

**Document Code No.:** ITG-P-21-03

**Title:** King County Application Security Policy

**Affected Agencies:** Countywide


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

**Keywords:** Application Security, AppSec, Software, Apps

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

**Chief Information Officer Signature:**

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

DocuSigned by:  
  
920AF9FCB611460...



**King County**

## I. Purpose:

The purpose of this policy is to ensure that software applications, purchased or developed by King County workforce members, are implemented through a consistent process that includes a review of required security controls. 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 workforce members responsible for technology asset ownership and support as well as workforce members responsible for purchasing or developing King County software applications.

### B. Technology Assets

This policy applies to all software applications purchased or developed by King County. "Software" and "application" are the same for purposes of this policy.

### 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 software applications purchased or developed by King County must be evaluated for security and privacy requirements during the procurement and development phases. The application developer(s) or procurement lead(s) (e.g., project manager, contracts lead, technical lead, etc.) shall assess and document security and privacy requirements in accordance with the Department of Information Technology (KCIT) policies and standards. Additionally, any material change to an existing software application requires a review and update to the initial security and privacy assessment to ensure requirements have not changed. Security and privacy controls must be an essential part of project planning, development, and implementation.

**A. Commercial Software Applications**

1. Vendors being considered through a procurement process must provide information about security and privacy programs during the procurement process. In addition to the requirements in this section vendors may be required to agree to additional information security and privacy requirements of King County as determined by an information security risk or privacy impact assessment.
2. Software applications being considered through a procurement process must determine whether a risk assessment is required by consulting with the Chief Information Security and Privacy Officer. Risk assessments can be requested by opening a ticket with the helpdesk.
3. Software applications procured on behalf of King County must:
  - a. Utilize an industry recognized secure development lifecycle process with third party validation of security program, controls, and vulnerability management practices
  - b. Utilize techniques to prevent command injection attacks
  - c. Utilize techniques to prevent misuse of special characters
  - d. Utilize techniques to validate all user input
  - e. Utilize King County's identity and access management platforms
  - f. Utilize techniques to validate authorization and access based on role and user
  - g. Utilize industry standard cryptographic techniques to protect data
  - h. Utilize industry standard cryptographic techniques to manage secrets and keys which may not be stored in plain text directly in software application code
  - i. Utilize intrusion and anomaly detection techniques
  - j. Utilize audit logging techniques using industry standard logging formats that provide the minimum amount of information needed for corrective action while not revealing sensitive information that could be exploited by a malicious party
  - k. Utilize industry standards or trusted third party frameworks, libraries, and components wherever possible
  - l. Comply with the Vulnerability Management Policy
  - m. Be located within geographic boundaries governed by United States law
  - n. Not be used for production purposes past 180 days of the end of support by the manufacturer
  - o. Have security advisories and patches with installation instructions made available to the general public by the manufacturer

**B. Software Applications Developed by King County**

1. Software applications being developed by King County must:
  - a. Be approved for development by the Department of Information Technology (KCIT) Chief Information or Chief Technology Officer to ensure custom application development is the most appropriate and sustainable technology solution
  - b. Include an information security risk and/or a privacy impact assessment if required. Assessments can be requested by opening a ticket with the helpdesk.
  - c. Comply with section IV(A)(3) requirements (a) through (m) of this policy referencing software applications procured by King County. Third party validation for internally developed software applications means King County workforce members who are not the developer or development team.
  - d. Comply with the Secure Coding Standard including the required use of approved and protected source code repositories
  - e. Comply with King County Architecture Review Team (ART) approved software development standards
  - f. Comply with the Vulnerability Management Policy
  - g. Be developed by workforce members who have completed secure coding training as defined in the Secure Coding Standard

**C. Environment Separation Requirements**

Separate environments must be utilized to protect the confidentiality, integrity, and availability of King County technology assets. Developers or those implementing technology on behalf of King County must:

1. Separate production environments from non-production environments (e.g., test, dev, pre-production) in compliance with the Data Security and Network Security Policies
2. Implement separation of duties such that the developer of an application cannot modify production environments without a code review and approval process by another party

**D. Application Firewalls and Proxies**

Software applications procured or developed by King County must utilize intrusion detection and prevention techniques (e.g., web application firewall) prior to allowing access to the application or application service if:

1. Exposed or made available to the public internet
2. Contains or interacts with category 3 or 4 data classified in accordance with the Information Classification Policy.

3. Required by a vulnerability, information security risk, or privacy impact assessment
4. Shares components (e.g., the same server or database) with category 3 and 4 software applications

#### **E. Change Management Requirements**

Material changes to King County technology assets (e.g., new module installation, patching, major version upgrades, major reconfiguration) must follow the Department of Information Technology (KCIT) change management process. Please contact the Chief Technology Officer in the Department of Information Technology (KCIT) regarding questions about change management.

#### **F. Emergency Changes**

Emergency changes must follow the Department of Information Technology (KCIT) Change Management Process where possible. Temporary changes are authorized to be made as part of the Department of Information Technology (KCIT) Major Incident Management process to reduce the impact of a security incident. These changes must be reviewed within 72 hours to determine whether these changes comply with policies and standards. If the emergency change does not comply then the Chief Technology Officer and Chief Information Security and Privacy Officer must be notified.

#### **G. Patch Management**

King County software applications must:

1. Have the security patch management information provided by the manufacturer recorded in the system of record as part of the Asset Management Policy and associated standards to ensure that the technology asset and support owner can determine how to design the patch management process for software applications.
2. Be procured or developed with the appropriate licensing required to enable access to security patches provided the manufacturer.
3. Be developed or implemented with security patch management in place prior to production use of the software application in accordance with manufacturer guidelines. Security patch management is not optional.
4. Comply with the Vulnerability Management Policy

#### **H. Documentation**

Software applications must be properly documented in authorized systems of record in compliance with the Asset Management Policy and associated Standards to ensure that the availability of a subject matter expert does not impact King County's ability to maintain and support operations and workflows that rely on software applications.

**I. Personally Identifiable Information (PII)**

1. Applications that will collect, store, process, or transmit personally identifiable information must include functionality that allows for documentation of records retention requirements and automatic removal of such information.
2. The application must indicate in the asset management system of record that PII is utilized.

**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**

- Department of Information Technology (KCIT) Change Management Process
- Department of Information Technology (KCIT) Major Incident Management Process
- ART Secure Coding Standards
- Vulnerability Management Policy
- Asset Management Policy
- 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
<b>CJIS Security Policy v5.9</b>	5.10.4.1	Patch Management
	Appendix G.8	Secure Coding
<b>PCI DSS v3.2.1</b>	6	Develop and maintain secure systems and applications
<b>NIST CSF</b>	PR.IP	Information Protection Processes and Procedures
<b>NIST 800-53r5</b>	CM	Configuration Management
	SA	System and Services Acquisition
<b>CIS Controls v7.1</b>	18	Application Software Security