Reference:	**ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Title:	**ACCEPTABLE USE POLICY**
Policy Number:	**06-01-16**
Issue Date:	**07-16-2018**
Revision Date:	**05-18-2021**

I. PURPOSE

The purpose of this policy is to detail the acceptable use of corporate information technology resources for the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority") and for the protection of all parties involved.

A) Overview

Though there are a number of reasons to provide an employee network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the employee is asked additionally to use common sense when using Authority resources. If an employee is questioning whether a particular use of computer-related systems or resources is appropriate, the employee should ask: Does this particular use serve the business interests of the Authority and its customers? Questions on what constitutes acceptable use should be directed to Chief Information Officer (CIO) x7251 or the IT Help Desk at help.desk@nfta.com.

B) Scope

The scope of this policy is applicable to all employees of the Authority and all other individuals with access rights (i.e., consultants, interns, temporary workers, etc.) and applies to any and all use of corporate IT resources, including but not limited to, computer systems, email, phones, the network, information on any of these systems, and the corporate Internet connection.

II. POLICY

A) E-mail Use

The email system is property of the Authority. Its primary focus is for business communications. Occasional incidental personal use is allowed as long as it does not interfere with, or unreasonably delay, business operations.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.

- The employee is prohibited from forging email header information or attempting to impersonate another person.

- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the Authority may not be sent via email, regardless of the recipient, without proper encryption.

- It is Authority policy not to open email attachments from unknown senders, or when such attachments are unexpected unless verified beforehand.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The system is currently set to 50Mb for internal emails and 10Mb for external emails. However, it may be altered with permission from the CIO.

Please note that detailed information about the use of email may be covered in the Authority's Email Policy.

B) Network Access

Employees should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to their job function (i.e., looking at systems/files for which they have no business purpose). Existence of access capabilities does not imply permission to use this access.

C) Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The employee may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.

- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the Authority, or to its employees.

- Share defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, insulting, threatening, obscene or otherwise inappropriate messages or media.

- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

- Make unauthorized offers for products or services.

- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.

- Install or distribute unlicensed or "pirated" software.

- Install any software not authorized, in writing, by the IT Dept. for installation or download. Authority provided phones are covered under a separate policy.

- Reveal Authority passwords to others, including family, friends, or other members of the household when working from home or remote locations.

D) Blogging and Social Networking

Blogging and social networking by the Authority's employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking is never allowed from the corporate computer network unless it is part of an employee's job function. The employee assumes all risks associated with blogging and/or social networking.

E) Instant Messaging

Instant Messaging is allowed for corporate communications only. The employee should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

F) Overuse

Actions detrimental to the Authority's computer network or other corporate resources, or that negatively affect job performance may be blocked (i.e., network sniffing, streaming video that is not authorized, etc.).

G) Personal Use

The Internet is a network of interconnected computers of which the Authority has very little control. All employees should recognize this when using the Internet, and understand that it is a public domain and an employee may come into contact with information, even inadvertently, that the employee may find offensive, sexually explicit, or inappropriate. The employee must use the Internet at their own risk. The Authority is specifically not responsible for any information that the employee views, reads, or downloads from the Internet.

Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this, is limited in amount and duration, and does not impede the ability of the individual or other employees to fulfill the Authority's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. The Authority may revoke or limit this privilege at any time. For example, employees may make occasional and incidental use of information technology resources to schedule a lunch date, cancel a sports practice, check their bank accounts or other personal investments, or to communicate with a volunteer charity organization. The employee's judgement regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgment by providing the above guidelines. If an employee is unclear about the acceptable "personal" use of an Authority provided resource, the employee should seek authorization from their immediate supervisor or the IT Department.

H) Infringement of Intellectual Property Rights of Others

The Authority's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized material protected by intellectual property laws relating to copyright©, trademarks™ ®, service marks ^{SM}, patents ℗, etc. The following activities constitute violations of acceptable use policy if done without permission of the material owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs and DVDs; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted material which an employee has not already legally procured. This list is not meant to be exhaustive and copyright law applies to a wide variety of works,much more than is listed above.

I) Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.

J) Monitoring and Privacy

Employees should expect no privacy when using the corporate network or Authority resources. Such use may include but is not limited to transmission and storage of files, data, and messages. The Authority reserves the right to monitor any and all use of the computer network. To ensure compliance with Authority policies, this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media. This monitoring includes all wired and wireless connections including the guest Wi-Fi.

K) Circumvention of Security

Using Authority-owned or Authority-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited. Disclosing or sharing of accounts and/or passwords is prohibited unless authorized by the CIO.

L) Use for Illegal Activities

No Authority-owned or Authority-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Network Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Downloading, storing, or distributing copyrighted material
- Harassment of any kind

The Authority will take all necessary steps to report and prosecute any violations of this policy.

M) Non-Authority-Owned Equipment

Non-Authority-provided equipment is expressly prohibited on the Authority's network with the exception of the guest Wi-Fi network. Visitors and Employees may, at their own risk, use the guest Wi-Fi network for laptops, tablets, and cell phones only.

N) Personal Storage Media

Personal storage devices represent a serious threat to data security and are expressly prohibited on the

Authority's network. Vendor provided devices (i.e., USB memory stick) should be scanned by IT prior to installation into an Authority system.

O) Software Installation

Installation of non-Authority-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. Authority provided mobile devices are covered on a separate policy.

P) Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the employee must immediately notify IT, their supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Being asked for login information by an unfamiliar program
- Suspected virus/malware/Trojan infection and/or odd system behavior
- Loss or theft of any device that contains Authority information
- Loss or theft of ID badge or keycard
- Any attempt by any person to obtain an employee 's password over the telephone or via email
- Any other suspicious event that may impact the Authority's information security

Employees must treat a suspected security incident as confidential information and report the incident only to their supervisor. Employees must not withhold information relating to a security incident or interfere with an investigation.

Q) 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. DEFINITIONS

Blogging **-** the process of writing or updating a "blog," which is an online, user-created journal (short for "web log")

Instant Messaging - a text-based computer application that allows two or more Internet-connected users to "chat" in real time

Peer-to-Peer (P2P) File Sharing - a distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access **-** remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media - information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

Network Sniffing - a program that captures and analyses network traffic for the purpose of examining the contents of the packets.

Port Scanning - a port scanner creates a series of messages and directs them to a system with the intention of breaking into the system. The messages are directed at “well-known” ports looking for a vulnerability.