

Statewide Information Security Standards

Standards Category: Information Security

Title: Statewide Wireless Access Standards

Number: S-107-03.21-10

Applicability: This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Status: Adopted Draft Other: _____

Dates: (Effective Dates/Revisions/Reviews)

Effective: June 1, 2010 Revisions: N/A Scheduled Review by: June 1, 2012

Prepared by: DAS Enterprise Information Strategy and Policy Division (EISPD)

Adopted by: 
Dugan Petty, State Chief Information Officer

6/30/10
Date

Statutory Authority: ORS 182.122

Enterprise Standard:

Minimum -

3.21. Wireless Access Standards:

- 3.21.1 Industry supported wireless access standards 802.11 shall be used by wireless access points.
- 3.21.2 The decision of whether, and how, guest access will be allowed shall be documented. Guest access via a wireless entry point shall be configured to only allow Internet access but prevent access to internal network resources.
- 3.21.3 For non-guest access the Wireless Protected Access2 (WPA2) protocol with AES encryption shall be deployed for data encryption to further protect transmitted information. Current versions of IEEE standards are 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i and 802.11n.
- 3.21.4 Comprehensive security assessments and inventory of wireless access shall be performed at regular and random intervals. Assessments shall include validating that unauthorized access points do not exist in the agency and testing the boundaries of wireless access.
- 3.21.5 Data shall be encrypted in transit in accordance with the Encryption Standards in section 4.4.
- 3.21.6 Access points shall be placed in physically secure or hidden areas to prevent unauthorized physical access and user manipulation.

- 3.21.7 Non-default SSID shall be used for wireless networks. SSIDs shall not reveal information about the network, agency name or location.
- 3.21.8 Nonessential management protocols shall be disabled on access points.
- 3.21.9 The "ad hoc mode" for 802.11 on wireless clients shall be disabled when technically possible.
- 3.21.10 Administrative access to manage the wireless device shall only be enabled via a dedicated wired management VLAN. Access to administrative functions shall be disabled via the wireless interface.
- 3.21.11 If the access point supports logging, turn it on and review the logs on a regular basis in accordance with the Log Management Standards in section 3.9.

Recommended –

3.22. Wireless Access Recommended Best Practices:

- 3.22.1 External boundary protection should be implemented around the physical perimeter of buildings containing access points. These protections include locating access points interior walls and, wherever possible, using enterprise class systems that use controller based AP configuration management.
- 3.22.2 Guest access should be restricted such that only authorized guests have access.
- 3.22.3 A firewall should be placed between the wired infrastructure and the wireless network in accordance with the Security Zone and Network Security Management (Local Area Network and Wide Area Network Standards in section 3.13

Section (1) - Purpose and Objective: The goal of communications and operations management is to ensure the correct and secure operations of information processing facilities. This section describes security standards and best practices for Antivirus and Malware, Workstation Management and Desktop Security, Mobile Device Management, Server Management, Log Management, Information Backup, Security Zone and Network Security Management, Intrusion Detection and Prevention, Email, Remote Access, and Wireless Access.

Section (2) – Agency Deviations: In circumstances where the standards can/will not be implemented, the agency director must sign the Statewide Information Security Plan and Statewide Information Security Standards Deviation Report documenting compensating controls have been applied to adequately protect the information or acceptance of risk. This report must be kept on file for review by auditors or during a security assessment.

Section (3) – Standards Review: This standard will be reviewed at least every two years and updated as needed.