State of Arkansas **Agency #200-00**
Office of the State Executive Chief Information Officer
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Best Practices Statement – Wireless Security

Title: Wireless Security

Document Number: BP-70-010

Effective Date: 2/1/2006

Published by: Office of Information Technology

1.0 Purpose

Wireless technology gives users the ability to access data and applications from more locations in a cost effective manner, but wireless technology also presents problems in terms of security. All information assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. For these reasons, appropriate security measures are essential when deploying wireless technology.

2.0 Scope

This best practices statement is recommended for all state agencies, boards, commissions and institutions of higher education.

3.0 Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies. The State Security Office, under the state's Executive Chief Information Officer, defines an environment for strategic security architecture and sets security standards and policies for information technology in state government. In order to apply appropriate security measures, data must first be classified to determine its sensitivity and required availability.

4.0 References

4.1 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.

4.2 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Best Practices Recommendation

5.1 All wireless devices should be protected by a personal firewall, except in instances where firewall technology is not available.

5.2 No agency should be entirely dependent on wireless technology for connectivity.

5.3 All WAP (wireless application protocol) configuration parameters (Service Set Identifier (SSID), keys, passwords, channels, etc.) that can be changed from the default manufacturer settings should be changed from the default. Also, the beacon interval on the WAP should be set to the longest interval possible. Where applicable, the new settings should be complex and not easily discerned or provide clues to the location, agency, or data / system description.

5.4 The placement of wireless LAN Access Points (WAP) should be strategically located to prevent the interception of wireless signals by unauthorized individuals or outside the intended coverage area. WAPs should be mounted above ceiling tiles, out of plain sight, or otherwise publicly inaccessible and not visible to unauthorized persons. The range of WAPs should also be tested to ensure that signals are not being transmitted outside the intended coverage area.

5.5 The strongest available Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) encryption should be employed with maximum key length and should be upgraded as newer technology is available.

5.6 WAP connections should be restricted to only identified, expected, listed, and known Message Authentication Code (MAC) addresses.

5.7 Shared encryption keys should be changed on a regular basis not to exceed 30 days.

5.8 Software and firmware updates from the wireless manufacturer should be applied to the WAP and affected wireless cards as soon as possible after release to keep the security updated.

5.9 Periodic security reviews should be conducted to ensure that changes to the wireless LAN have not exposed the network to intruders. In addition, the network should be periodically scanned to detect unauthorized devices.

5.10 The 802.11 series wireless data technology uses frequencies not requiring individual FCC licensing. Therefore, it is easy to end up with two groups with devices using overlapping frequencies. State agencies should be mindful of this fact and cooperate with their wireless neighbors.

6.0 Revision History

Date	Description of Change
2/1/2006	Original Best Practices Statement Published

7.0 Definitions

7.1 LAN (Local Area Network):
A group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area

7.2 MAC (Message Authentication Code) address:
A MAC is a cryptographic checksum that results from passing data through a message authentication algorithm.

7.3 SSID (Service Set Identifier):
Identifies and specifies which 802.11 network you are joining

7.4 WEP (Wired Equivalent Privacy):
A security protocol, specified in the IEEE Wireless Fidelity (WiFi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

7.5 WPA (Wi-Fi Protected Access):

7.5.1.1 Wi-Fi Protected Access is a specification of standards-based, interoperable security enhancements that increase the data protection and access control for wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is derived from and will be forward compatible with the upcoming IEEE 802.11i standard.

8.0 Related Resources

8.1 FCC Wireless Website: http://wireless.fcc.gov/

8.2 SANS website: www.sans.org

8.3 Bluetooth website: www.bluetooth.com

8.4 Wi-Fi Alliance website: www.wifialliance.org

9.0 Inquiries

Direct inquiries about this best practice recommendation to:

Office of Information Technology
Enterprise Architecture
124 West Capitol Avenue Suite 990, Little Rock, Arkansas 72201
Phone: 501-682-4300
FAX: 501-682-2040
Email: SharedArchitecture@arkansas.gov

OIT policies can be found on the Internet at: http://www.cio.arkansas.gov/techarch