REQUIREMENT #5: USE & REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

Malicious software, commonly referred to as "malware" (including viruses, worms, rootkits, and Trojans) enters network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices. This can result in the exploitation of system vulnerabilities, so anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS CONTROL 5.1

Control Objective: The organization deploys anti-malware software on systems commonly affected by malicious software.

Standard: Asset custodians are required to:

(a) Deploy the City of Waukesha-approved anti-malware software on all systems capable of running anti-malware software, including, but not limited to: [64]
    1. Workstations;
    2. Servers;
    3. Tablets;
    4. Mobile phones;

(b) Ensure that the City of Waukesha-approved anti-malware software is capable of detecting, removing, and protecting against all known types of malware; [65] and

(c) Perform periodic evaluations to identify and evaluate evolving malware threats on information systems considered to be not commonly affected by malware, in order to confirm whether such information systems continue to not require anti-malware software. [66]

Supplemental Guidance: Systems not capable of running anti-malware software should have a documented business justification as to why anti-malware software cannot be run and what compensating controls are in place to minimize the risk associated with the lack of anti-malware software on that system.

Typically, mainframes, mid-range computers (such as AS/400) and similar systems may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems. For example, by monitoring vendor security notices and anti-malware newsgroups to determine whether their systems might be coming under threat from new and evolving malware.

Trends in malware should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into City of Waukesha's configuration standards and protection mechanisms as needed

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 5.2

Control Objective: The organization ensures that anti-malware mechanisms are current, actively running, and generating audit logs.

Standard: Asset custodians are required to ensure the City of Waukesha-approved anti-malware software is: [67]

(a) Kept current with updates from the anti-malware vendor;
(b) Actively running on systems the anti-malware software is deployed to; and
(c) Generating audit logs per PCI DSS requirement 10.7.

Supplemental Guidance: Even the best anti-malware solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

[64] PCI DSS v3.2 Requirement 5.1
[65] PCI DSS v3.2 Requirement 5.1.1
[66] PCI DSS v3.2 Requirement 5.1.2
[67] PCI DSS v3.2 Requirement 5.2

Procedures: Anti-malware test files from the European Institute for Computer Antivirus Research (EICAR) should be downloaded (http://www.eicar.org/85-0-Download.html) and copied to either a CD/DVD or write-protected USB.

- This CD/DVD or USB should be inserted into systems to test that anti-malware software is running "on demand" scans and detects the presence of the EICAR test file; and
- Logs should be checked to verify the EICAR test file was detected and logged.

PCI DSS CONTROL 5.3

Control Objective: The organization ensures that anti-malware mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

Standard: Asset custodians are required to ensure the City of Waukesha-approved anti-malware software is actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.[68]

Supplemental Guidance: Anti-malware that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software. Additional security measures may also need to be implemented for the period of time during which anti-malware protection is not active (e.g., disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after it is re-enabled).

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 5.4

Control Objective: The organization ensures that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.[69]

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for protecting systems against malware are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

[68] PCI DSS v3.2 Requirement 5.3
[69] PCI DSS v3.2 Requirement 5.4

REQUIREMENT #6: DEVELOP & MAINTAIN SECURE SYSTEMS & APPLICATIONS

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Since many of these vulnerabilities are fixed by vendor-provided security patches, all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

PCI DSS CONTROL 6.1

Control Objective: The organization implements a process to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.

Standard: Asset custodians and data owners are required to rank vulnerabilities according to the National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system. [70]

Supplemental Guidance: The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores.[71]

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 6.2

Control Objective: The organization ensures that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

Standard: Asset custodians and data owners are required to ensure that: [72]

(a) All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;
(b) Critical security patches are installed within thirty (30) days of the vendor's release data; and
(c) Non-critical security patches are installed within ninety (90) days of the vendor's release data.

Supplemental Guidance: City of Waukesha is allowed to apply a risk-based approach to prioritize its patch installations. For example, by prioritizing critical infrastructure (e.g., public-facing devices and systems, databases) higher than less-critical internal devices, this helps ensure high-priority systems and devices are addressed within one month and still allows for addressing less critical devices and systems within three months.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 6.3

Control Objective: The organization develops all internal and external software applications in accordance with PCI DSS and based on industry-recognized leading practices.

Standard: Contract owners, asset custodians, and data owners are required to ensure that internal and external developers:

(a) Develop software applications in accordance with PCI DSS and based on industry-recognized leading practices; [73]
(b) Incorporate cybersecurity throughout the software development lifecycle; [74]
(c) Remove custom application accounts, user IDs, and passwords before applications become active or are released to customers; [75] and
(d) Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated process) to include at least the following: [76]

---

[70] PCI DSS v3.2 Requirement 6.1
[71] National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm
[72] PCI DSS v3.2 Requirement 6.2
[73] PCI DSS v3.2 Requirement 6.3
[74] PCI DSS v3.2 Requirement 6.3
[75] PCI DSS v3.2 Requirement 6.3.1
[76] PCI DSS v3.2 Requirement 6.3.2

1. Code changes must be reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices;
2. Code reviews must ensure code is developed according to secure coding guidelines;
3. Appropriate corrections must be implemented prior to release; and
4. Code-review results must be reviewed and approved by management prior to release.

Supplemental Guidance: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.[77]

Procedures:

PCI DSS CONTROL 6.4

Control Objective: The organization follows change control processes and procedures for all changes to system components.

Standard: Asset custodians and data owners are required to follow change control processes and procedures for all changes to system components. The change control processes for assets within scope for PCI DSS include the following: [78]

(a) Utilize separate environments for development/testing/staging and production; [79]
(b) Utilize a separation of duties between development/testing/staging and production environments; [80]
(c) Prohibit the use of production data (e.g., live PANs) for testing or development; [81]
(d) Remove test data and accounts before production systems become active / goes into production; [82] and
(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following: [83]
    1. Documentation of impact; [84]
    2. Documented change approval by authorized parties;[85]
    3. Functionality testing to verify that the change does not adversely impact the security of the system; [86] and
    4. Back-out procedures; [87] and
(f) Upon completion of significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. [88]

Supplemental Guidance: Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.

Procedures: See ITCM-1.0 CHANGE MANAGEMENT POLICY for more details.

PCI DSS CONTROL 6.5

Control Objective: The organization develops applications based on secure coding guidelines.

Standard: Contract owners, asset custodians, and data owners are required to address common coding vulnerabilities in the software development process by ensuring the following:

(a) At least annually, developers are properly trained in current, secure coding techniques, including: [89]
    1. How to avoid common coding vulnerabilities, and
    2. Understanding how sensitive data is handled in memory
(b) Applications are developed based on secure coding guidelines: [90]

[77] Open Web Application Security Project (OWASP) Guide https://www.owasp.org
[78] PCI DSS v3.2 Requirement 6.4
[79] PCI DSS v3.2 Requirement 6.4.1
[80] PCI DSS v3.2 Requirement 6.4.2
[81] PCI DSS v3.2 Requirement 6.4.3
[82] PCI DSS v3.2 Requirement 6.4.4
[83] PCI DSS v3.2 Requirement 6.4.5
[84] PCI DSS v3.2 Requirement 6.4.5.1
[85] PCI DSS v3.2 Requirement 6.4.5.2
[86] PCI DSS v3.2 Requirement 6.4.5.3
[87] PCI DSS v3.2 Requirement 6.4.5.4
[88] PCI DSS v3.2 Requirement 6.4.6
[89] PCI DSS v3.2 Requirement 6.5
[90] PCI DSS v3.2 Requirement 6.5

1. Injection flaws, particularly SQL injection: [91]
    i. OS Command Injection;
    ii. LDAP and XPath injection flaws, and
    iii. Other forms of injection flaws;
2. Buffer overflow; [92]
3. Insecure cryptographic storage; [93]
4. Insecure communications; [94]
5. Improper error handling; [95]
6. All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS requirement 6.1; [96]
7. Cross-site scripting (XSS); [97]
8. Improper access control, including but not limited to: [98]
    i. Insecure direct object references,
    ii. Failure to restrict URL access; and
    iii. Directory traversal;
9. Cross-site request forgery (CSRF); [99] and
10. Broken authentication and session management. [100]

Supplemental Guidance: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.[101]

Procedures: The City does not develop in-house applications that deal with cardholder data. The City staff that do application development do annual training that meets these requirements. ~~[insert a description of the actual procedures that you follow to meet this requirement]~~

PCI DSS CONTROL 6.6

Control Objective: The organization address new threats and vulnerabilities on an ongoing basis and ensure public-facing web applications are protected against known attacks.

Standard: Asset custodians and data owners are required to address public-facing web application threats and vulnerabilities by either of the following methods: [102]

(a) Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods:
    a. At least annually; and
    b. After any changes to the public facing website
(b) Installing an automated technical solution that detects and prevents web-based attacks (e.g., a web-application firewall) in front of public-facing web applications, to continually check all traffic.

Supplemental Guidance: Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices.

- Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities

[91] PCI DSS v3.2 Requirement 6.5.1
[92] PCI DSS v3.2 Requirement 6.5.2
[93] PCI DSS v3.2 Requirement 6.5.3
[94] PCI DSS v3.2 Requirement 6.5.4
[95] PCI DSS v3.2 Requirement 6.5.5
[96] PCI DSS v3.2 Requirement 6.5.6
[97] PCI DSS v3.2 Requirement 6.5.7
[98] PCI DSS v3.2 Requirement 6.5.8
[99] PCI DSS v3.2 Requirement 6.5.9
[100] PCI DSS v3.2 Requirement 6.5.10
[101] Open Web Application Security Project (OWASP) Guide https://www.owasp.org
[102] PCI DSS v3.2 Requirement 6.6

- Web-application firewalls filter and block nonessential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured.

An organization that specializes in "application security" can be either a third-party company or an internal team/department, as long as the reviewers specialize in application security and can demonstrate independence from the development team.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 6.7

Control Objective: The organization ensures that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for developing and maintaining secure systems and applications are kept current and disseminated to all pertinent parties. [103]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.

Procedures: The City does not develop in-house applications that deal with cardholder data. The City staff that do application development do annual training that meets these requirements.

[103] PCI DSS v3.2 Requirement 6.7