Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Section: **ADMINISTRATIVE SERVICES**
Title: **REMOTE ACCESS TO AUTHORITY E-MAIL**
Policy Number: **06-01-04**
Issue Date: **11-15-2002**
Revision Date: **05-14-2021**

I. PURPOSE

Remote access to Microsoft Outlook Email via the Internet and mobile devices will be provided to the authorized personnel of the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as “NFTA” or “Authority”) only. This authorization can be in the form of a request made by the employee's manager or supervisor.

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 office equipment and
- System sign-on identifications and passwords could be intercepted and reused to access systems and data files without authorizations.

II. POLICY

This policy is designed to ensure the Authority's IT resources are appropriately protected when authorizing the remote access of the Authority's automated information and systems.

Remote Access To Email Form.doc

When accessing the Authority’s Microsoft Outlook Email via the Internet and mobile devices authorized personnel must adhere to the following:

1. Must complete (Section A) with all appropriate information along with justification for access.

2. Must sign and agree to abide by the provisions of the "*Remote Access to Authority Email Application Form*." (Section B)

3. Must 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.

4. When possible, install a home base firewall software package.

5. Delete and report e-mails from unknown senders, which contain attachments or are otherwise suspicious without opening them.

6. When prompted to save your user name and password the user must respond "No". This information is stored in your computers cache memory and can be obtained by hackers.

7. The user must never share their account / password with others.

8. Users should never use someone else's account.

9. Users should never use their account to harass another person.

10. Users should never invade the privacy of other individuals or computer systems.

11. Users should never use their account to send anonymous messages.

12. Users must not attempt to read another person's electronic mail or other protected files.

13. Users should refrain from the sending of chain letters or broadcast messages to lists or individuals, which wouldcause congestion of the networks or otherwise interfere with the work of others.

III. PROCEDURE

All employees/Board members authorized to use Microsoft Outlook Email remotely are required to complete the REMOTE E-MAIL ACCESS STATEMENT OF UNDERSTANDING (Section B) and are subject to the provisions of this policy.

The messages are retained on the server until deleted by the authorized user. It is important that users actively manage disk space to minimize storage requirements. Access to email is a privilege and certain responsibilities accompany that privilege.