Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Section: **ADMINISTRATIVE SERVICES**
Title: **ACCEPTABLE USE POLICY**
Policy Number: **06-01-16**
Issue Date: **07-16-2018**
Revision Date: **02-10-2026**

1. Purpose

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

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 NFTA resources. Inappropriate use exposes NFTA to potential risks including, but not limited to, virus attacks, compromised network systems and services, and legal issues. 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 NFTA and its customers? Is it a security risk? Questions on what constitutes acceptable use shall be directed to the Chief Technical Officer (CTO) or the IT Help Desk at servicedesk@nfta.com or 716-855-7370.

The NFTA will interpret and apply this policy in a manner that is consistent with all applicable laws, rules, and regulations.

2. Scope

This policy is applicable to all authorized users including NFTA employees and all other individuals with access rights (i.e., consultants, interns, temporary workers, etc.) and applies to any and all use of Authority IT resources, including but not limited to, computer systems whether located in-house or accessed remotely, email, phones, the network, information on any of these systems, and the Authority Internet connection.

3. Authorized User Responsibilities

Authorized Users are responsible for:

a. Taking reasonable steps to protect sensitive information entrusted to them wherever it is located, e.g., held on physical documents, stored digitally, communicated over voice or data networks, exchanged in conversation, collaboration tools, etc.

b. Completing required computer security training. Training must be current to continue to access Authority IT systems.

c. Accessing sensitive information only for a defined business purpose.

d. Safeguarding any physical key, ID card or computer/network account that allows you to access NFTA information.

e. Selecting secure passwords for their computer accounts and for always keeping those passwords secret. High quality password manager applications are acceptable for storing passwords.

f. Protecting their files when sharing to ensure only intended recipients can access.

g. In accordance with the NFTA Incident Response Plan, reporting all suspected security issues to the Help Desk immediately.

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

i. Involving the CTO in any discussions with vendors and subcontractors in all matters concerning the selection of IT resources for Authority projects.

j. Adhere to the Mobile Device policy when requesting and using an authorized NFTA portable device.

k. Only using approved methods when accessing Authority cloud services or other applications with personal computing devices such as a smartphone, laptop, or home PC. Cloud services include O365 Outlook, Teams, and any other application the Authority supports.

l. Exercise ethical judgment when accessing, selecting, reviewing, printing, downloading, uploading or sending information through the provided Internet service.

m. Exercise extreme care when sending or receiving email from Authority accounts. Users shall follow the guidance in Appendix A - Email.

n. Use solid judgment and discretion when communicating via Social Media (e.g. Facebook, X, Instagram, Snapchat, etc.) especially when posting information may reflect on the image of the NFTA, or is detrimental to the efficiency of operation of the NFTA, or would potentially interfere with or disrupt activities of the NFTA. Users must not conduct Authority business over Social Media unless authorized. Users shall follow the guidance in Appendix B – Social Media.

o. Exercise extreme care when utilizing Artificial Intelligence (AI) services. Users shall follow the guidance in Appendix C – Artificial Intelligence

p. Understanding that Authority management reserves the right to regulate and monitor emails or other messages sent or received, Internet traffic, inspection of data stored on personal file directories, hard disks, mobile devices and removable media on all NFTA IT resources. Employees should expect no privacy when using the Authority network or Authority resources. Monitoring policy details are in Appendix D – Monitoring.

4. Unacceptable Use

The following is a list of Unacceptable Uses of NFTA IT resources. The Authority may take steps to report and prosecute violations of this policy, in accordance with Authority standards and applicable laws. Violators can be subject to loss of privileges, and disciplinary action, up to and including termination of employment. This list does not cover every possible Unacceptable Use but provides many key examples.

It is Unacceptable for an NFTA IT user to:

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

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

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

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

e. Make unauthorized offers for products or services

f. 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

g. Knowingly attempting to use any type of malware, worm, virus etc.

h. 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.

i. Attempt to gain access to systems and/or information for which they are unauthorized, or attempt to acquire the computer account and password of authorized users

j. Use someone else's account

k. Users must not write passwords down in obvious places, store in clear text anywhere, or give them 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. The use of an approved password manager is permitted.

l. Users may not permit any other person, including other authorized users, to access Authority computer systems with their personal computer account.

m. Allow others to use a personal device without direct supervision.

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

o. Attempt to impersonate another person or forge an email header.

p. Send spam, solicitations, chain letters, or pyramid schemes.

q. Knowingly misrepresent the Authority's capabilities, business practices, warranties, pricing, or policies.

r. Conduct non-Authority-related business.

s. Authorized Users must not install network hardware or software that provides network services (e.g. routers, switches, wireless access points, etc.) without prior approval from the CTO or designate.

5. Compliance

APPENDICES

Appendix A - Email

The following are the email standards:

Sending Email

When using an Authority email account, email must be addressed and sent carefully. Employees should keep in mind that the Authority loses any control of email once it is sent external to the Authority network. Employees must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the Authority avoid the unintentional

disclosure of sensitive or non-public information.

General Guidelines and Personal Use

- 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.
- Employees are 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.
- Basic 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.
- Use encrypted email when sending sensitive information.
- It is Authority policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails shall not contain attachments of excessive file size. The system is currently set to 50Mb for internal emails and 10 MB for external emails. However, it may be altered with permission from the Chief Technology Officer (CTO).

Business Communications and Email

- The email system is the property of the Authority and its primary focus is for business communications. However, occasional incidental personal use is allowed as long as it does not interfere with business operations.
- The Authority uses email as an important communication medium for business operations. Employees of the Authority email system are expected to check and respond to email in a consistent and timely manner during business hours.
- Employees must recognize that email sent from an Authority account reflects on the Authority, and, as such, email must be used with professionalism and courtesy.

Email Signature

- Email signatures (contact information appended to the bottom of each outgoing email) may or may not be used, at the discretion of the individual employee. Employees are asked to keep any email signatures professional in nature.

Auto-Responders

- The Authority recommends the use of an auto-responder (if the email system is equipped with such a feature) if the employee will be out of the office for an entire business day or more. The auto-response should notify the sender that the employee is out of the office, the date of the employee's return, and who the sender should contact if immediate assistance is required.

Mass Emailing

- The Authority makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with the Authority's employees or customer base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.
- The Authority requires compliance with applicable laws governing the sending of mass emails. For this reason and to be consistent with good business practice, the Authority requires that email sent to more than twenty

(20) recipients external to the Authority have the following characteristics:

- The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.
- The email must contain a subject line relevant to the content.
- The email must contain contact information, including the full physical address, of the sender.
- The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.
- Note that emails sent to Authority employees, existing customers, or persons who have already inquired about the Authority's services are exempt from the above requirements.

Opening Attachments

Employees must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Employees must:

- Never open unexpected email attachments
- Never open email attachments from unknown sources
- Never click links within email messages unless the employee is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted emails can hide a malicious URL.
- The Authority may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

Authority Ownership of Email

Employees are advised that the Authority owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the Authority and may be subject to use for purposes not anticipated by the employee. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, employees are advised that email sent to or from certain public or governmental entities may be considered public record.

Contents of Received Emails

Employees must understand that the Authority has little control over the contents of inbound email, and that this email may contain material that the employee may find offensive. If unsolicited email becomes a problem, the Authority may attempt to reduce the amount of this email that the employees receive, however no solution will be 100 percent effective. The best course of action is not to open emails that, in the employee's opinion, seem suspicious. If the employee is particularly concerned about an email, or believes that it contains illegal content, they should notify their supervisor or the IT Help Desk.

External and/or Personal Email Accounts

- The Authority recognizes that employees may have personal email accounts in addition to their Authority-provided account.
- Employees should use the Authority email system for all business-related email. Employees are prohibited from sending business email from a non-Authority-provided email account without permission from the Executive Director.
- Employees are prohibited from accessing external or personal email accounts from the Authority network with the exception of using a personal device on the guest Wi-Fi network.

Confidential Data and Email

- As with any Authority passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the CTO, the Authority may further secure email with certificates, two factor authentication, or another security mechanism.
- Email is an insecure means of communication. Employees should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient. The Authority recommends, but does not require, the encryption of email that contains confidential information. This is particularly important when the email is sent to a recipient external to the Authority.

Authority Administration of Email

- The Authority will use its best effort to administer the Authority's email system in a manner that allows the employee to both be productive while working as well as reduce the risk of an email-related security incident.
- The Authority will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed a) contrary to this policy, or b) a potential risk to the Authority's IT security. No method of email filtering is one hundred percent (100%) effective, so employees must be cognizant of this policy and use common sense when opening emails.
- Many email and/or anti-malware programs will identify and quarantine emails that they deem suspicious. This functionality may or may not be used at the discretion of the CTO.

Email Disclaimers

The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in the Authority's risk reduction efforts. The Authority requires the use of email disclaimers on every outgoing email, which must contain the following notices:

- The email is for the intended recipient only
- The email may contain private information
- If the email is received in error, the sender should be notified and any copies of the email destroyed
- Any unauthorized review, use, or disclosure of the contents is prohibited. An example of such a disclaimer is:

The information contained in this email is intended only for the use of the person or entity to whom it is addressed and may contain information that is confidential and exempt from disclosure under applicable laws. If you read this message and are not the addressee, you are notified that use, dissemination and reproduction of this message is prohibited. If you have received this message in error, please notify the sender immediately and delete this message from your system.

Email Deletion

- Employees are encouraged to delete unimportant/non-work-related emails/spam periodically. The goal of this policy is to keep the size of the employee's email account manageable and reduce the burden on the Authority to store and backup unnecessary email messages.
- Employees are strictly forbidden from deleting email in an attempt to hide a violation of this or another Authority policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

Address Format

- Email addresses must be constructed in a standard format in order to maintain consistency across the Authority. The standard format is firstname.lastname@nfta.com

- The Authority can choose virtually any format, as long as it can be applied consistently throughout the organization. Special characters like apostrophes and hyphens are possible but are discouraged for simplicity. The intent of this policy is to simplify email communication as well as provide a professional appearance.

Email Aliases

- The use of an email alias, which is a generic address that forwards email to an employee account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for Authority email, as well as (often) the names of Authority employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack. A few examples of commonly used email aliases are:

    - sales@Authoritydomain.com
    - techsupport@Authoritydomain.com
    - pr@Authoritydomain.com
    - info@Authoritydomain.com

- The Authority may or may not use email aliases, as deemed appropriate by the CTO and/or executive team. Aliases may be used inconsistently, meaning the Authority may decide that aliases are appropriate in some situations but not others, depending on the perceived level of risk.

Email Account Activation

- Email accounts will be set up for each employee determined to have a business need to send and receive Authority email. Accounts will be set up at the time a new hire starts with the Authority, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.
- Email accounts may be given to non-employees, contractors, or other individuals authorized to conduct certain aspects of the Authority's business. In these cases, the Authority should consider designating the temporary or non-employee status of the account in the account name, such as:

    - firstname.lastname@temporary.nfta.com
    - firstname.lastname@contractor.nfta.com
    - firstname.lastname@consultant.nfta.com

Account Termination

When an employee leaves the Authority, or their email access is officially terminated for another reason, the Authority will disable the employee's access to the account by password change, disabling the account, or another method. The Authority is under no obligation to block the account from receiving email and may continue to forward inbound email sent to that account to another employee, or set up an auto-response to notify the sender that the employee is no longer employed by the Authority.

Storage Limits

As part of the email service, email storage may be provided on Authority servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the CTO. Storage limits may vary by employee or position within the Authority.

Data Leakage

- Data can leave the network in a number of ways. This can occur unintentionally by an employee with good intentions. For this reason, email poses a particular challenge to the Authority's control of its data.
- Unauthorized emailing of Authority data, confidential or otherwise, to external email accounts for the purpose of saving this data external to Authority systems is prohibited. If an employee needs access to information from external systems (such as from home or while traveling), that employee shall notify their supervisor rather than emailing the data to a personal account or otherwise removing it from Authority systems.
- The Authority may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the CTO.

Sending Large Emails

- Email systems were not designed to transfer large files and as such emails shall not contain attachments of excessive file size. The Authority does not wish to impose a hard limit on email attachment size, but employees must exercise discretion so that the system isn't unnecessarily strained.
- The employee must recognize the additive effect of large email attachments when sent to multiple recipients and use restraint when sending large files to more than one person.

Appendix B - Social Media

The specifications for Social Media are maintained within the Social Media Policy (1-03-05)

Appendix C - Artificial Intelligence

All employees are expected to adhere to the cyber security best practices when using any system which features Artificial Intelligence (AI) tools:

- Only AI tools approved by the IT department can be used on Authority computers and devices
- Evaluation of AI tools: AI tools must be evaluated for security and privacy considerations before using. This includes reviewing the tool’s security features, terms of service, developer reputation and privacy policy.
- Protection of confidential data: Employees must not upload or share any data that is confidential, proprietary, or protected by regulation without prior approval from the appropriate department. This includes data related to customers, employees, or partners.
- Access control: Employees must not give access to AI tools outside the company without prior approval from the appropriate department or manager and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.
- Use of reputable AI tools: Employees must only use reputable AI tools and be cautious when using tools developed by individuals or companies without established reputations. Any AI tool used by employees must meet our security and data protection standards.
- Compliance with security policies: Employees must apply the same security best practices we use for all company and customer data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies.
- Data privacy: Employees must exercise discretion when sharing information publicly. Before uploading or sharing any data into AI tools employees must ask themselves:

    - Do I need to obtain approval from my manager before sharing this information?
    - Would I be comfortable sharing this information outside of the company?
    - Would we be okay with this information being leaked publicly?

Appendix D - Monitoring

- Employees should expect no privacy when using the Authority 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 use of IT resources. 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.
- The Authority will investigate properly identified allegations of misuse and will report such violations to the employee's direct supervisor or Authority management. Actions taken by the direct supervisor may result in loss of privileges, disciplinary action, up to and including termination of employment.
- IT Services, under the guidance of Human Resources and the Office of General Counsel, may at any time perform additional investigation and ongoing review, monitoring, and investigation (including transmissions by telephone, email, websites or social media) of specific individuals.