Reference:	**ADMINISTRATIVE SERVICES - MIS**
Title:	**Patch Management Policy**
Policy Number:	**06-01-09**
Effective Date:	**06-15-2020**
Revision Date:	

I. PURPOSE

The Purpose of this policy is to ensure compliance by the Niagara Frontier Transportation Authority (the "NFTA") and Niagara Frontier Transit Metro System, Inc. ("Metro") with New York State's Information Technology Standards. This policy is considered an extension of the New York State (NYS) IT Policies and is subject to change based on updates to those policies.
If a conflict occurs the NYS policy supersedes this policy.

II. APPLICABILITY

This Policy applies to all NFTA and Metro owned, leased, and operated computer systems.

III. POLICY

A. The IT department of the NFTA is responsible for patch management of all NFTA and Metro owned systems. Patch management involves the identification, tracking, application and testing of software updates to operating systems, applications, firmware, etc. This authority extends to the verification of compliance of all third-party entities that house, store, or process, NFTA data.

B. Patches are required protect the NFTA from security vulnerabilities, software failures, and to ensure continued vendor support.

C. Patch management will be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.

D. Vulnerability advisories from the NYS ITS Chief Information Security Office (CISO) Cyber Security Operations Center (CSOC) are based on a NYS specific analysis of impact and will be considered high impact vulnerabilities, regardless of CVSS score.

E. To the extent possible, the patching process must follow the timeline contained in the table below:

Impact/Severity	**Patch Initiated**	**Patch Completed**
High	Within **24 hours** of patch release	Within **1 week** of patch release
Medium	Within **1 week** of patch release	Within **1 month** of patch release
Low	Within **1 month** of patch release	Within **2 months** of patch release, unless ISO determines this to be an insignificant risk to the environment

F. If patching cannot be completed in the timeframe listed in the table above, compensating controls must be put in place within the timeframes above and the exception process must be followed.

G. If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.

IV. RELATED DOCUMENTS

NYS-ITS-S15-001 – NY State Patch Management Policy

National Institute of Standards and Technology, Special Publication 800-40, Guide to Enterprise Patch Management Technologies

Common Vulnerability Scoring System

National Vulnerability Database Vulnerability Severity Rankings

NYS Vulnerability Scanning Standard