



Taylor County

Board of County Commissioners'

Policy Manual

7.07

Policy #:	Title:	Effective Date:
2010-13	Wireless Communication Policy	07/06/10

PURPOSE

This policy prohibits access to TCBCB networks via unsecured wireless communication devices. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by DTIS are approved for connectivity to TCBCB networks.

REFERENCE

Not Applicable

POLICY

Register Access Points and Cards

All wireless Access Points / Base Stations connected to any TCBCB network must be registered and approved by DTIS. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in county laptop or desktop computers must be registered with IS

Approved Technology

All wireless LAN access must use DTIS-approved vendor products and security configurations.

Encryption and Authentication

All computers with wireless LAN devices must utilize a DTIS-approved wireless device to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.

Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the county name, division title, employee name, or product identifier.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

RESPONSIBLE DEPARTMENT

Technology and Information Systems

SUNSET DATE

Sunset Date: 07/06/15