

Document Code No.: ITG-P-22-1
Title: Mobile Cellular Policy
Affected Agencies: All Agencies
Authorities: KCC 2A.380.200
Keywords: Cellular, Mobile, Phone, Provider, Tablet
Sponsoring Agency: Department of Information Technology



King County

Chief Information Officer signature: David Mendel
Date signed and effective: 11/30/2022

I. Purpose:

This policy establishes standardization of a single preferred cellular service, cellular devices, procurement, and support for King County, and ensures appropriate controls are established by delegating decision making authority and responsibilities.

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 are provided a King County technology asset. These requirements apply whether the user is working within a King County facility or working remotely.

B. Technology Asset

This policy applies to all King County owned cellular devices. This policy does not apply to personally owned cellular devices.

C. Exceptions

Requests for exception to this policy must follow the Department of Information Technology (KCIT) policy exception handling process.

IT Governance Policies apply to the Executive Branch. Applicable to independently elected agencies as baseline policy requirements.

III. Definitions

Cellular Service Provider: A company that sells wireless connectivity to customers for cellphone data and telephone calls.

Contractors: A business or entity that agrees to perform work under terms of a contract.

King County Owned: Any device, owned by King County, with the capability to process, store or transmit information independently.

Mobile Operating System: Software that allows smartphones, tablet PCs and other devices to run applications and programs.

Personal Device: Any device, owned by an individual, with the capability to process, store or transmit information independently.

Remotely: From a distance without physical contact, typically by means of an electronic connection

Service Upgrades: The process of replacing a product and/or service with a newer version of the same product.

Document Code No.: [Note: Assigned by IT Governance before submitting to CIO for approval]

Title:

Page 2 of 3

Third Parties: A person or group besides the two primarily involved in a situation

Volunteers: A person who offers to take part in a task or job

Workforce members: Employees, residents, students, volunteers, and other persons who conduct, in performance of work for a covered entity, is under the direct control of King County.

IV. Policy

A. King County Owned Devices

1. The Department of Information Technology (KCIT) establishes a single primary cellular provider.
2. New cellular service will be provisioned on the primary cellular network, and the hardware assets will be procured from the primary cellular network authorized device list.
3. King County owned devices are required to have a supported mobile operating system version installed.
4. King County owned devices must adhere to the King County Device Security Policy ITG-P-21-13.

B. Personal Devices

1. Personal devices do not need to have service through King County's primary cellular service provider.
2. Personal devices must adhere to the King County Device Security Policy ITG-P-21-13.

V. Implementation Plan

- A. This policy becomes effective for countywide use on the date that it is signed by Chief Information Officer. All new cellular service and service upgrades must ensure compliance with this policy as of the effective date. The Business Management Council is responsible for implementation of this policy.
- B. Organization leadership is responsible for communicating this policy to the management structure within their respective departments and agencies and other appropriate parties.

VI. Maintenance

- A. This policy will be maintained by the Department of Information Technology, 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 continue is kept current
 3. Recommending updates to this policy and related resources

Document Code No.: [Note: Assigned by IT Governance before submitting to CIO for approval]

Title:

Page 3 of 3

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 and exceptions 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

- A. Potential threats to Information Technology security due to unknown or incorrect Asset's information
1. Unknown valuation of King County Information Technology Asset Inventory
 2. Auditor finding of incomplete and inaccurate Information Technology Asset Inventory
 3. Impacts to monetary discounts as part of vendor contracts due to inaccurate assets\
 4. Inability to realize provisioning and operational savings through standardization.

VIII. Appendices: [Note: List Appendices using formal titles.]

Associated standard to be developed
Exception request
King County Device Security Policy ITG-P-21-13