Education and Workforce Development Cabinet
POLICY/PROCEDURE

Policy Number: EDU-18 **Effective Date: June 1, 2007**
Revision Date: March 7, 2007

Subject: Intranet Wireless Local Area Network (WLAN) Policy

Policy: This policy supports the Commonwealth Office of Technology (COT) and Education and Workforce Development Cabinet (EDU)

Scope: This policy applies to all EDU employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to agency business on an EDU maintained server or workstation.

Policy/Procedure Maintenance Responsibility: The EDU Security Audit Group (SAG) is responsible for the maintenance of this policy. The Chief Information Officer (CIO) is responsible for the revision of the EDU Policy and Procedures Manual (PPM). The EDU CIO is responsible for authorizing all changes to the PPM. However, departments/agencies within the Cabinet may choose to add to this policy, in order to enforce more restrictive policies as appropriate. Therefore, employees are to refer to their department/agency's internal policy, which may have additional information or clarification of this Cabinet policy.

Applicability: All EDU employees and contractors shall adhere to the following policy. With respect to any Internet and Electronic Mail usage over wireless networks, all aspects of the Internet and Electronic Mail Acceptable Use Policy GOT-060 shall apply.

Responsibility for Compliance

Each Department is responsible for assuring that employees within their organizational authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that unauthorized and/or neglectful installations of wireless LANs that expose the Commonwealth's network infrastructure or State's confidential data to intruders and/or attack may result in disciplinary action pursuant to KRS 18A up to and including dismissal. It is also each Department's responsibility to enforce and manage this policy.

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 more frequently, test and evaluate system security controls when wireless technologies are deployed.

Enterprise Standards:

The following security standards and network configurations are required for all intranet wireless LAN installations, within the state infrastructure see:
CIO-078 -- Wireless LAN Policy

- http://gotsource.ky.gov/dsweb/Get/Document-21536

CIO-076 -- Firewall and Virtual Private Network Administration Policy

- http://gotsource.ky.gov/dsweb/Get/Document-13776

Cabinet Standards:

Personnel conducting State Business with state issued equipment and using WLAN (other than Email) shall:

- Sign policy acknowledgement
- Use VPN CIO-076 -- Firewall and Virtual Private Network Administration Policy
- Meet the requirements in Laptop Policy (EDU- 08) http://www.my.edcabinet.ky.gov/Policy/LaptopPolicyEDU-08.pdf
- In addition the home WLAN will be configured to provide the most secure computing environment and encryption as possible.

Agency Responsibilities

It is the responsibility of each Cabinet and agency to enforce and manage this policy within the state's infrastructure. 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.

It is the responsibility of each agency to enforce and manage this policy of users requesting WLAN. Failure to comply may result in termination of the capability of Wireless Access on the device used.

Employee Responsibilities

It is the responsibility of each employee to ensure the most secure environment as possible and comply with this policy. Failure to comply may result in termination of the capability of Wireless Access on the device used.

Use the strongest encryption practical for the network encrypt all of the information transmitted through the access point. When using the wireless Access Point (WAP) there are two types, the security-enabled wireless network and the unsecured wireless network. Use the security-enabled access point to prevent signals from being "hijacked" and data compromised, if a security-enabled access point is not available then all system updates must be current (operating patches, software patches and virus protection). Using a wireless connection outside the state network and then accessing data inside the network requires a VPN connection to ensure data confidentiality and integrity.

Recommended procedures for configuring and securing personal WLAN (home) to prevent "hijacking" of the wireless signal and gaining access to information stored on the computer.

Password Protect Your Base station / Change the Default Password

All too often when setting up a WiFi base station users will fail to change the manufacturer's default password. The default password for any base station model is well known. Anyone within range of a base station using the default user name and password could commandeer it and create all sorts of mischief. We strongly recommend that you change the default username and password to your base station.
How-to Tutorials: Linksys | NETGEAR | D-Link | Apple Airport

Require Encrypted Passwords for WiFi Access

If you don't want strangers accessing the Internet over your WiFi network, you can set the base station to allow access only to those users who enter the correct password. These passwords are encrypted (or scrambled) to prevent interception when transmitted. Older base stations use Wireless Equivalent Privacy (WEP) encryption to scramble the passwords. A newer encryption protocol, called Wireless Protected Access (WPA), is more secure. We recommend WPA. Here are instructions for both.
How-to Tutorials for WPA Passwords: Linksys | NETGEAR | Apple Airport
How-to Tutorials for WEP Passwords: Linksys | NETGEAR | D-Link | Apple Airport

Restrict WiFi Access to Only Your Computers (MAC Address Control)

You can set your base station to allow WiFi access to only your computers. The base station will recognize your computer by a unique identifying number called a Machine Access Code (MAC) address. Each computer has one. Type in the addresses of each MAC address you want to allow onto your WiFi network.
How to Find A MAC Address: Windows XP OS
How-to Tutorials: Linksys | NETGEAR | Apple Airport

Don't Broadcast Your SSID

Another security option you may want to employ in conjunction with strong password access and/or MAC address control is disabling the SSID broadcast. By default, all WiFi base stations broadcast their presence -- known as the Service Set Identifier (SSID) -- to anyone within range. It's a call sign. You can reconfigure the base station to not broadcast the SSID -- somewhat like a stealth mode. This is not an inherently secure option. Nevertheless, this tactic will keep out most random passersby.
How-to Tutorial: Linksys | NETGEAR | Apple Airport

Review Cycle:
Annually

Timeline:
Revision Date: March 9, 2007
Review Date: November 30, 2011
Effective Date: June 1, 2007

Enterprise Security and Policies
Cross Reference #: http://technology.ky.gov/governance/Pages/policies.aspx
CIO-078 -- Wireless LAN Policy
CIO-076 -- Firewall and Virtual Private Network Administration Policy

DTS Standards
Cross Reference #:
Education Cabinet Internet and E-mail Acceptable EDU-01
Laptop Policy (EDU- 08)
Anti-Virus Policy (EDU-11)
Digital Data Storage-Transport (EDU-13)

Acknowledgement of Policy

I _____(**print name**) have read and understand the conditions of the Laptop Policy EDU-16 for the laptop computer assigned to me.

Laptop Inventory Tag number:_____

Laptop Serial number:_____

Signature: _____

Date: _____

Management signature: _____

Date: _____