

**Office of the Chief Information Officer  
Enterprise Policy**

**Policy Number:** CIO-078

**Effective Date:** 06/10/2003

**Revision Date:** 03/01/2013

**Subject:** Intranet Wireless Local Area Network (WLAN) Policy

**Policy:** The Commonwealth Office of Technology (COT) is responsible for ensuring the confidentiality, integrity, and availability of the Commonwealth's computing environment. The purpose of this policy is to outline security and data integrity measures required for secure wireless LAN installations within the state's intranet zone.

**Policy Maintenance:** The Office of the CIO has issued this Enterprise Policy. The Commonwealth Office of Technology (COT), Office of Infrastructure Services, is responsible for the maintenance of this policy. All agencies and employees within the Executive Branch of state government shall adhere to this policy. However, agencies may choose to add to this policy, in order to enforce more restrictive policies as appropriate. Therefore, employees are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy. All CIO policies are on an annual review cycle.

**Responsibility for Compliance:** Each agency is responsible for assuring that appropriate employees within its organizational authority have been made aware of the provisions of this policy, that compliance is expected, and that unauthorized and/or neglectful installations of wireless LANs that expose the Commonwealth's network infrastructure to intruders and/or attacks may result in disciplinary action pursuant to KRS 18A up to, and including dismissal.

Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Therefore, it is important that agencies assess risks at least annually by testing and evaluating system security controls when wireless technologies are deployed. Agencies should use this risk assessment to determine business needs and wireless access for users.

***An agency should not undertake wireless deployment for any operations until it has examined and can acceptably manage and mitigate the risks to its information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies because their unique security requirements will determine which products should be considered for purchase.***

*It is the responsibility of each Cabinet and agency to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for COT's efforts to remediate issues related to insecure wireless LAN installations. Failure to comply may also result in termination of access to the network infrastructure.*

**Procedures:**

**Before implementation, all customers that utilize the Kentucky Information Highway (KIH) must have installation approval by COT, Office of Infrastructure Services for any intranet wireless LAN.** At this time, the Commonwealth Office of Technology recommends the use of wireless network technology only as a solution for special or unique business requirements and not for general-purpose deployment.

**Enterprise Standards:**

The following security standards and network configurations are required for all intranet wireless LAN installations:

- Three standard network SSIDs are broadcasted from the Commonwealth's access points. These SSIDs are **ky-secure, ky-open, and ky-voip**.

- The **ky-secure** network is designed to provide secure wireless access for Commonwealth controlled equipment. Utilizing Active Directory and the security zone design of the Commonwealth's networks, wireless users can be logically placed behind their agency's firewall, eliminating the need for a separate VPN connection. This allows the wireless users to be controlled by the agency's firewalls in a network that is separate from the traditional wired equipment. Active directory groups should be utilized to restrict wireless access to select groups of users.
- The **ky-open** network is designed to provide wireless Internet access to guests and vendors of the Commonwealth. This network is restrictive of traffic, and utilizes a Captive Portal to require users to login for access. Access to this network is granted via a self-registration portal and user passwords are delivered via SMS or email. This network must not terminate inside the intranet in order to separate non-Commonwealth equipment from the Commonwealth's networks.
- The **ky-voip** network provides wireless access for COT managed Voice Over IP phones that utilize wireless technologies. This SSID is controlled with MAC Address filtering, so that only authorized voice equipment can connect to the voice network.
- The **ky-secure** network utilizes WPA2 Enterprise with AES encryption. Authentication is controlled by Avaya Identity Engines (IDEngines) and utilizes active directory to validate credentials. Communication between wireless controller and IDEngines utilizes the MSCHAPv2 protocol to secure transmission of these credentials.
- The **ky-open** network is an open network and is developed for non-sensitive information for guests and vendors of the Commonwealth. Authentication is controlled by Avaya Identity Engines Guest Manager. A wireless portal is presented to the user that allows authentication or registration. Registered accounts within Guest Manager are valid for 24 hours in order for guests and vendors to register for internet access. This network does not allow access into the Commonwealth's networks without a VPN connection.
- Usernames and passwords must conform to the [Commonwealth's Enterprise User ID and Password Policy, CIO-072](#).

The following wireless security best practices should be reviewed and considered by agencies before deployment and during operation of a wireless LAN:

- Periodic security reviews should be conducted to ensure that changes to the wireless LAN have not exposed the network to intruders. Software and firmware updates from the manufacturer should be applied to all wireless equipment as soon as possible after release.
- A wireless survey should be completed in order to minimize signal bleed to the outside of the planned coverage area.

SSIDs should be separated into secure and insecure networks. Networks that connect to the Commonwealth's intranet zones should be secured using encryption in accordance to [Enterprise Architecture and Standards, 5000 Domain, Category 5100 Encryption](#) in order to protect credentials and sensitive data. Insecure networks that will not be used to transmit any sensitive data, and/or have non-commonwealth hardware connected to them should not traverse sensitive data segments and should utilize another form of authentication to provide the identities of those users.

#### Resources:

- CIO-072, Commonwealth's Enterprise UserID and Password Policy:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13212/>
- Enterprise Architecture and Standards, 5000 Security Domain, Category 5100 Encryption:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-301110/>

**\*END\***