Reference: **ADMINISTRATIVE SERVICES - INFORMATION TECHNOLOGY (IT)**
Section: **ADMINISTRATIVE SERVICES**
Title: **INFORMATION SECURITY POLICY**
Policy Number: **06-01-20**
Issue Date: **02-4-2026**
Revision Date:

I. PURPOSE

At Niagara Frontier Transportation Authority (NFTA), we recognize the critical importance of information security in our operations. This policy outlines our commitment to establishing and maintaining an effective information security management system in alignment with NYS-P03-002 – Information Security Policy.

This policy acts as an umbrella document to all other NFTA security policies and associated standards and defines our commitment to the following objectives:

a) **Confidentiality**: We are committed to ensuring the confidentiality of our information assets by implementing appropriate controls to prevent unauthorized access, disclosure, or use of sensitive information.
b) **Integrity**: We strive to maintain the integrity of our information assets by protecting them against unauthorized modifications, ensuring accuracy, and preventing data corruption.
c) **Availability**: We aim to ensure the availability of our information assets by implementing measures to protect against interruptions to business operations and minimizing the impact of incidents.
d) **Compliance**: We are committed to complying with all applicable legal, regulatory, and contractual requirements related to information security.
e) **Risk Management**: We will establish and maintain a risk management framework to identify, assess, and mitigate information security risks in a systematic and ongoing manner.
f) **Incident Response**: We will develop processes to detect, respond to, and recover from security incidents.
g) **Awareness and Training**: We will foster a culture of security awareness and provide regular training to authorized users.

A. Overview

This policy benefits NFTA by defining a framework that will ensure appropriate measures are in place to protect the confidentiality, integrity, and availability of NFTA information; and ensure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures, and practices, and know how to protect NFTA information.

B. Scope

The scope of this policy includes all Authorized Users, defined as employees of the Authority and all other individuals with access rights (i.e., consultants, interns, temporary workers, etc.) to Authority-owned / Authority-provided computers or require access to the corporate network and/or systems. In a 2019 IT audit, the Office of the State Comptroller determined that the NFTA must adhere to the State Information Security Policy established by the Office of Information Technology Services.

This policy applies to all information assets owned, controlled, or processed by NFTA, including but not limited to:

- Digital information stored on servers, databases, and electronic devices.
- Physical records, documents, and media containing sensitive information.
- Communication networks, systems and network connected devices.
- Software applications, tools, and utilities.
- Personnel and customer information.
- Intellectual property, trade secrets, and proprietary data.

II. Information Security Responsibilities

NFTA Management Team is responsible for:

1. setting the risk tolerance levels for NFTA to enable management to implement the appropriate safeguards against threats to information security
2. establishing a target maturity level for information security.
3. ensuring Department Heads fulfill the responsibilities outlined within the information security policies and standards and hold them accountable for the implementation of the applicable components relevant to their departments;
4. ensuring adequate resources and funding is made available for the Information Security program;
5. identifying NFTA information security responsibilities and goals and integrating them into relevant processes;
6. promoting a culture of security within the organization by communicating the requirements of, and supporting the consistent implementation of, information security policies and standards; and
7. establishing information ownership and classification policies and practices to govern the collections, handling, storage and protection of data.

NFTA Chief Technology Officer (CTO) is responsible for:

1. Developing and maintaining the NFTA's information security program and strategy, including measures of effectiveness;
2. establishing and maintaining enterprise information security policies and standards;
3. establishing the requirements for the assessment and treatment of information security-related risks facing NFTA;
4. providing incident response coordination (may be delegated) and expertise; and
5. establishing a business continuity and disaster recovery program (BC/DRP) to ensure that appropriate and reasonable measures are in place to provide for the continued availability of IT services that support NFTA business activities.

NFTA Information Security Officer (ISO) is responsible for:

1. overseeing the development, implementation, and monitoring of information security measures;
2. overseeing the management of risk assessments and security incidents and providing guidance on information security matters resulting from these activities;

3. defining roles and responsibilities for information security policies and determining methods of implementing and enforcing security policies;
4. assessing NFTA compliance with information security policies and legal and regulatory information security requirements;
5. representing and ensuring security architecture considerations are addressed;
6. advising on security issues related to procurement of products and services; and
7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures.

Authorized Users are responsible for:

1. understanding their information security responsibilities and comply with the policies, procedures, and guidelines defined by the organization;
2. taking appropriate measures to protect sensitive information entrusted to them wherever it is located, e.g., held on physical documents, stored digitally including cloud and AI services, on smartphones, communicated over voice or data networks, exchanged in conversation, collaboration tools, etc.;
3. accessing sensitive information only for a defined business purpose;
4. safeguarding any physical key, ID card or computer/network account that allows you to access Institutional Information; and
5. reporting any activities that they suspect may compromise NFTA systems or information.

Human Resources and Talent Management Department is responsible for:

1. facilitating background checks on authorized users; and
2. supporting the awareness and training of Authorized Users.

III. POLICY

NFTA IT will maintain information security policies and standards that are applicable and enforceable within the NFTA enterprise. The CTO will establish and implement these policies to ensure the following control areas are addressed for the protection of information assets:

a) **Separation of Duties:** To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility will be implemented where appropriate. Whenever separation of duties is not technically feasible, other compensatory controls will be implemented, such as monitoring of activities, audit trails, and management supervision.

b) **IT Risk Management**: Practices will be defined and applied for the assessment and treatment of information security-related risks facing NFTA.

c) **Information Classification and Handling**: Information assets will be classified based on their sensitivity and guidelines established for their appropriate handling, storage, transmission, and disposal. The Information Classification and Handling Policy must address data ownership and the sharing and release of information with outside parties.

d) **IT Asset Management**: Asset Management practices will be implemented including the implementation of procedures for proper handling and disposal of assets, as well as maintaining an accurate asset inventory.

e) **Personnel Security**: Personnel Security practices will be implemented including conducting background checks.

f) **Incident Management**: An incident management process will be implemented to detect, respond to, and recover from, security incidents promptly. This includes reporting incidents, investigating their root causes, and implementing corrective actions to prevent their recurrence.

g) **Physical and Environmental Security**: Physical and environmental security measures will be implemented to protect the premises that house the organization's IT equipment and storage areas from unauthorized access, theft, damage, or destruction.

h) **Account Management and Access Control**: Account management and access controls will be implemented to ensure that only authorized individuals have access to information assets. This includes user authentication, access rights management, and segregation of duties.

i) **Systems and Operations Security**: Procedures for the secure operation, maintenance, and monitoring of information systems will be implemented to ensure their availability, integrity, and confidentiality. Controls will be implemented to manage changes to information systems, and protect against malware, unauthorized software, and other threats.

j) **Network Security**: To help ensure the reliable operation of the network, Controls will be implemented to secure NFTA communication networks.

k) **Vulnerability and Patch Management:** Patch and vulnerability management processes will be implemented to ensure systems are configured securely and updated with the latest security patches. Where patches cannot be applied, mitigating controls will be considered where appropriate.

l) **Supplier Relationships**: Guidelines for selecting, engaging, and managing third-party suppliers will be implemented to ensure they meet our information security requirements and protect the confidentiality, integrity, and availability of our information assets.

m) **Citizens' Cyber Security Notification**: Processes will be implemented to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with NY State Technology Law, Article II, Internet Security and Privacy Act

n) **Training and Awareness:** NFTA will provide appropriate training and awareness programs to ensure that employees and contractors understand their responsibilities regarding information security. Training will be conducted upon onboarding and periodically thereafter to address changes in technology, threats, or regulations

IV. 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.

A. Exceptions

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, an exception shall be requested through the CTO as noted below. An exception may be granted by the CTO or the Executive Director.

V. DEFINTIONS

Authorized Users are defined as employees, contractors and third parties with approved access to NFTA systems.