Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Section: **ADMINISTRATIVE SERVICES**
Title: **REMOTE ACCESS TO MAINTENANCE INFORMATION MANAGEMENT SYSTEMS (MIMS)**
Policy Number: **06-01-06**
Issue Date: **11-15-2002**
Revision Date: **05-17-2021**

I. PURPOSE

Remote Access to the Maintenance Information Management System (MIMS) of the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority") using an Internet Service Provider (ISP) and a Virtual Private Network (VPN, via Internet) connection will be provided to the authorized personnel only. This benefit is not intended as a means of telecommuting from home but as to supplement monitoring and completing daily work tasks for management staff.

While offering potential benefits, remote access to Information Technology (IT) resources introduces new risks to the security of Authority's automated information and systems, as well as to the privacy of the authorized personnel it serves. For example, without appropriate safeguards to protect the integrity of the electronic functions and processes the authorized personnel working remotely is to perform, the following security issues could occur:

- Malicious software could be introduced to the user and/or Authority assets and
- System sign-on identifications and passwords could be intercepted and reused to access systems and data files without authorizations.

II. POLICY

All management with Remote Access to the MIMS must:

1. Sign and agree to abide by the provisions of the "*Application for Remote Access to Authority Maintenance Information Management System (MIMS) Application Form*." (Exhibit 4)
2. Maintain the latest release of virus software loaded on their computer equipment to protect the Authority's automated information systems from attacks of malicious software.
3. When possible, install a home base firewall software package.
4. When prompted to save employee's username and password the user must respond "No." This information is stored in your computers cache memory and can be obtained by hackers
5. Never share their account / password with others.
6. Never use someone else's account.
7. Never invade the privacy of other individuals or computer systems.

III. PROCEDURE

All employees authorized to use MIMS remotely are required to complete a MIMS Statement of Understanding (Exhibit 4 Section B) and are subject to the provisions of this policy.

All employee so authorized, and those persons whom they report to, shall ensure:

1. Employee applications for access to the MIMS should be made by completing the Application for Remote Access to MIMS (Exhibit 4)
2. The employee's signed statement and application approved by the appropriate Department Manager shall be forwarded to the IT Manager.

3. IT will provide the employee with proper system setup for accessing the system remotely upon receipt of the approved statement of understanding and application.

4. IT will monitor system use monthly.

5. Ethical judgments are exercised when accessing, selecting, printing, and reviewing system data.

6. Compliance with all Authority policies including those specifically referenced by this document.