METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: ISM 11
SUBJECT: PROTECTION AGAINST MALICIOUS CODE	DISTRIBUTION DATE: 05/01/2017 EFFECTIVE DATE: 05/15/2017
ISSUING AUTHORITY: DIRECTOR OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to reduce the risk to Metropolitan Government of Nashville and Davidson County (Metropolitan Government) assets by protecting against malware.

POLICY

Metropolitan Government shall: (i) identify, report, and correct information and system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within systems; and (iii) monitor system security alerts and advisories and take appropriate actions in response.

1 Malicious Code Protection

1.1 In General

Metropolitan Government shall use a variety of controls in order to prevent such threats from exploiting any vulnerability on its information systems.

1.2 Enterprise Controls

1.2.1 Principal Risk Mitigation Methods

Metropolitan Government shall:

a. Employ malicious code protection mechanisms at information system entry and exit points, including network based anti-malware tools, and at workstations, servers, or mobile devices, where possible, located on the network to detect and eradicate malicious code that may be:
    i) Transported by e-Mail, e-mail attachments, web access, removable media, or other common means; or
    ii) Inserted through the exploitation of information system vulnerabilities;
b. Employ automated tools to monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, and, if applicable, host-based intrusion prevention system functionality;
c. Use enterprise administrative features to check the number of systems daily that do not have the latest anti-malware signatures, keeping the number of such systems small or eliminating them entirely through rapid and continuous updates;
d. Send all malware detection events to enterprise wide anti-malware administration tools and event log servers;

e. Update Malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with Metropolitan Government's configuration management policy and procedures and:
    i) Employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis;
    ii) After applying an update, verify that each system, which is automated, has received its signature update;
    iii) Provide method of retrieving signatures from an external source if system does not have access to internal update source;
    iv) Provide a backup of all anti-malware software and signatures for efficient and rapid disaster recovery.
f. Configure malicious code protection mechanisms to:
    i) Perform weekly scheduled scans of Metropolitan Government desktops, laptops and servers and real-time scans of all files on Metropolitan Government systems and external sources as the files are downloaded, created or modified in accordance with the Metropolitan Government security policy; and
    ii) Attempt to clean any detected malicious code from files or infected devices. Unsuccessful attempts to clean will result in deletion of infected file. All malicious code detection will be logged on the client device and be reported to anti-malware technicians; and
    iii) Allow clients to do manual scans of files; and
    iv) Allow clients to manually update anti-malware signatures.
g. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the Metropolitan Government information system.
h. Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc.
i. Provide a mechanism for requesting exceptions to the anti-malware scanning settings. These exceptions will be documented and periodically visited to determine if the exceptions are still needed. Exception requests processing is defined in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

1.2.2 Additional Risk Mitigation Methods

Information system entry and exit points include firewalls, e-mail servers, web servers, proxy servers, and remote-access servers. A variety of technologies and methods exist to help Metropolitan Government limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect Metropolitan Government missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, Metropolitan Government shall rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not

perform functions other than those intended. Metropolitan Government shall deploy network access control (NAC) tools, if available, or use another methodology, to verify security configuration and patch level compliance before granting access to a network.

1.2.3 Use of Honeypots

The Metropolitan Government Information Technology system shall include components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. The Metropolitan Government Information Technology system shall include components that proactively seek to identify web-based malicious code. Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots, honey clients or tar pits.

1.2.4 Management of Malicious Code Prevention

Metropolitan Government shall:

a. Centrally manage malicious code protection mechanisms;
b. Configure malicious code protection to prevent non-privileged Users from circumventing malicious code protection capabilities;
c. Confirm that the Metropolitan Government information system updates malicious code protection mechanisms only when directed by a privileged user;
d. Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external SATA devices, mounted network shares, or other Removable Media and configure real-time scanning of files so that an anti-malware scan of content from removable media is done when content is accessed;
e. Test malicious code protection mechanisms, using the EICAR anti-virus test file monthly on all anti-malware applications. This will be done in order to verify that both detection of the test case and associated incident reporting occur, as required;
f. Configure protections so that e-mail file attachments, including compressed files, are scanned at the SMTP gateway and that any attachments that are not scannable, including encrypted messages and password protected compressed files, are quarantined and e-mail administrator and recipient is notified;
g. Protect against the sending or receipt of certain types of files (e.g., .exe files) via e-mail from external resources;
h. Prepare appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements;
i. Implement procedures to verify information relating to malicious code and other “warning bulletins” are accurate and informative. Metropolitan Government anti-malware managers shall use qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, to differentiate between hoaxes and real malicious code. All users shall be made aware of the problem of hoaxes and what to do upon receipt of them.

1.2.5 User Related Requirements

Common malware prevention related policy considerations for Users include the following:

a. Users are required to scan all media from outside of Metropolitan Government for malware before they can be used;
b. Users are restricted from the use of unnecessary software, such as user applications that are often used to transfer malware (e.g., personal use of external instant messaging, desktop search engine, and peer-to-peer file sharing services), and services that are not needed or duplicate the organization-provided equivalents (e.g., e-mail) and might contain additional vulnerabilities that could be exploited by malware;
c. Users are restricted from using accounts with administrator-level privileges for any purposes other than those required by job function, which helps to limit the privileges available to malware introduced to systems by users;
d. Users are permitted access to other networks (including the Internet) only through Metropolitan Government-approved and secured mechanisms;
e. Users are required to report any malware detection to the appropriate Metropolitan Government Information Technology department.

1.2.6 Malware Incident Handling

The procedure for reporting and handling all malware-related security incidents has been defined in the *Metropolitan Government Security Incident Management Policy*.

2 Mobile Code

2.1 Decisions regarding the employment of mobile code within Metropolitan Government information systems are based on the potential for the code to cause damage to the system. Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance shall apply to both the selection and use of mobile code installed on Metropolitan Government servers and mobile code downloaded and executed on individual devices including, but not limited to, workstations, laptops, mobile devices. Policy and procedures related to mobile code shall address preventing the development, acquisition, or introduction of unacceptable mobile code within the Metropolitan Government information system[s].

Metropolitan Government shall:

a. Define acceptable and unacceptable mobile code and mobile code technologies, or block any use of mobile code;
b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;
c. Make sure the acquisition, development, and/or use of mobile code to be deployed in Information Technology systems meets the definitions as set forth in 2.1.a.;
d. Authorize, monitor, and control the use of mobile code within the Metropolitan Government Information Technology system[s] by:
    i. Considering protection against mobile code performing unauthorized actions through the use of cryptographic controls to uniquely authenticate mobile code;
    ii. Preventing the download and execution of prohibited mobile code and the automatic execution of any mobile code. (e.g., Actions required before executing mobile code shall include prompting users prior to opening e-mail attachments.);

iii. Implementing detection and inspection mechanisms to identify unacceptable/ unauthorized mobile code and take corrective action, when necessary. Such corrective action shall include, but not be limited to, blocking, quarantine, and alerting the appropriate administrator[s]; and

iv. Disabling information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300.

4/16/20147

Keith Durbin
Director of Information Technology Services
Metropolitan Government of Nashville and Davidson County

Date

REFERENCES

ISO 27002: section 12.2
Center for Internet Security Critical Control 8
NIST Special Publications 800-53 rev5, *Security and Privacy Controls for Federal Information Systems and Organizations* AT-2, SI-3
NIST Special Publications 800-83, *Guide to Malware Incident Prevention and Handling*
NIST Special Publications 800-28 v2, *Guidelines on Active Content and Mobile Code*
NIST Cybersecurity Framework ver. 2.0
NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES

0.1	1/11/2017	Draft
1.0	05/01/2017	Approved Policy
1.1	8/29/2025	Change to reflect use of rev 5 of NIST 800-53 as a reference Change to reflect use of rev 2 of NIST Cybersecurity Framework Change to reflect use of NIST 800-171 r3 as a reference