Diocese of Pensacola-Tallahassee Wireless Communication Policy

1. Overview

The purpose of this policy is to secure and protect the information assets owned by Diocese of Pensacola-Tallahassee. Diocese of Pensacola-Tallahassee provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Diocese of Pensacola-Tallahassee grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Diocese of Pensacola-Tallahassee network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a Diocese of Pensacola-Tallahassee network.

2.0 Scope

All employees, contractors, consultants, temporary and other workers at the Diocese of Pensacola-Tallahassee, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Diocese of Pensacola-Tallahassee must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Diocese of Pensacola-Tallahassee network or reside on a Diocese of Pensacola-Tallahassee site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, tablets, pads and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

The Information Security Department must approve exceptions to this policy in advance.

3.0 Policy Statement

All wireless infrastructure devices that reside at a Diocese of Pensacola-Tallahassee site and connect to a Diocese of Pensacola-Tallahassee network, or provide access to information classified as Diocese of Pensacola-Tallahassee Confidential, Diocese of Pensacola-Tallahassee Highly Confidential, or Diocese of Pensacola-Tallahassee Restricted must:

3.1 Use Diocese of Pensacola-Tallahassee approved authentication protocols and infrastructure.
3.2 Use Diocese of Pensacola-Tallahassee approved encryption protocols.
3.3 Maintain a hardware address (MAC address) that can be registered and tracked.
3.4 Not interfere with wireless access deployments maintained by other support organizations.

4.0 Home Wireless Device Requirements

4.1 Wireless infrastructure devices that provide direct access to the Diocese of Pensacola-Tallahassee network must conform to Section 3.0.
4.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Diocese of Pensacola-Tallahassee network. Access to the Diocese of Pensacola-Tallahassee network through this device must use standard remote access authentication.
4.3 Secured connections to Diocesan data, using RDS, VPN, or terminal services using authenticated user access, are acceptable**.**
4.4 Using data "hotspots" are acceptable as secured connections as they use cellular encryption standards that meet Diocesan requirements.

5.0 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the Diocese of Pensacola-Tallahassee

6.0 Definitions

Term	Definition
Corporate connectivity	A connection that provides access to a Diocese of Pensacola-Tallahassee network.
Diocese of Pensacola-Tallahassee network	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Diocese of Pensacola-Tallahassee approved authentication protocols	Strong password access to any system, non-default network device password**s**
Diocese of Pensacola-Tallahassee approved encryption protocols	WEP, WPA2 or standard cellular data encryption
Enterprise Class Teleworker (ECT)	An end-to-end hardware VPN solution for teleworker access to the Diocese of Pensacola-Tallahassee network.
Information assets	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
MAC address	The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

7.0 Revision History

May 5, 2011: Section 3.0: delete
~~3.1 Abide by the standards specified in the Wireless Communication Standard.~~
~~3.2 Be installed, supported, and maintained by an approved support team.~~
May 5, 2011: Section 4.0: delete
~~**4.2** Be isolated from the diocesan network (that is it must not provide any connectivity to diocesan systems) and comply with the DMZ Lab Security Policy or the Internal Lab Security Policy.~~
May 5, 2011: Section 4.0: update
4.1 All lab wireless infrastructure devices that provide access to Diocese of Pensacola-Tallahassee Confidential, Diocese of Pensacola-Tallahassee Highly Confidential, or Diocese of Pensacola-Tallahassee Restricted information must adhere to section **3.0**
May 5, 2011: Section 5.0: update
5.1 Wireless infrastructure devices that provide direct access to the Diocese of Pensacola-Tallahassee network must conform to **Section 3.0.** ~~the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.~~
July 1, 2012: Section 4.0: delete
~~**4.0 Lab and Isolated Wireless Device Requirements**~~
~~**4.1** All lab wireless infrastructure devices that provide access to Diocese of Pensacola-Tallahassee Confidential, Diocese of Pensacola-Tallahassee Highly Confidential, or Diocese of Pensacola-Tallahassee Restricted information must adhere to section Lab and isolated wireless devices that do not provide general network connectivity to the Diocese of Pensacola-Tallahassee network must:~~
~~**4.2** Be isolated from the diocesan network; that is it must not provide any connectivity to diocesan systems.~~
~~**4.3** Not interfere with wireless access deployments maintained by other support organizations.~~
18 July 2013: Section 2.0: addition: to endpoint devices including, but not limited to, laptops, desktops, cellular phones, tablets, pads and personal digital assistants (PDAs).

18 July 2013: added Section 4.3 Secured connections to Diocesan data, using RDS or terminal services using authenticated user access, are acceptable**.**
30Jan2020: added: section 4.3 " RDS, or VPN,"
30Jan2020: added: Section 4.4 "Using data "hotspots" are acceptable as secured connections as they use cellular encryption standards that meet Diocesan requirements."
30Jan2020: added: Section 6.0 Definitions "Diocese of Pensacola-Tallahassee approved authentication protocols, Diocese of Pensacola-Tallahassee approved encryption protocols"