SECTION: 3.4

SUBJECT: **Wireless Communication Policy**

AUTHORITY: **Florida Statute Chapter 282.318 - Security of Data and Information Technology Resources;**
Florida Statute Chapter 815 – Computer Related Crimes;
Florida Administrative Code Chapter 71A-1 - Florida Information Technology Resources Security Policies and Procedures

Policy:

In accordance with the above statutes and rule, it is the policy of the Florida Fish and Wildlife Conservation Commission (FWC) to ensure protection and security of its electronic networks. This policy establishes the standard for the use and configuration of wireless access devices that connect to the FWC's networks. The policy is designed to minimize the potential exposure to FWC from damages that may result from the use of insecure wireless access devices. Damages include the loss of sensitive exempt or confidential and exempt data, intellectual property, damage to public image, damage to critical FWC internal systems, etc. Only wireless access devices that meet the criteria of this policy are approved for connectivity to the FWC's networks.

Contents:

General guidelines:

3.4.1 Definitions

A. **Access** – To approach, view, instruct, communicate with, store data in, retrieve data from or otherwise make use of computers or information resources.

B. **Access Point** – A station that transmits and receives data.

C. **Audit** – See: Security Audit

D. **Authentication** – The process that verifies the claimed identity or access eligibility of a station, originator or individual as established by an identification process.

E. **Authorization** – A positive determination by the information resource/data owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the resource/data owner's permission to access the resource.

F. **Data** – A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted or processed by people or automated means.

G. **Encryption** – Cryptographic transformation of data (called “plaintext”) into a form (called “cipher-text”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption”, which is a transformation that restores encrypted data to its original state. Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are control parameters: a key value that varies the transformation and, in some cases, an initialization value that establishes the starting state of the algorithm.

H. **IP Forwarding** – is the relaying of IP packets from one network segment to another in a computer network.

I. **“Information Technology,” “information technology resources” “information resources” or “information technology system”** include any transmission, emission and reception of signs, signals, writings, images and sounds of intelligence of any nature by wire, radio, optical or other electromagnetic systems and includes all facilities and equipment owned, leased or used by all agencies and political subdivisions of state government and a full-service information-processing facility offering hardware, software, operations, integration, networking and consulting services.

J. **LAN** – Local Area Network – See Networks or Networking.

K. **Networks or Networking** – Networks provide design, programming, development and operational support for local area networks (“LANs”), wide area networks (“WANs”) and other networks. Networks support client/server applications, telephony support, high-speed or real-time audio and video support and may develop and/or utilize bridges, routers, gateways and transport media.

L. **Personal Password** – A password that is known by only one person and is used to authenticate that person’s identity.

M. **User Authentication** - A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

N. **Security Audit** – An independent formal review and examination of system records and activities to determine the adequacy of system controls ensure compliance with established security policy and operational procedures, detect breaches in security and recommend any indicated changes in any of the foregoing.

O. **Site Survey** – A report on the physical, architectural, geographical and electrical limitations of the site and their effect on a wireless solution.

P. **Wireless Access Device** – Any data communication device (e.g., computer, cellular phone, PDA, laptop, etc.) that connects to the internal FWC network. This includes anypersonally-owned device which connects wirelessly to the internal FWC network and locally stores FWC data or email messages. It does not include non-FWC-owned devices which connect to FWC email through an Internet browser using Outlook Web Access (OWA).

3.4.2 Scope:

This policy covers all wireless access devices capable of transmitting and receiving packet data, including but not limited to: wireless access points, personal computers using either integrated or removable wireless networking technology such as a PC card, cellular phones, PDAs, etc. connected to any FWC internal network. Wireless access devices and/or networks without any connectivity to FWC's networks do not fall under the purview of this policy.

3.4.3 User Requirements:

A. All wireless Access Points connected to the corporate network must be installed and approved by the Office of Information Technology, Network Support. These Access Points are subject to periodic penetration tests and audits.
B. All wireless LAN access must use Office of Information Technology, Network Support -approved vendor products and security configurations.
C. Wireless network adapters must **NOT** be configured to use Ad-Hoc mode.

3.4.4 Network Services Requirements:

A. All wireless LAN access must use Office of Information Technology, Network Support-approved vendor products and security configurations.
B. A site survey shall be conducted by the Office of Information Technology prior to wireless implementation. The site survey will include tests and measurements to define coverage requirements, locate potential sources of interference and identify potential security risks and threats.
C. Strong mutual user authentication shall be utilized.
D. When passing wireless traffic over public networks use of strong encryption or utilization of State of Florida sanctioned VPNs shall be used.
E. IP forwarding shall be disabled on all wireless clients.
F. Theft or loss of a wireless-enabled device shall be reported using the FWC's Incident Reporting Procedures.
G. Wireless devices shall not be connected simultaneously to another wired or wireless network other than standard utilization of a commercial carrier signal.
H. Wireless devices shall be password protected and must be configured to automatically lock after 15 minutes or less of inactivity.
I. Wireless devices having the features of personal firewalls and anti-virus capability shall be enabled.
J. In order to ensure wireless access points and wireless networks remain secure after their initial installation, periodic checks will be performed by the FWC IT Security Manager.

3.4.5 Enforcement

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

Established: 03/2006 Rev: 09/2010; 07/01/2011

Approved:

Gregory L. Holder **July 1, 2011**

Executive Director or Designee **Date**