Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Title: **NETWORK ACCESS AND AUTHENTICATION POLICY**
Policy Number: **06-01-18**
Issue Date: **03-25-2019**
Revison Date: **05-18-2021**

I. PURPOSE

The purpose of this policy is to describe what steps must be taken to ensure that employees connecting to the corporate network are authenticated in an appropriate manner, in compliance with standards of the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority") and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

A) Overview

Consistent standards for network access and authentication are critical to the Authority's information security and are often required by regulations or third-party agreements. Any employee accessing the Authority's computer systems has the ability to affect the security of all employees of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

B) Scope

The scope of this policy includes all employees of the Authority and all other individuals with access rights (i.e., consultants, interns, temporary workers, etc.) to Authority-owned / Authority-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the Authority's externally-reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

II. POLICY

A) Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with the Human Resources Department is required
- Users will be granted least amount of network access required to perform their job function

- Users will be granted access only if the user accepts the Acceptable Use Policy (NFTA Policy No. 06-01-16)

- Access to the network will be granted in accordance with the Acceptable Use Policy (NFTA Policy No. 06-01-16)

B) Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format. The standard format for the Authority is firstname.lastname

- Accounts must be password protected (refer to the Password Policy for more detailed information) (NFTA Policy No. 06-01-08)

- Accounts must be for individuals only. Account sharing and group accounts are not permitted unless approved by the Chief Information Officer (CIO)

- User accounts must not be given administrator or 'root' access unless this is necessary to perform the employee's job function

- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed

- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the CIO or executive team, or as requiredby applicable regulations or third-party agreements

C) Account Termination

When managing network and employee accounts, it is important to stay in communication with the Human Resources Department so that when an employee no longer works at the Authority, that employee's account can be disabled. The Human Resources Department must notify the IT Department in the event of a staffing change, which includes employment termination, employment suspension, location changes, or a change of job function (promotion, demotion, suspension, etc.).

D) Authentication

User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

E) Use of Passwords

When accessing the network locally, the username and password combination is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the Authority's Password Policy (NFTA PolicyNo. 06-01-08).

F) Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passwords are required. Screens will lock automatically on desktops and servers after fifteen (15) minutes of inactivity. This feature cannot be disabled by a malicious user or employee. This security control may not be bypassed without approval from the CIO.

G) Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, employees must strictly adhere to corporate standards with regard to antivirus software and patch levels on their machines. Employees must not be permitted network access if these standards are not met. This policy will be enforced with a product that provides network admission control.

H) Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the Authority must lock an employee's account after five (5) unsuccessful logins. This can be implemented as a time-based lockout or requires a manual reset at the discretion of the CIO.

I) 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.

III. 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 employee 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.

IV. DEFINTIONS

Antivirus Software - an application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

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

Encryption - the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

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