Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHONOLOGY (IT)**
Section: **ADMINISTRATIVE SERVICES**
Title: **INFORMATION SECURITY BREACH AND NOTIFICATION ACT**
Policy Number: **06-01-14**
Issue Date: **12-30-2005**
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") complies with the provisions of the State of New York Information Security Breach and Notification Act, requiring notification to Authority employees in the event there is any breach of security of computerized data that contains private information about that individual.

The data covered by this law is an individual's name in combination with any one or more of the following (unless all the information is encrypted):

- Social Security number.
- Driver license number or non-driver identification card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

II. POLICY

The State of New York Information Security Breach and Notification Act requires that owners of computerized data must give notice of any security breach to affected persons in the most expedient time possible and without unreasonable delay. The Act also allows for substitute notice (e.g., via posting on the agency's website and notification to major statewide media) in certain circumstances. The Act specifies that an agency that maintains its own notification procedures as part of an information security policy shall be deemed to be in compliance with the Act's notification requirements, as long as the agency notifies people in accordance with its policies in case of a security breach and as long as the agency is otherwise consistent with the Act's timing requirements for notification.

III. PROCEDURE

If an employee has a concern regarding a breach of security or to report a breach (where an unauthorized individual has acquired unencrypted private information) at the Authority, the employee should contactthe IT Help Desk via phone: 716-855-7370 or via email: help.desk@nfta.com.

1. INITIAL RESPONSE. If a breach of security is suspected on a computing system that contains or has network access to unencrypted private data, the Systems Support Specialist and/or Network Administrator will immediately:

    a) Remove the computing system from the Authority network.

    b) Conduct a local analysis of the breach to determine the number of individuals whose protected data may have been acquired.

    c) Notify the Chief Information Office (CIO), who will notify the Chief Financial Officer (CFO) if there is a reasonable belief that protected data may have been acquired, regardless of the quantityof information that might have been compromised.

2. NOTIFICATION OF SECURITY BREACH. If, after consulting with IT security staff and the CIO, the CFO is reasonably certain that a security breach has occurred, the CFO will immediately report the breach to the Executive Director and if warranted, the Authority's Transit Police Department.

3. RECOMMENDATION CONCERNING NOTIFICATION TO INDIVIDUALS IMPACTED BY THE SECURITY BREACH. The Executive Director will bring together the appropriate Authority Officials to make a determination whether criteria for notification under Section 208 of the State

Technology Law has been met and to determine the means of notification. If such notification is required, as follows:

- Written Notice
- Electronic notification provided (i) the affected individual has expressly consented to its receipt and (ii) logs are kept
- Substitute notice, pursuant to State Technology Law Section 208 (5) (c)
- If more than Five Thousand (5,000) persons must be notified at one time, consumer-reporting agencies must also be notified