Reference: **ADMINISTRATIVE SERVICES - MIS**
Title: **Support and Obsolete Software-Hardware Policy**
Policy Number: **06-01-19**
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. All software that is used within the NFTA must be maintained at a vendor-supported level to be connected to a NFTA network.

B. All hardware that is used within the NFTA must be maintained at a vendor-supported level to be connected to a NFTA network.

C. Software upgrades, in coordination with the business areas are the responsibility of the IT department. Upgrades will be completed at least yearly to ensure systems are kept current and support all current operating system and hardware patches.

D. Vendor support agreements are required for all current production systems of the NFTA. The IT department will be responsible for these agreements to ensure that they are accurate, compliant with NYS IT and NFTA IT Policies and support the needs of the NFTA.

E. Vendor support agreements shall include all third-party applications required by the vendor application. The agreement shall enforce the requirement that the vendor maintains support for the updated versions of the required third-party applications. This will ensure proper security patching of the vendor software as well as the third-party applications.

F. Software support agreements shall be maintained to cover both application support and application upgrades. This will ensure proper user support and the ability to comply with system security patches.

G. Hardware support agreements shall be maintained to cover hardware failures and firmware/operating system upgrades. This will ensure that any/all security threat notices can be applied to effected systems.

H. Software and/or hardware that is approaching end-of-life must have a transition plan for its replacement or decommissioning at least one year before the date of end-of-life.

I. Software that has reached End-of-Life or End-of-Support must be removed in a timely manner. If this software is needed for business operations, then the potential security threats of the software must be evaluated, and proper controls must be put in place. The controls include, but are not limited to, increased vulnerability and penetration scanning, network segmentation, network isolation, firewall wrapping, and/or removal from the network.

J. Hardware that has reached End-of-Life or End-of-Support must be removed in a timely manner. If this hardware is needed for business operations, then the potential security threats of the hardware must be evaluated, and proper controls must be put in place. The controls include, but are not limited to, increased vulnerability and penetration scanning, network segmentation, network segregation, firewall wrapping, and/or removal from the network.

IV. RELATED DOCUMENTS

NYS-P03-002 – NY State Information Security 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