


Florida Fish and Wildlife Conservation Commission
Internal Management Policies and Procedures (IMPP)

	TITLE Remote Access Policy	IMPP 3.2
		EFFECTIVE DATE 02/20/2017
	APPLICABILITY All Employees	RESCINDS/AMENDS 06/27/2011

REFERENCES:

AUTHORITY: Executive Director; Florida Statute Chapter 282.318 and Florida Administrative Code Chapter 71A-1

Policy

The purpose of this policy is to establish reasonable conditions the FWC would impose to ensure the appropriate use and maintenance of any FWC equipment or items provided for use at remote locations (e.g. home as office). This policy also addresses installation and maintenance of any telephone equipment and ongoing communications costs at the remote site which is to be used for official use only. Reference Section 110.171, Florida Statutes.

This policy defines standards for connecting to FWC's network from any device. These standards are designed to minimize the potential exposure to FWC from damages that may result from unauthorized use of FWC resources. 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.

- Contents:
- 3.2.1** Definitions
 - 3.2.2** Scope
 - 3.2.3** Requirements
 - 3.2.4** Enforcement

3.2.1 Definitions

Modem - Stands for **Modulator/demodulator**, a peripheral device that connects computers to each other via some cabling infrastructure, for sending and receiving data.

Dial-in Modem – A dial-in modem is required if a standard telephone line and technology is the available transmission medium for data. The telephone number of the target device is “dialed” to initiate the data connection. This is legacy technology.

Digital Subscriber Line (DSL) - Another form of high-speed Internet access. DSL works over standard phone lines and also supports higher data transfer speeds than traditional/legacy dial-in modems.

Cable Modem - Cable and communications companies provide residential and business Internet access over coaxial and fiber cable. A cable modem is required when coaxial cable is the transmission medium. Coaxial cable is widely available and distributed.

Remote Access - Any access to FWC's network through a non-FWC controlled network, device or medium.

Wireless Connectivity - A connection to a network via a wireless data provider network. Normally, the wireless data provider provides access to the Internet and the connection is secured via a Virtual Private Network (VPN) for connection to the FWC or State of Florida network

3.2.2 Scope

This policy applies to all individuals with a FWC-owned or personally-owned computer or workstation used to connect to the FWC network. This policy applies to remote access connections used to do work on behalf of FWC, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, DSL, VPN, wireless and cable modems, etc.

- A. Participation in a remote access program may not be possible for every individual. Remote access is meant to be an alternative method of meeting FWC business needs. The Commission may refuse to extend remote access privileges to any individual or terminate a remote access arrangement at any time. An individual's eligibility to remotely access the FWC's computer network will be determined by their manager.

It is the responsibility of all individuals with remote access privileges to FWC's network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to FWC.

- B. The Commission may provide tools and equipment for remotely accessing the computer network. This may include computer hardware, software, wireless access, phone lines, e-mail, voicemail, connectivity to host applications and other applicable equipment as deemed necessary. The use of equipment and software provided by FWC for remotely accessing the Commission's computer network, is limited to authorized persons and for purposes relating to FWC business. The Commission will provide for repairs to Commission equipment. When an authorized individual uses her/his own equipment, he/she is responsible for maintenance and repair of equipment.
- C. In regards to telecommunications circuits, it is acceptable for the Commission to install and pay for the telecommunications equipment and lines when limited to Commission use. It is also acceptable for the employee to install and pay for the telecommunications equipment and lines and use those facilities for Commission and personal use.
- D. FWC Technical Support Staff will only provide support for equipment and software provided by the Commission.
- E. The Commission will bear no responsibility if the installation or use of any necessary software causes system lockups, crashes or complete or partial data loss. The individual is solely responsible for backing up data on their personal machine before beginning any Commission work. At its discretion, the Commission will disallow remote access for any individual using a personal computer that proves incapable, for any reason, of not working correctly with the Commission-provided software or being used in a production environment.

- F. For additional information regarding FWC's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., call FWC Tech Support at 850-487-8438.

3.2.3 Requirements

- A. All individuals with FWC remote access may only connect to the FWC network using FWC-approved secure remote connections.
- B. Secure remote access must be strictly controlled. Control will be enforced via a one-time password authentication or public/private keys with standard FWC login procedures.
- C. FWC logins and passwords must be kept strictly confidential, known only to the user.
- D. All individuals with FWC remote access privileges must ensure that their FWC-owned or personal computer or workstation, which is remotely connected to FWC's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- E. All individuals with FWC remote access privileges to the FWC network shall not share their client connections while connected to the FWC network.
- F. All individuals with FWC remote access privileges to FWC's network should use their FWC email accounts to conduct FWC business. In the event the FWC email is not available, it is permissible to send from external email accounts with a copy sent to the originator's FWC email account.
- G. All hosts that are connected to FWC internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes individually owned personal computers.

3.2.4 Enforcement

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

Approved: **Eric Sutton**
Nick Wiley, Executive Director or Designee

Date: **02/20/2017**

History: Est. 12/14/2014; Rev. 09/2010; 06/2011; 02/2017