Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Title: **EMAIL POLICY**
Policy Number: **06-01-17**
Issue Date: **07-16-2018**
Revision Date: **05-18-2021**

I. PURPOSE

The purpose of this policy is to detail the usage guidelines for the email system for the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority"). This policy will help the Authority reduce risk of an email-related security incident, foster good business communications both internal and external to the Authority, and provide for consistent and professional application of the Authority's email principles.

A) Overview

Email is an essential component of business communication; however, it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on the Authority's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

B) Scope

The scope of this policy includes the Authority's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, mobile devices, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the Authority network. This policy is applicable to all employees of the Authority and all other individuals with access rights (i.e., consultants, interns, temporary workers, etc.) and applies to any and all use of corporate IT resources, including but not limited to, computer systems, email, the network, information on any of these systems, and the corporate Internet connection.

II. POLICY

A) Proper Use of Authority Email Systems

Employees are asked to exercise extreme care when sending or receiving email from Authority accounts. Additionally, the following applies to the proper use of the Authority email system.

1) 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.

2) Personal Use and General Guidelines

The email system is 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 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.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The system is current set to 50Mb for internal emails and 10 MB for external emails. However, it may be altered with permission from the Chief Information Officer (CIO).

Please note that the topics above may be covered in more detail in other sections of this policy.

3) Business Communications and Email

The Authority uses email as an important communication medium for business operations. Employees of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, employees are asked to recognize that email sent from an Authority account reflects on the Authority, and, as such, email must be used with professionalism and courtesy.

4) 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.

5) 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.

6) 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 thesender.
- 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.

7) Opening Attachments

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

- 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.

8) Monitoring and Privacy

Employees should expect no privacy when using the corporate 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 and all use of the computer network. 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.

9) Authority Ownership of Email

Employees should be 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, the employee should be advised that email sent to or from certain public or governmental entities may be considered public record.

10) 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 finds 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 to not 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, he or she should notify his or her supervisor or the IT Help Desk.

B) External and/or Personal Email Accounts

The Authority recognizes that employees may have personal email accounts in addition to their Authority-provided account. The following sections apply to non-Authority provided email accounts:

1) Use for Authority Business

Employees must use the corporate email system for all business-related email. Employees are prohibited from sending business email from a non-Authority-provided email account.

2) Access from the Authority Network

Employees are prohibited from accessing external or personal email accounts from the corporate network with the exception of using a personal device on the guest Wi-Fi network.

C) Confidential Data and Email

The following sections relate to confidential data and email:

1) Passwords

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 CIO, the Authority may further secure email with certificates, two factor authentication, or another security mechanism.

2) Emailing Confidential Data

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.

D) 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.

1) Filtering of Email

A good way to mitigate risk from email is to filter it before it reaches the employee so that the employee receives only safe, business-related messages. For this reason, 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 are asked to be cognizant of this policy and use common sense when opening emails.

Additionally, 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 CIO.

2) 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.

3) Email Deletion

Employees are encouraged to delete email periodically when the email is no longer needed for business purposes. 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.

However, 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.

4) Retention and Backup

Email should be retained and backed up in accordance with the applicable policies, which may include, but are not limited to, the Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

5) 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.

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.

6) Email Aliases

Often 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 CIO 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.

7) 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.

At times, 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

8) 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.

9) 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 CIO. Storage limits may vary by employee or position within the Authority.

E) Prohibited Actions

The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. Employees may not use the corporate email system to:

- Send any information that is illegal under applicable laws.
- Access another employee's email account without a) the knowledge or permission of that employee - which should only occur in the extreme circumstances, or b) the approval of Authority executives in the case of an investigation, or c) when such access constitutes a function of the employee's normal job responsibilities.
- Send any emails that may cause embarrassment, damage to reputation, or other harm to the Authority.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent the Authority's capabilities, business practices, warranties, pricing, or policies.
- Conduct non-Authority-related business.

The Authority may take steps to report and prosecute violations of this policy, in accordance with Authority standards and applicable laws.

1) Data Leakage

Data can leave the network in a number of ways. Often this occurs 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 should 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 CIO.

2) Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The Authority does not wish to impose a hard limit on email attachment size, but asks the employee to exercise discretion so that the system isn't unnecessarily strained.

The employee is further asked to 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.

F) Applicability of Other Policies

This document is part of the Authority's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

III. COMPLIANCE

This policy shall take effect upon publication. Compliance is expected with all applicable laws and Authority policies and standards. IT may provide notification of amendments to its policies and standards at any time; compliance with amended policies and standards is expected.

Any violation of this policy may subject the employee to disciplinary action, civil penalties, and/or criminal prosecution. The Authority will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

IV. DEFINITIONS

Auto Responder - an email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees, who will not have access to email for an extended period of time, to notify senders of their absence.

Certificate - also called a ”Digital Certificate”." A file that confirms the identity of an entity, such as an Authority or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage - also called “Data Loss”, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by employees with good intentions.

Email - short for electronic mail, email refers to electronic letters and other communication sent between networked computer employees, either within an Authority or between companies.

Encryption - the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Mobile Device - a portable device that can be used for certain applications and data storage. Examples are Personal Digital Assistants (PDAs) or Smartphones.

Password - a sequence of characters that is used to authenticate an employee to a file, computer, network, or other device. Also known as a passphrase or passcode.

Spam - unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

Smartphone - a mobile telephone that offers additional applications, such as PDA functions and email.

Two Factor Authentication - a means of authenticating an employee that utilizes two methods: something the employee has, and something the employee knows. Examples are smart cards, tokens, or biometrics, in combination with a password.