Reference: **ADMINISTRATIVE SERVICES -INFORMATION TECHNOLOGY (IT)**
Title: **PASSWORD POLICY**
Policy Number: **06-01-08**
Issue Date: **03-31-2004**
Revision Date: **05-17-2021**

I. Purpose

The purpose of this policy is to specify guidelines for use of passwords for employees of the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority"). Most importantly, this policy will help users understand why strong passwords are a necessity and will help them to create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

II. Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

III. Scope

This policy is applicable to all employees of the Authority and all other individuals with access rights (i.e., consultants, interns, temporary employees, etc.) and applies to any and all use of Authority IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection (collectively "assets").

IV. Policy

A) Construction

The best security against a password incident is simple: following a sound password construction strategy. The Authority mandates that users adhere to the following guidelines on password construction:

- Passwords must be at least 8 characters
- Passwords must be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols) and at least two of the three
- Passwords should be comprised of a mix of upper- and lowercase characters
- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information about the employee, their spouse, their pet, their children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add

additional characters, numbers, and/or symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

B) Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the Authority's proprietary information. The following guidelines apply to the confidentiality of Authority passwords:

- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured
- Users must not use the same password for different systems and/or accounts
- Users must not send passwords via email
- Users may not re-use the last five passwords

C) Change Frequency

In order to maintain high security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. The Authority may use software that enforces this policy by expiring users' passwords after this time period.

D) Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the Chief Information Officer (CIO). Any request for passwords over the phone or email, whether the request came from Authority personnel or not, should be expediently reported. When a password is suspected to have been compromised, the CIO will request that the user, or users, change all passwords.

E) Applicability of Other Policies

This document is part of the Authority's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

V. Compliance

This policy shall take effect upon publication. Compliance is expected with all applicable laws and Authority policies and standards. IT may provide notification of amendments to its policies and standards at any time; compliance with amended policies and standards is expected.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The Authority will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

VI. Definitions

Authentication **-** a security method used to verify the identity of a user and authorize access to a system or network.

Password **-** a sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.