DEVELOPMENT AUTHORITY OF THE NORTH COUNTRY

AUTHORITATIVE POLICY: Information Technology and Security

Resolution No. 2013-10-01

PROCEDURE: 2.4 - Computer Virus and Malware

1.0 Introduction

Policy:
The Authority shall protect its IT assets from infection by malicious software, viruses or malware.

Purpose:
To prevent data loss, corruption, or misuse of Authority computing resources or information that may occur when malware is introduced to the Authority's IT network.

Scope:
This policy applies to all Authority personnel and to all computer hardware and software comprising the Authority's IT network.

Responsibilities:
The IT Director is responsible for implementing malware control procedures, evaluating and updating appropriate computer malware detection software, and training users on computer malware control.

The IT Director is responsible for coordinating actions required to prevent computer malware outbreaks, coordinating all actions required to eradicate the malware, and recovering data to the greatest extent possible.

The IT Director is responsible for installing and maintaining malware protection on IT assets and for cleaning malware infections from Authority applications, devices, etc.

Network/computer users are responsible for following the guidelines of this policy document and for immediately notifying the IT Director in the event a malware attack is suspected.

Definitions:
Malware - Short for "malicious software", malware is designed to damage, disrupt, or abuse an individual computer or an entire network and/or steal or corrupt an organization's most valuable and sensitive data. Some viruses, worms, and Trojan horses are examples of malware.

Spam, or junk e-mail – Unsolicited commercial e-mail sent in bulk over the Internet. Spam puts a cost and a burden on recipients by clogging up network bandwidth, consuming disk space, and wasting employees' time. Spam is frequently a malware vector.

User – Anyone with authorized access to the Authority technology resources including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties with valid Authority access accounts.

Subscription service – A service whereby a software vendor offers support for its product, usually for a predetermined time period. Anti-malware vendors typically include a one-year subscription (for updates, notices, etc.) with the purchase of a product license. Many vendors offer fee-based subscription services whereby subscribers automatically receive notifications, security bulletins, etc, for a set period of time.

Target – The ultimate destination for malware; that which the malware is designed to attack. Boot sectors, hard disk drives, e-mail servers, and departmental (admin, accounting, etc.) servers are examples of malware targets.

Vector – How malware is carried to a computer, server, or system.

2.0 Procedure -

2.1 Malware Defense Planning

How does malware typically work and what threats exist? Malware is commonly passed to a potential target through e-mail. The person who receives the e-mail opens an attachment, which unleashes the malware, which then spreads to other computers via a shared network. (Malware may attack by other means but this is a common method.) To lessen the potential for damage to Authority's IT assets by malware, the Authority has developed and implemented a multifaceted approach to malware prevention.

To prepare Authority's Malware Defense Plan, the IT Director shall review the following items:

- IT Industry standards and best practices
- Anti-malware vendor web sites or portals
- IT security alerts and bulletins

2.2 Malware Defense Plan

The IT Staff shall ensure that operating systems, web browsers, e-mail programs, and related software are configured for optimum security.

The IT Staff shall install an anti-malware program on every PC and server and all anti-malware software shall be automatically updated through the use of a subscription service.

As vendors learn of vulnerabilities (bugs) in their software and repair them, they notify registered users, post bulletins on their web sites, and notify news media that these patches are available for download. Many vendors offer subscription services, through which the Authority may be notified of security threats and related issues and obtain software patches.

The Authority shall subscribe to one or more notification services, in order to maintain its awareness of threats and to ensure all software is updated in a timely fashion.

All anti-malware protections shall be configured so as to prevent their being disabled by users. Only the IT Director shall be allowed to temporarily disable anti-malware measures (for example, disabling a local anti-malware program to install and configure an application locally).

Users shall not be allowed to install software. Only the IT Staff shall be allowed to install approved software.

The Authority shall minimize malware risks by backing up critical information, in accordance with the IT Disaster Recovery Plan

All users shall be trained on the Malware Defense Plan at the outset. Users shall be retrained (updated) on the Plan at least once a year. The IT Director shall be responsible for Malware Defense Plan training.

All users shall sign a statement at the end of training, indicating that they have received training, that they understand the Plan, and that they will conduct their business in accordance with the Plan.

2.3 Malware Defense Plan Review

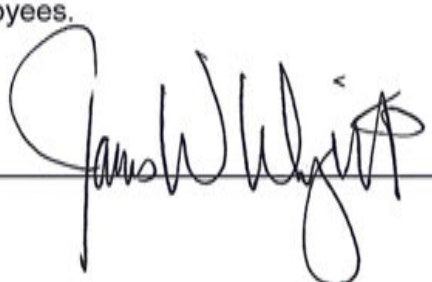
The IT Director shall periodically review all anti-malware, firewall, and other relevant logs to determine if the software is up-to-date and is performing as expected.

The IT Director shall periodically (annually, at a minimum) review security incident information to determine incident trends and progress toward Authority's goals.

The IT Director shall periodically discuss the incident information with the Technology Committee to determine its continuing applicability and conformity to Authority's requirements.

2.4 Malware Defense Plan Update

The IT Director shall incorporate updates into the Malware Defense Plan and ensure communication of Plan changes to all employees.

Date Adopted: April 1, 2014 Authorized: 

User Signature _____ Date _____