Reference:	**ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Section:	**ADMINISTRATIVE SERVICES**
Title:	**COMPUTER AND NETWORK ACCESS AND USE**
Policy Number:	**06-01-01**
Issue Date:	**03-31-2004**
Revision Date:	**05-14-2021**

I. PURPOSE

The Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as “NFTA” or “Authority”) operates and maintains a large network of computer systems ranging from large shared systems to desktop workstations connected together by networks and other communications systems of many types.

This policy is designed to define the appropriate and responsible use of Authority computer systems and network facilities by all employees. This policy applies to all computer systems of the Authority regardless of their operating system or manufacturer. As used in this policy statement, the term *user* refers to any person utilizing Authority computing or networking facilities.

The term *computer account* refers to the user’s identification, logon/login identification, or other system specific terms issued to a user permitting access to a computer network system.

Other terms:

Computer hardware - any and all tangible or physical devices attached to or used in conjunction with a computer system.

Computer network - the interconnection of communication lines with a computer through remote terminals, workstations or a complex consisting of two or more interconnected computers.

Computer resources - any and all computerized Authority data, computer hardware, and computer software owned by or operated at the Authority.

Data - a representation of information, knowledge, facts, concepts, or instructions that have been prepared or are being prepared in a formalized manner and have been processed are being processed, or are intended to be processed, in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, compact discs, thumb drives, and as stored in the memory of Authority computers.

Information technology - any and all computer electronic resources that are utilized in the search, access acquisition, transmission, storage, retrieval, or dissemination of data.

Responsible Use - any action or behavior of an individual that does not cause accidental or unauthorized destruction, disclosure, misuse, or modification of or access to the information technology or computer resources owned or operated by the Authority.

E-Mail - for the purpose of this policy, is a means of sending messages between the Authority's computer and other computers using the Internet.

Asset - any Authority computer or device that can be used to access data available on the Internet.

FTP – short for ***F****ile* ***T****ransfer* ***P****rotocol,* the protocol used on the Internet for exchanging files. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).

II. POLICY

A) Compliance

All Authority employee users of the Authority information technology resources are required to comply with and, by using such resource, be subject to this policy.

B) Ownership

The Authority owns and operates the computers, computer networks, and software, data files, connections to external computer networks and service agreements to external computer services. Authority users do not own any of the computer resources and must comply with this policy and all other polices that govern the use of Authority assets.

C) Privacy

User privacy is not guaranteed. When the Authority systems are functioning properly, a user can expect the files and data they generate and store in their network drive to be private information, unless the creator of the file or data takes action to reveal it to others.

The Authority's IT manager will not routinely monitor the contents of electronic communications such as e-mail, but will investigate properly identified allegations of misuse and will report such violations to the employee's direct supervisor. Actions taken by the direct supervisor may result in loss of privileges, disciplinary action, up to and including termination of employment.

D) Right to Monitor

The Authority owns the computer systems networked together on a common network backbone. Every computer attached to the network for any reason (e.g., Internet connectivity, e-mail accessibility, etc.) is subject to monitoring by the IT Manager and Network Administrator. Due to the exponential growth of the number of data packets transmitted through the Authority network, this monitoring is required in order to detect and correct network problems as they occur, thereby ensuring the continued stability of the Authority computing environment. System monitoring is a mechanism for monitoring the computers system or user activity, not a method of accessing private information.

E) FORMS OF ABUSE

- **Worms and Viruses**

Anyone knowingly attempting to proliferate, write, ftp worms or viruses of any size, shape, or form will be subject to loss of privileges, and disciplinary action, up to and including termination of employment.

- **FTP**

Using ftp to transfer files to or from remote sites which violate the policies of the remote site is prohibited. In particular, transferring files which are large, contain material offensive to either site, contain information to be used for pecuniary interests of any party, or contain monetary or sexual solicitations is prohibited.

III. PROCEDURE

In order for an employee to obtain access to a computer system for the performance of assigned job duties, the Manager or General Manager must submit the **"Employee Access to Computer Systems Request Form"**

Computer Systems Access Request Form.doc

A. Access to Authority Computing Systems

- Only properly authorized persons may access Authority computer systems; proper authorization is provided by the system administrator in the form a computer account issued in the name of the authorized person.
- Users may not permit any other person, including other authorized users, to access Authority computer systems with their personal computer account. It is recognized that in some cases it is necessary to share a computer account. For those specific cases, the account must be authorized by the Department Manager/Supervisor, and should only be used when the activities requiring the shared computer account are ongoing. All other activities must be conducted using the personal computer account.

B. Employee Departure Requirements

- When an employee who has access to the Authority's computer systems resigns, retires or is otherwise separated from employment, the department manager is responsible for submitting the **"Employee Departure Checklist Form"**, ensuring that access to all Authority systems have been deactivated.

Employee Departure Checklist Form.doc

- Employee references on the company website should be removed.
- Update accounts and password required to access specialized systems, if applicable.

C. User responsibilities

- Each authorized user of information technology resources must assume responsibility for their own behavior while utilizing these resources.
- Users are responsible for selecting secure passwords for their computer accounts and for keeping those passwords secret at all times. Passwords should not be written down in obvious places, stored on-line, or given to others. Passwords should never be given out to someone claiming to be a system or account administrator. If, for any reason, your password is divulged to another person, it should be changed immediately. *Refer to "Common Recommendations Concerning Passwords."
- Users are responsible for protecting their own files and data from reading and/or writing by others, using whatever protection mechanisms provided by the operating system in use. For microcomputer systems users are responsible for maintaining backup of computer files and data. See attached End User Preventive Maintenance Checklist

End User Preventive Maintenance Checklist_09.doc

- Users are responsible for reporting any system security violations, or suspected system security violations, to the IT Manager immediately.
- Users attempting to gain access to systems and/or information for which they are unauthorized, or attempting to acquire the computer account and password of authorized users, will be in violation of this policy.

Violations of any portion of this policy may result in loss of account privileges, initiation of legal action by the Authority and/or appropriate disciplinary action.