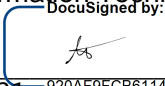


**Document Code No.:** ITG-P-21-13  
**Title:** King County Device Security Policy  
**Affected Agencies:** Countywide  
**Authorities:** King County Code Title 2A.380  
**Keywords:** Device Security, Configuration, Hardening  
**Sponsoring Agency:** Department of Information Technology (KCIT)



**Chief Information Officer Signature:**   
**Date signed and effective:** 3/1/2021 DocuSigned by: 920AF9FCB611460...

**I. Purpose:**

The purpose of this policy is to ensure hardware technology assets and devices are configured in a secure and hardened manner. 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 persons working for, or on behalf of King County, including workforce members, third parties, volunteers and contractors who access King County technology assets. These requirements apply whether the user is working within a King County facility or working remotely.

**B. Technology Assets**

This policy applies to all King County hardware technology assets. This policy also applies to the use of third party or personal devices, if used to access King County’s technology assets in the process of working for or on behalf of King County.

**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**

**A. King County Owned Devices**

1. The Department of Information Technology (KCIT) is responsible for providing centralized enterprise platforms for device configuration management and device security.
2. The Department of Information Technology (KCIT) will ensure that technology asset and support owners are provided appropriate rights to manage devices in centralized

platforms for which they are authorized to manage in accordance with the Access Management Policy.

3. King County owned devices are required to comply with the Device Security Policy and associated Device Configuration standards as approved by the Architecture Review Team (ART) within the Department of Information Technology (KCIT).
4. All King County owned devices that support configuration management automation must utilize centralized enterprise security and configuration management platforms provided by the Department of Information Technology (KCIT). This includes but is not limited to:
  - a. Asset Management and Provisioning Systems
  - b. Configuration and Patch Management Systems
  - c. Identity and Access Management Systems
  - d. Remote Access and Remote Administration Systems
  - e. Endpoint Detection and Response, Anti-Virus, Anti-Malware Systems
  - f. Full Disk/Device Encryption
  - g. Mobile Device Management Systems
  - h. Network Device Management Systems
  - i. IoT Device Management Systems
  - j. Vulnerability Detection Systems
  - k. Inactive/Anomalous Session Termination or System Lock Configurations
  - l. Firmware and Hardware Security Controls
  - m. Device Certificate and Cryptographic Controls and Configurations
5. King County owned technology assets to remain within a geographic area governed by United States law.
6. Care should be taken to prevent unauthorized access to King County technology assets. If a user suspects that unauthorized access to their device has occurred and may have involved King County technology assets (e.g., someone accessed King County data), they must report the incident immediately to the Department of Information Technology (KCIT) by opening a ticket with the helpdesk.
7. Care should be taken to prevent lost or stolen devices. All lost or stolen devices must be reported to the Department of Information Technology (KCIT) immediately by opening a ticket with the helpdesk.

## **B. Personal Devices**

Personal devices (i.e. owned by workforce members, contractors, or vendors) may be used to access King County technology assets but are subject to the following requirements:

1. Personal devices will only be allowed to connect to applications and data authorized by the Department of Information Technology (KCIT) for use on a personal device. Personal devices are prohibited from being directly connected to King County's wired or wireless private internal network infrastructure (i.e., personal devices should not be brought into a King County facility and plugged into King County's private network).
2. King County may use technology that detects security flaws and other information prior to allowing personal device connections and may automatically deny these connections if security flaws or vulnerabilities are detected. These may include end of life operating systems or browsers, out of date or disabled anti-virus/anti-malware protections and signatures, insufficient encryption, passwords/PIN not in use, detection of malicious software, etc.
3. Care should be taken to prevent lost or stolen devices and/or unauthorized access to King County technology assets. If a workforce member suspects that unauthorized access to their device has occurred and may have involved King County technology assets (e.g., someone accessed King County data), or if their personal device is lost or stolen and King County applications or data are present they must report the incident immediately to the Department of Information Technology (KCIT) by opening a ticket with the helpdesk.
4. Workforce members are responsible for keeping their personal devices patched and up to date.
5. Workforce members should not bypass security warnings when connecting their devices to insecure or unknown wireless networks.
6. Workforce members must exercise caution when using a personal device to conduct public business. RCW 42.56 and other statutes relating to legal discovery may require a workforce member to search their personal device for public records that are responsive to a public records request or litigation discovery request.
7. Workforce members, as part of working for or on behalf of King County, may be asked to search for and produce content on their personal device solely for King County purposes (i.e., not on behalf of a third party) such as King County's compliance with other laws. King County will not confiscate nor request a search of an employee's personal device for any purpose except as explicitly permitted by law. King County workforce members are responsible for and have rights regarding their personal devices and property. King County workforce members in managerial or supervisory positions are required to request legal advice prior to requesting workforce members to search for and produce content from a personal device when the request is related to employee conduct or performance.

8. The Department of Information Technology (KCIT) may deny connections by the device, initiate a remote wipe of King County data, or take action on the King County provided user account to prevent unauthorized access to King County technology assets if a suspected or confirmed security incident is in progress.
9. Workforce members shall not share access to King County applications or data with an unauthorized individual such as other King County workforce members (if not authorized), friends or family members.

### **C. Contractors and Vendors**

1. Vendors may not use their corporate owned or personal devices to directly connect to King County's technology assets (e.g., private wired or wireless internal network) other than those intended for public use.
2. A Vendor may be issued a King County device such as a laptop and/or a King County user account to perform contracted services as part of a project. King County technology assets issued to Vendors must be configured to limit access to only those King County technology assets for which the Vendor is authorized to access. Devices and accounts shall not be issued for more than 90 days and should be done so only as a last resort. The Vendor must receive and acknowledge King County's Acceptable Use Policy.
3. Volunteers, time or term limited temporary workforce members, contracted labor, or other types of temporary labor unrelated to the sale or implementation of professional and commercial products and services may be issued a King County device such as a laptop and/or a King County user account and are subject to the same information security policy requirements as a full time workforce member of King County.

### **D. Device Configuration Standards**

The Architecture Review Team (ART) is required to develop and maintain countywide standards for device configurations utilizing manufacturer provided hardening guides and/or industry best practices for securing device configurations.

### **E. Device Security Compromise**

The Department of Information Technology (KCIT) may take action on a device (e.g., disabling it, prevent network connections, isolating the device, wiping King County data, etc.) if a security incident is suspected or in progress. Security incidents include but are not limited to:

1. A device has malicious software installed (e.g., rootkit or jailbroken)
2. A device contains an app known to contain a security vulnerability (if not removed within a given timeframe after informing the user)
3. A device is reported lost or stolen
4. The maximum number of failed password attempts has been reached

5. A user has reported a security incident
6. King County security technology has detected an active security incident in progress

#### **F. Help and Support**

1. The Department of Information Technology (KCIT) will support King County-owned hardware and software. Support can be requested by opening a ticket with the helpdesk.
2. The Department of Information Technology (KCIT) will not support personally owned devices beyond the delivery of standardized instructions for how to utilize King County provided applications or while working through a security incident involving King County technology assets.
3. The Department of Information Technology (KCIT) will not support devices owned by contractors or vendors.

#### **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**

- Acceptable Use Policy
- Chapter 42.56 RCW
- 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
	164.310(c)	Workstation Security
	164.310(d)(1)	Device and Media Controls
<b>PCI DSS v3.2.1</b>	5	Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs
<b>CJIS Policy v5.9</b>	5.7	Configuration Management
	5.13	Mobile Devices
	5.10.4	System and Information Integrity Policy and Procedures
<b>NIST CSF</b>	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
<b>NIST 800-53r5</b>	CM	Configuration Management
	MA	Maintenance
	SI	System and Information Integrity
<b>CIS Controls v7.1</b>	5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
	11	Secure Configuration for Network Devices such as Firewalls, Routers and Switches