

**Document Code No.:** ITG-P-21-12

**Title:** King County Vulnerability Management Policy

**Affected Agencies:** Countywide


**Authorities:** King County Code Title 2A.380

**Keywords:** Vulnerability Management Policy, Vulnerabilities

**Sponsoring Agency:** Department of Information Technology (KCIT)

**Chief Information Officer Signature:**

**Date signed and effective:** 2/16/2021

DocuSigned by:  
  
920AF9FCB611460...



## I. Purpose:

The purpose of this policy is to detect and remediate the risk of vulnerabilities introduced through the manufacturing process, implementation, or configuration of technology assets (e.g., hardware, software, data, and authentication information) used by King County. This policy reflects King County's pro equity and social justice commitment. Implementation of this information security policy aligns and complies, in every regard, with King County's equity and social justice policies and practices.

## II. Applicability and Audience

### A. Users

This policy applies to all King County workforce members responsible for technology asset ownership and support.

### B. Technology Assets

1. This policy applies to all King County owned and operated technology assets.
2. This policy applies to all commercially owned and operated (e.g., cloud service providers, vendors, partners) technology assets used in support of King County service delivery or that reside within King County owned and operated environments. Vulnerability detection and remediation processes may be different than with King County owned and operated assets in that King County and/or the owner/operator of the technology asset may play a role in detection and/or remediation processes.
3. Personal technology assets are not in scope of this policy except when security tools detect a vulnerable system. King County utilizes security tools to detect vulnerabilities in various ways such as when a personal device attempts to make a virtual private network (VPN) connection or when a mobile device attempts to connect to King County email. Security tools may deny a personal device if vulnerabilities are detected that represent a violation of security policy such as the use of an end of life operating system or a mobile phone that is not configured to require a PIN/password to unlock.

### C. Exceptions

Requests for exceptions to this policy must follow the Department of Information Technology (KCIT) information security policy exceptions handling process. Please open a ticket with the helpdesk to request a policy exception.

### III. Definitions

*All definitions are contained within the King County Information Security Policy and Standards Glossary.*

### IV. Policy

All technology assets must be protected through the deployment and installation of security patches and updates provided by the manufacturer for the purposes of remediating a security risk. If security patches or updates cannot be installed, then alternative solutions to mitigate the security risk must be identified and implemented.

Vulnerability assessments, penetration tests, and other monitoring and auditing will be periodically performed by the Chief Information Security and Privacy Officer to verify that vulnerabilities are mitigated in a timely manner.

There are five (5) primary processes that must be followed to appropriately manage vulnerabilities:

1. Identification
2. Risk Assessment
3. Prioritization and Mitigation plan
4. Patch Management and Deployment
5. Validation

#### A. Identification

Vulnerabilities can be identified several ways including vulnerability publication sources, such as the United States Computer Emergency Readiness Team (US-CERT) and the National Vulnerability Database (NVD), vulnerability scans, risk assessments and penetration tests. Manufacturers are also increasing visibility into the status of vulnerabilities within their products including information on the necessary actions to resolve or remediate the vulnerability.

The Chief Information Security and Privacy Officer will establish procedures for monitoring vulnerability publication sources and warnings from manufacturers, regulators, and industry sources to provide timely information to technology asset owners and technology support owners regarding newly identified vulnerabilities, including a ranking based on criticality.

For vulnerabilities rated “Emergency”, “Critical” or “High” by the relevant rating systems of the publisher or manufacturer, the Chief Information Security and Privacy Officer will ensure procedures are established and utilized by technology asset and support owners to assess the impact to King County technology assets.

## **B. Risk Assessment**

A risk assessment is not required for each vulnerability but can be used to reduce the priority of a vulnerability if mitigating factors are present. If a risk assessment is not performed, the vulnerability must be addressed according to the highest known vulnerability risk rating. A request for a risk assessment can be made to the Department of Information Technology (KCIT) by opening a service request at the helpdesk.

The Chief Information Security and Privacy Officer must approve any mitigating factors used to justify the reduction of the priority or rating of a vulnerability.

## **C. Prioritization and Mitigation Plan**

1. Not all discovered vulnerabilities require the same prioritization or mitigation approach. King County will prioritize emergency, critical, and high vulnerabilities as established by the manufacturer or industry standard scoring. Criticality ratings (e.g., manufacturer recommendations, vulnerability management platforms, CVSS or Common Vulnerability Scoring System or other industry standards) must be used to prioritize remediation activities. Business impact, information classification, and/or the presence or absence of mitigating factors identified during a risk assessment may be used to modify the priority or rating of a vulnerability.
2. Workforce members responsible for technology asset ownership and support will ensure that vulnerability remediation activities are appropriately resourced and prioritized (e.g., Department or Agency leadership, Chief Technology Officer, IT Director of agency with separately elected officials, technology asset owners, technology support owners).
3. Vulnerabilities can be mitigated through a variety of methods, including but not limited to:
  - a. Installing a patch or modifying a configuration
  - b. Turning off a service or capability related to the vulnerability if not needed
  - c. Modifying or adding security controls (i.e. firewalls, IDS/IPS, etc.)
  - d. Increased logging and monitoring to detect actual attacks and respond quickly
  - e. Alternative mitigations in addition to those listed above may be approved by the Chief Information Security and Privacy Officer.
4. Vulnerabilities must be patched or resolved by the technology support owner within the time windows specified in this policy. The time window begins when awareness of the vulnerability occurs. In some cases the manufacturer may notify that a vulnerability exists but does not yet have a resolution. Technology support owners must notify the Chief Information Security and Privacy Officer by opening a ticket

with the helpdesk when this occurs for vulnerabilities rated emergency, critical, or high.

<b>Patch Criticality Rating</b>	<b>Internet-Facing System Time Window</b>	<b>Internal Systems Time Window</b>
Emergency Rated	48 hours	5 days
Critical Rated	5 days	30 days
High Rated	30 days	60 days
Medium Rated	90 days	180 days
Low Rated	As Needed	As Needed
Informational Rated	As Needed	As Needed

#### **D. Patch Management and Deployment**

1. The Department of Information Technology (KCIT) will procure and manage centralized enterprise systems that enable patching and configuration management for King County technology assets by authorized technology support personnel. Deployment of patches must follow the Department of Information Technology (KCIT) change management process.
2. All hardware and software technology assets must be regularly reviewed for missing security updates and patches provided by the manufacturer.
3. Security updates and patches must be installed unless doing so would knowingly create an adverse impact to a King County technology asset or has already caused an adverse impact and has been removed. Deployment or implementation can be delayed until the root cause of the adverse impact has been identified and addressed by the manufacturer or developer. Such delayed deployment must be documented and submitted to the Chief Information Security and Privacy Officer including cause of delay and estimated deployment date if delay will be longer than 90 days.

#### **E. Validation**

1. Validation must be completed as part of the patching or vulnerability remediation procedure to ensure the patches have been applied properly and the vulnerability has been remediated.
2. The Chief Information Security and Privacy Officer may perform penetration tests at any time on King County technology assets and business processes in order to find vulnerabilities before malicious actors do. The penetration tests may include network

and application-level testing, both from external (untrusted) and internal (trusted) sources, and against external facing or internal only systems. Security controls, limitations, network connections, and restrictions will be routinely tested to make sure any unauthorized access attempts can be identified or stopped and to meet regulatory requirements.

3. The Chief Information Security and Privacy Officer will conduct vulnerability assessments including automated and authenticated scans. Assessments will be reported to asset owners and technology support personnel responsible for vulnerability remediation. All internal and external systems and networking devices will be routinely scanned for:
  - a. Patch levels
  - b. Functions, ports, protocols, and services accessible to users or devices
  - c. Improperly configured or incorrectly operating information flow control mechanisms
  - d. Known vulnerabilities

## **V. Implementation Plan**

This policy becomes effective for countywide use on the date that it is signed by Chief Information Officer. All new technology implementations and new material changes to existing technology implementations must ensure compliance with this policy as of the effective date. All other technology implementations must be brought into compliance within four years after the effective date.

## **VI. Maintenance**

- A.** This policy will be maintained by the Department of Information Technology (KCIT), Office of the CIO, or its successor agency. This includes, but may not be limited to:
  1. Interpretation of this policy
  2. Ensuring this policy content is kept current
  3. Recommending updates to this policy and related resources
  4. Developing an escalation and mitigation process if an Organization is not in compliance
  5. Assisting Organizations to understand how to comply with this policy
  6. Monitoring annual compliance by Organizations
- B.** This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by the Office of the CIO, or its successor agency prior to the expiration date.

## **VII. Consequences for Noncompliance**

Violations of this policy may be grounds for disciplinary action, up to and including termination and enforcement action which may include civil or criminal charges.

**VIII. Appendix A: References**

- Asset Management Policy
- Vulnerability Management Standard
- Department of Information Technology (KCIT) Change Management Process
- Information Security Policy and Standards Glossary

**IX. Appendix B: Relevant Compliance Requirements**

This section provides references to key regulations and standards that apply to King County. This section does not replace the authoritative source and is just a reference to assist with further research. Please use the Compliance Standard and Section No. to further research the entirety of the regulation, framework or standard from the authoritative source.

<b>Compliance Standard</b>	<b>Section No.</b>	<b>Description</b>
<b>HIPAA</b>	45 CFR 164 Subpart C	Security Standards for the Protection of Electronic Protected Health Information
	164.308(a)(1)(ii) (A)	Risk Analysis
	164.308(a)(1)(ii) (B)	Risk Management
<b>CJIS Policy v5.9</b>	5.1.2	Monitoring, Review, and Delivery of Services
	5.10.4.1	Patch Management
<b>PCI DSS v3.2.1</b>	5	Maintain a Vulnerability Management Program
	6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
	6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
	6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding

		<p>vulnerability (using either manual or automated processes) to include at least the following:</p> <ul style="list-style-type: none"> <li>- Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.</li> <li>- Code reviews ensure code is developed according to secure coding guidelines</li> <li>- Appropriate corrections are implemented prior to release.</li> <li>- Code-review results are reviewed and approved by management prior to release.</li> </ul>
	6.6	<p>For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:</p> <ul style="list-style-type: none"> <li>- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.</li> <li>- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.</li> </ul>
	11.2	<p>Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).</p>
	11.2.1	<p>Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.</p>

11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
11.3	<p>Implement a methodology for penetration testing that includes the following:</p> <ul style="list-style-type: none"> <li>- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115).</li> <li>- Includes coverage for the entire CDE perimeter and critical systems.</li> <li>- Includes testing from both inside and outside the network.</li> <li>- Includes testing to validate any segmentation and scope-reduction controls.</li> <li>- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.</li> <li>- Defines network-layer penetration tests to include components that support network functions as well as operating systems.</li> <li>- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.</li> <li>- Specifies retention of penetration testing results and remediation activities results.</li> </ul>
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).



	11,3,2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
	11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.
	11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.
<b>NIST CSF</b>	ID.RA	Risk Assessment
	PR.IP	Information Protection Processes and Procedures
	DE.CM	Security Continuous Monitoring
	RS.AN	Analysis
	RS.MI	Mitigation
<b>NIST 800-53r5</b>	RA-5	Vulnerability Monitoring and Scanning
	SA-11	Developer Testing and Evaluation
	CA-2	Control Assessments
	SI-2	Flaw Remediation
<b>CIS Controls v7.1</b>	3	Continuous Vulnerability Management
	20	Penetration Tests and Red Team Exercises