



S T A T E O F M A R Y L A N D
DEPARTMENT OF INFORMATION TECHNOLOGY

Wireless LAN Security Policy

1.0 Purpose

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to any DoIT network. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Director of EIS are approved for connectivity to DoIT's networks.

2.0 Scope

This policy covers all wireless data communication devices physically connected to any of DoIT's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without connectivity to DoIT's networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points

All wireless Access Points / Base Stations connected to the network must be registered and approved by DoIT. All approved Access Points / Base Stations are subject to periodic penetration tests and audits.

3.2 Approved Technology

All wireless LAN hardware implementations shall utilize Wi-Fi certified devices that are configured to use the latest security features available.

3.3 Physical Location

Security mechanisms should be put in place to prevent the theft, alteration, or misuse of Access Points / Base Stations. All devices shall be locked and secured in an appropriate manner.

3.4 Configuration

The default SSID and administrative username / password shall be changed on all Access Points / Base Stations. Device management shall utilize secure protocols such as HTTPS and SSH. If SNMP is used in the management environment, change all default SNMP community strings, otherwise disable it. Access Points / Base Stations should be placed strategically and configured so that the SSID broadcast range does not exceed the physical perimeter of the building. If configurable, adjust the SSID beacon transmission rate to the highest value. Console access shall be password protected.

3.5 Authentication and Transmission

All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology.

3.6 Internet-only Deployments

Access Points / Base Stations deployed to provide Internet-only service shall be separated from the internal network by denying all internal services. Access Point / Base Station management shall be limited to internal or console users and not available to wireless clients.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Term	Definition
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach.
Wi-Fi Certified	Wi-Fi certified is a program for testing products to the 802.11 industry standards for interoperability, security, easy installation, and reliability.

6.0 Revision History

Policy Created	September 2008
Revised to address Internet-only applications	December 2008
Revised to drop WPA and add Wi-Fi requirement Added secure authentication channel requirement	December 2009