I. PURPOSE

This policy establishes controls related to Wireless Voice and Data Services. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

II. POLICY

The Commonwealth of Kentucky allows use of wireless devices, to include cellular telephones, when such use will improve efficiency, provide the ability to respond in emergencies, and/or enhance staff/client safety.

Commonwealth staff members should use wireless services, when appropriate, to accomplish job responsibilities more effectively and to enrich their performance skills.

If in the best interest of the Commonwealth, an agency may allow a staff member to use a personally owned wireless device for state business.

Unless secured by an available encryption method, staff members have no expectation of privacy associated with wireless services.

All requests for wireless services in the executive branch must be coordinated with the Cabinet/ Agency Wireless Coordinator.

Prior to submittal to the Cabinet/Agency Wireless Coordinator, the Commissioner or agency head must approve requests for wireless services. When a wireless device is reassigned to another staff member, the Cabinet/Agency Wireless Coordinator must be notified immediately.

Agency Responsibilities

To effectively manage communication cost and to provide a device for staff members, agencies should consider the creation of a loaner pool of wireless devices for distribution to staff on an as-needed basis. Agencies may also use calling cards to provide communication services.

The Cabinet/Agency is responsible for the replacement of lost or stolen state-owned devices.

The Cabinet/Agency is responsible for assigning a Cabinet/Agency Wireless Coordinator. It is the responsibility of the Cabinet/Agency Wireless Coordinator to maintain a master list of all state-owned wireless devices issued in their area of responsibility. This master listing shall indicate username, location, and wireless phone number or serial number. Upon request, monthly billing statements are

available to the Cabinet/Agency Wireless Coordinator. These may be further disseminated to management as necessary.

The agency may maintain records of staff usage.

Staff Responsibilities for Use of State-Owned Devices

Commonwealth staff members shall use their state-owned wireless devices and services according to CIO-060 Acceptable Use Policy.

Commonwealth staff members are required to comply with KRS 189.292(2) that provides "no person shall, while operating a motor vehicle that is in motion on the traveled portion of a roadway write, send or read text-based communication using a personal communication device to manually communicate with any person."

Staff members shall avoid transmitting sensitive or confidential information over any wireless network without approved security services or encryption tools. All state-owned devices shall use a security access code to open the device. Manufacturer-deemed critical security updates will be installed within five business days. Routine manufacturer's updates will be complete within 30 days. State owned devices shall include a missing device application, and the service provided by the application shall be activated to help locate the missing device. The device and the assigned wireless service number is the property of the Commonwealth and shall be returned to the Commonwealth. The state-owned device accessing ky.gov must use the associated application for email and multi-factor authentication.

Staff using state owned wireless devices are responsible for always securing them. All wireless device losses shall be reported to the Cabinet/Agency Wireless Coordinator immediately.

Staff Responsibilities for Use of Personal Devices to Access ky.gov Email Accounts

Commonwealth staff members shall access their ky.gov email account from personal devices in accordance with CIO-060 Acceptable Use Policy.

Commonwealth staff members are required to comply with KRS 189.292(2) that provides "no person shall, while operating a motor vehicle that is in motion on the traveled portion of a roadway write, send or read text-based communication using a personal communication device to manually communicate with any person."

All personal devices used to access ky.gov email accounts shall comply with the following:

- Staff members shall avoid transmitting sensitive or confidential information over

any wireless network without approved security services or encryption tools.

- All personal devices shall use a security access code to open the device.
- Manufacturer-deemed critical security updates will be installed within five business days. Routine manufacturer's updates will be complete within 30 days.
- Devices shall include a missing device application, and the service provided by the application shall be activated to help locate the missing device.
- The personal device accessing ky.gov must use the associated application for email and multi-factor authentication.

The ky.gov account is the property of the Commonwealth.

Staff using wireless devices to access their ky.gov accounts are responsible for always securing the device. All wireless device losses shall be reported to the Cabinet/Agency Wireless Coordinator immediately.

III. COMPLIANCE AND DISCIPLINARY ACTION

Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Failure to comply with this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

IV. APPLICABILITY

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

V. REFERENCES

Helpful references can be found on the Enterprise IT Policies webpage.