Reference: **SAFETY**
Section: **GENERAL**
Title: **SECURITY SYSTEMS**
Policy Number: **07-01-07**
Issue Date: **02-08-2013**
Revision Date: **05-18-2021**

I. PURPOSE

The purpose of this policy is to establish control of the operation and administration of the Security Systems of the Niagara Frontier Transportation Authority and the Niagara Frontier Transit Metro System, Inc. (collectively referred to as "NFTA" or "Authority").

II. APPLICABILITY

This policy applies to all Authority employees.

III. POLICY

The operation and administration of the Authority Security Systems, which are comprised of the Closed-circuit Television (CCTV) and Access Control Systems, shall adhere to the guidelines as established by this policy.

The Security Systems were installed at the Authority's facilities and in revenue vehicles to enhance security and safety for our patrons and employees.

A) NFTA Security Systems Oversight Committee

The Oversight Committee is responsible for developing and maintaining this policy and all procedures pertaining to the Authority Security Systems. Workstation, camera, and access control locations, as well as system users and the level of individual user Security Systems access privileges will be determined and assigned by this Committee. The Committee is madeup of the following Authority personnel:

- Chief of Police
- Director, Health, Safety and Environmental Quality (HSEQ)
- Manager, System Security
- CCTV System Administrator
- Access Control System Administrator
- Manager, Claims

B) Request for Access

All employee requests for access to the Authority Security Systems must be sent to the Oversight Committee for authorization and determination of the level of privileges. Access to the Security Systems will be limited to those employees that have an operational need, and they will only be provided with access to their own operational area(s).

C) Passwords

Each system user will be assigned a username and password. This username and password can only be used by them and is not to be shared with anyone else. When using the Security Systems, users will have to login using their assigned username and password and are responsible for all activities that take place under their login.

Users must sign-off the system whenever they leave the workstation area. Live monitoring systems used by the Controllers and Police Dispatch can be left on and are exempt from this requirement.

Passwords must be at least eight (8) characters long and contain at least one letter and one number. Passwords must be reset every ninety (90) days as required by the system. Passwords must not be written down on or near the workstation; all users are required to keep their passwords private.

D) Request for DVD

The viewing of video should only be done by those employees that are authorized to do so.

There are two primary CCTV systems in place at the Authority. The Pelco Endura system has been installed at most Authority facilities and is a fixed networked CCTV system managed by the Authority's Police Department. The Revenue Vehicle CCTV systems are separate from the CCTV system and the Metro Maintenance Department manages the operation of these systems.

All facility video digital copy requests must go to the Authority's Police Department through an official request. The Authority Police Department will make the copy and provide it to the requesting management employee. It is the responsibility of the requesting management employee to control the digital copy and ensure that it is secured and does not become available to unauthorized individuals.

All vehicle video digital copy requests must go to the appropriate Metro Maintenance Department via an official request. The Metro Maintenance Department will make the copy and provide it to the requesting management employee. It is the responsibility of the requesting management employee to control the digital copy and ensure that it is secured and does not become available to unauthorized individuals.

Requests for copies of videos by outside agencies or individuals, other than FOIL requests and requests by police agencies investigating a crime, must go through the Oversight Committee. Any FOIL requests for videos will be handled pursuant to the FOIL regulations. Any requests by police agencies for copies of videos required to investigate a crime shall be approved by the Chief of Police or his authorized designee.

Anyone making a copy of the video being viewed on a workstation using a cell phone or other type of video recording device will be in violation of this policy unless the Oversight Committee has granted prior approval.

Any copy of a video that has been made without approval of the Authority Police Department, other than a copy made by the Metro Maintenance Department or a copy made pursuant to the FOIL regulations, will be deemed an uncontrolled copy and will be subject to confiscation.

E) Destruction of Copied Material(s)

All Authority video is considered protected Authority confidential information and must be safeguarded. Workstations are to be logged off when not in use, and all hard copy (DVDs and printed copies) must be locked up at all times if not in use. If the copies are no longer needed, they must be destroyed properly by shredding or other method that will ensure permanent destruction.