Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Section: **ADMINISTRATIVE SERVICES**
Title: **THIRD-PARTY ACCESS TO AUTHORITY NETWORK**
Policy Number: **06-01-15**
Issue Date: **09-18-2008**
Revision Date: **05-18-2021**

I. PURPOSE

The Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority"), on occasion, has received requests for direct connections to the network from third-party firms. Such requests for network access are typically either from firms that provide system implementation support services to the Authority or from area network service providers that offer remote-access solutions to the Authority. This policy has been developed to ensure that all such network access requests are treated consistently, fairly, and without violation to existing Authority policies.

Outside agencies conducting business with the Authority requiring network communication will be able to conduct this business using the Authority's existing Virtual Private Network (VPN) or direct access through the issuance of an IP address. The following guidelines apply to any request for third-party connections to the Authority network:

- The connection must be used solely to provide the improvement in, or the implementation of, services indicated by the Authority department in its request.

- The Authority's Management IT Department is responsible for all external connections to the Authority network. Departments must initiate special connections to outside firms by submitting the Third-Party Access to Authority Network Request Form to IT. The request must explain the nature of the desired connection and the benefit(s) expected from the connection.

- Agencies with special connections must agree to abide by any and all computing-related policies, especially security, privacy, acceptable use, auditing and software licensing policies, of the Authority. Violation of any such policy will result in immediate termination of the connection.

II. POLICY

A) Authority Third-Party Access accounts are to be used only by the person in whose name the account was created. Corporate accounts are to be used only by members of the group or organization named by the account.
B) All accounts are granted subject to compliance with this policy statement. Failure to comply with these guidelines may result in account termination.
C) The Manager of IT reserves the right to cancel accounts without giving notice of intention to do so.
D) Attempts, whether successful or not, to gain access to any other system, or user's private data is in violation of this policy.
E) Third-Party Access account holders may not attempt to circumvent security or authentication systems on any host, network hardware, or user accounts. This includes, but is not limited to, the account holder logging into a server or account the account holder is not expressly authorized to access, or probing network security.

III. TERMINATION OF ACCESS

Access to the Authority network is a privilege that may be granted or withdrawn by the Authority at any time. The Authority may terminate the special connection if it is determined not to be in the Authority's interest to continue the connection. The Authority may also impose temporary service interruptions for

operational reasons.

IV. APPLICATION PROCEDURE

Step 1: The Authority Department Manager must complete the Departmental Manager Request for Vendor Access to Authority Network Form for any vendor that is requesting access to the Authority Network Assets and submit the Manager of IT.

Departmental Manager Request for Vendor Access.pdf

Step 2: The requesting vendor will then receive the Vendor Informational Form from either the IT Manager or Authority Department Manager, upon receipt the vendor must send the completed form to via email to:

help.desk@nfta.com

Step 3:Once the IT Manager receives the Vendor Informational Form, access will be either granted or denied. If access is denied, the Manager of IT will provide an explanation to both the Department Manager and requesting vendor. If access is granted, the requesting Department Manager will be provided with the Vendor Access Response Form with the requested information and will have the responsibility of providing that information to the vendor.

Step 4: When access is no longer needed by the requesting vendor the Department Manager must submit the Vendor Termination Form to the Manager of IT.

Vendor Termination Form.pdf