Policy Title and #	CIO-078: Wireless LAN				
Effective Date:	06/01/2003	Revision Date:	04/21/2021	Review Date:	04/21/2021

POLICY STATEMENT:

This policy establishes controls related to the security and data integrity measures required for secure wireless Local Area Network installations within the state's intranet zone to balance the interests of the various stakeholders and increase business value for all parties. The policy provides guidance in decision-making and practices that optimize resource, mitigate risk, and Maximize return on investment.

DEFINITIONS:

Local Area Network (LAN): a computer network that links devices within a building or group of adjacent buildings.

Service Set Identifier (SSID): a unique ID for naming wireless networks.

POLICY:

The Commonwealth Office of Technology shall provide wireless access to state government employees, contractors, and vendors through two standard network SSIDs: ***KY-Secure*** and ***KY-Guest***. COT may allow agencies to use vendor-managed networks, but they must be isolated from the state's managed network SSIDs and shall not be used for official Commonwealth business. Agencies shall request approval for vendor-managed networks via the COT exceptions process.

Usernames and passwords for the two standard network SSIDs shall conform to the Commonwealth's CIO-072 IT Access Control and User Access Management Policy, and use of wireless resources shall comply with the CIO-060 Acceptable Use Policy.

State government employees and contractors with state-provided wireless devices shall authenticate to ***KY-Secure*** using their Active Directory (AD) credentials when accessing internal state resources and networks. COT shall use AD groups to restrict wireless access to appropriate users.

COT provides wireless Internet access to guests and vendors of the Commonwealth through the ***KY-Guest*** network. Users must self-register to receive login credentials prior to allowing access. This network shall not terminate inside the intranet, separating non-Commonwealth equipment from the Commonwealth's networks.

COT will conduct periodic security reviews of the wireless network. COT shall review wireless LANs periodically to minimize signal bleed outside of planned coverage areas. COT shall apply appropriate software and firmware updates to managed wireless equipment on a regular schedule, as updates are released.

AUTHORITY:

KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

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.

RESPONSIBILITY FOR COMPLIANCE:
Each agency shall ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding 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.

MAINTENANCE:
COT's Office of Contracts and Privacy is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

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