METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 12
SUBJECT: PATCH AND VULNERABILITY MANAGEMENT	DISTRIBUTION DATE: 12/15/2016
	EFFECTIVE DATE: 01/30/2017
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OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED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 ensure Metropolitan Government of Nashville and Davidson County (Metropolitan Government) reduces risks resulting from exploitation of published technical vulnerabilities.

POLICY

1. Generally

Metropolitan Government shall:

a. ensure all applications are fully supported by the manufacturer;
b. maintain all support and maintenance agreements for the lifetime of the application;
c. include language in contracts requiring timely updates of applications;
d. obtain timely information about technical vulnerabilities of information systems and applications being used;
e. evaluate its exposure to such vulnerabilities;
f. take appropriate, timely measures to address the associated risk, including patching vulnerabilities.

As set forth below, Metropolitan Government management of technical vulnerabilities is supported through the use of the controls set forth in: (i) risk assessment (see Section 2.0 below); (ii) vulnerability scanning (see Section 3.0 below); (iii) patch management (see Section 4.0 below); and (iv) security alerts, advisories and directives (see Section 5.0 below).

2. Vulnerability Risk Assessment

Metropolitan Government shall:

a. conduct an assessment of risk from technical vulnerabilities and the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores or transmits;
b. update the risk assessment on a defined schedule or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of

the system; and

c. establish expected patching timelines based on the risk assessment.
    1) Patching of security vulnerabilities should be completed as soon as adequate testing has been done to ensure risk of adverse impact due to patch deployment is less than risk of impact from vulnerability exploit.
    2) Patching of security vulnerabilities should preferably occur within two weeks of patch release.
    3) Patching addressing vulnerabilities that are being actively exploited should be tested and deployed within forty eight hours.
    4) Non security related patches, such as ones that provide additional functionality or address performance issues, should be completed as soon as adequate testing has been done, if the issue the patch addresses is being experienced and/or if the additional functionality is desired.

3. Vulnerability Scanning

Metropolitan Government shall:

a. scan for vulnerabilities in its information system and hosted applications in accordance with a defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- enumerating platforms, software flaws and improper configurations;
- measuring vulnerability impact using a defined method; and
- reporting and providing clearly documented and defined results;
- looks for code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries); and
- looks for configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

c. analyze vulnerability scan reports and results from security control assessments;
d. remediate legitimate vulnerabilities in accordance with its assessment of risk;
e. share information, when appropriate, obtained from the vulnerability scanning process and security control assessments with designated personnel throughout Metropolitan Government to help eliminate similar vulnerabilities in other information systems;
f. employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned;
g. update the list of information system vulnerabilities scanned or when new vulnerabilities are identified and reported;
h. attempt to discern what information about the information system is discoverable by adversaries;
i. include privileged access authorization for selected vulnerability scanning activities to facilitate more scanning;
j. employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities; and
k. employ an independent penetration agent or penetration team to periodically conduct a vulnerability analysis on the information system as deemed necessary.

Due to the interdependency of the Metropolitan Government network and resources, any vulnerability assessment scan shall be performed in cooperation with the Metropolitan Government Information Technology Services Department and shall follow defined and approved procedures for running such scans.

4. Patch Management and Flaw Remediation

Metropolitan Government shall:

a. identify, report and correct information system flaws;
b. test software updates and patches related to flaw remediation for effectiveness and potential side effects on the Metropolitan Government information systems before installation;
c. incorporate flaw remediation and patch management into its configuration and change management process;
d. develop processes for assessing the success and extent of patch management efforts;
e. deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe;
f. and if automated tools cannot be used, develop process for provisioning updates and ensuring updates are deployed.

5. Security Alerts, Advisories and Directives

Metropolitan Government shall:

a. receive information system security alerts, advisories and directives from designated external organizations on an ongoing basis;
b. generate internal security alerts, advisories and directives as deemed necessary;
c. disseminate security alerts, advisories and directives to appropriate personnel; and
d. implement security directives in accordance with established time frames.

6. Miscellaneous

This policy shall supersede all previous Metropolitan Government technical vulnerability management policies. This policy may be amended or revised at any time. Users are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions.

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.

_____ _____

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

REFERENCES

- ISO 27002: sections 12.6.1, 13.1.2, 15.2.2
- NIST Special Publication 800-40, *Creating a Patch and Vulnerability Management Program*
- NIST Special Publication 800-51, *Guide to Using Vulnerability Naming Schemes*
- NIST Special Publication 800-53 rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations:* Control numbers – CA-2, CA-7, RA-5, SC-34, SI-4, SI-7
- NIST Special Publication 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP)*
- Metropolitan Government *Risk Assessment and Treatment Policy*
- Center for Internet Security Critical Security Benchmark #4

REVISION HISTORY

REVISION	DATE	CHANGES
0.1	09/09/2016	Draft
1.0	12/15/2016	Approved Version