Wireless Networks

Standard ID
IOT-CS-SEC-111

Published Date
9/16/2006

Effective Date
9/16/2006

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
11.0 Protective Technology (PR.PT)
  11.4 PR.PT-4
    11.4.1 Network Protection

Purpose
The information below sets the requirements for implementation of wireless access points on the state network.

Scope
All Devices that Connect to the State Network

Statement
The following are requirements for Wireless Networking at the State:

1. IOT must be included in discussions related to deployment or changes to 802.11 Wi-Fi (Wireless Fidelity) needs.
2. IOT will work with the agency to determine the number of wireless access points necessary and design a configuration capable of meeting the security policy, technology and business needs.

Clarification: No access points are permitted on the state network or in state facilities if not part of the IOT Wi-Fi service. (Do not connect Wi-Fi access points that were not provided by IOT)

IOT Service

IOT's 802.11 service is subject to the compliance requirements below:

- Wireless access points (AP) are centrally configured, controlled and monitored by IOT. IOT reserves the right to disable the wireless networks as needed if problems occur.
- Default SSIDs are changed using long non-meaningful strings of characters, including letters & numbers
- SSID broadcast are disabled, except for the Public Wireless LAN.
- Administrator account default passwords are changed.
- Use the highest encryption algorithm possible (minimum allowed would be AES).
- All traffic over the WLAN is encrypted, except for the traffic on the Public WLAN, which is tunneled outside the firewall.
• IOT’s Wireless network utilizes WPA2-PEAP authentication using Active Directory credentials.

Roles
Agency Management
IOT Personnel

Responsibilities
Agency Management/Executive Management must include IOT in any discussions related to wireless deployment needs. IOT shall configure wireless networking in accordance with this Standard.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this standard

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to appropriately configure wireless networking.

Compliance
IOT Security will periodically walk through the building looking for wireless access points. It will also establish a list of contacts throughout the building that will be asked to notify IOT if they notice any wireless access points of concern.

Exceptions
Exceptions will be handled on a case by case basis through the State CISO.