| **CITY OF SHELBYVILLE** | POLICY |
| --- | --- |
| **INFORMATION TECHNOLOGY DEPARTMENT** | NUMBER: ITD 5 |
| SUBJECT: | DISTRIBUTION DATE: 8/12/2024 |
| **PATCH AND VULNERABILITY MANAGEMENT** | EFFECTIVE DATE: 8/12/2024 |
| ISSUING AUTHORITY: City Council | EXPIRATION: UNTIL RESCINDED |

**PURPOSE**

The purpose of this policy is to ensure Shelbyville City Government (City) reduces risks resulting from exploitation of published technical vulnerabilities, outdated software, and end of life software.

**POLICY**

1. The City of Shelbyville Government Shall:
    1.1. ensure all applications are fully supported by the manufacturer;
    1.2. maintain all support and maintenance agreements for the lifetime of the application;
    1.3. include language in contracts requiring timely updates of applications;
    1.4. obtain timely information about technical vulnerabilities of information systems and applications being used;
    1.5. evaluate its exposure to such vulnerabilities;
    1.6. take appropriate , timely measures to address the associated risk, including patching vulnerabilities.

    As set forth below, the City management of technical vulnerabilities is supported through the use of the controls set forth in:
    - Risk assessment (see Section 2.0 below);
    - vulnerability scanning (see Section 3.0 below);
    - patch management (see Section 4.0 below);
    - and security alerts, advisories and directives (see Section 5.0 below).

2. Vulnerability Risk Assessment
    The City 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.

    i. 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.

    ii. Patching of security vulnerabilities should preferably occur within two weeks of patch release.

    iii. Patching addressing vulnerabilities that are being actively exploited should be tested and deployed within forty-eight hours.

    iv. 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

The City 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:

    i. enumerating platforms, software flaws and improper configurations;

    ii. measuring vulnerability impact using a defined method; and

    iii. reporting and providing clearly documented and defined results;

    iv. looks for code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries); and

    v. 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. employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned;

f. update the list of information system vulnerabilities scanned or when new vulnerabilities are identified and reported;

g. include privileged access authorization for selected vulnerability scanning activities to facilitate more scanning;

h. employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities; and

i. employ an independent penetration agent or penetration team to conduct a vulnerability analysis on the information system annually.

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

4. Patch Management and Flaw Remediation

The City 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 City 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

The City 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 City 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.

**DEFINITIONS**

Terms used in this policy are defined in the Shelbyville Information Security Glossary

**CONTACT**

Questions should be directed to email at kade.stier@shelbyvilletn.org, or by mailing them to Director, Information Technology Department, 201 N Spring St, Shelbyville, TN 37160.

**REFERENCES**

- ISO 270 02: sections 12.6.1, 13. 1.2, 15.2.2
- NIST Special Publication 80 0 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)
- Center for Internet Security Critical Security Benchmark #4

**REVISION HISTORY**

| REVISION | APPROVAL DATE | CHANGES |
|----------|---------------|---------|
| 1.0 | 8/9/2024 | First released version |