report the incident to the NFN IT Manager. Examples of a potential compromise might include:

i. A password reset notice sent to your email when you did not request one.
ii. A staff member sends you an email that appears to be suspicious or the staff member confirms they did not send the email.
iii. Opening a potential phishing link and realizing after the fact.
iv. If a physical device is lost or stolen from your possession.

13. <u>Penalties</u>

a. Any employee found to have violated this policy may be subject to disciplinary action in accordance with HR Policy.