Travis County Technology & Security Standard

Secure Wireless Access Point (AP) Standard

Version #: 1.1 **Approved By**: Paul Hopingardner, Chief Information Officer
Effective Date: November 28, 2016

Standard

The standard is intended for Wireless Access Points (AP) that provide access to any portion of the Travis County Infrastructure.

Placement

APs must be mounted in secured areas or in a manner as to prevent unauthorized physical access and user manipulation. Range boundaries must limit the coverage area to only what is needed for operational purposes.

AP Wireless network must be insulated, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), from the infrastructure. Access between wireless networks and the wired network should be limited to only operational needs.

Configuration

Any production network SSIDs should not be broadcast openly. SSID feature must be disabled so that the client SSID match that of the AP. The SSID character string should not contain any agency identifiable information (division, department, street, etc.) or services.

The minimally acceptable cryptographic algorithms is WPA2 AES or higher. Encryption key sizes must be at least 128-bits and the default shared keys must be replaced by unique keys.

Ad hoc mode and all other nonessential management protocols on the APs must be disabled. If logging is supported, it should be enabled.

Management

User authentication and encryption mechanisms for the management interface of the AP must be enabled with strong administrative passwords and ensure that all passwords are changed in accordance with the Travis County Password Policy.

APs can only be access and authenticated through Active Directory. APs should not have any SSH or Telnet to the local access point.

Management access and authentication must occur via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.

Publicly Available Wireless Network

The public wireless network must be completely separated from the Travis County Infrastructure. The public wireless may be throttled depending on network performance. Additionally, the network may be monitored per the County's Acceptable Use Policy.

Contact

Chief Security Information Officer
700 Lavaca Street, 4th Floor
Austin, TX 78701
P: 512.854.9175

Travis County Technology & Security Standard

Standard Revision

Version	Purpose/Changes	Editor	Date
1.0	Standard Creation	ITS Policy Committee	11/23/2016
1.1	Updated contact information and name due to new CIO	Joyce Miller	12/13/2019