


Florida Fish and Wildlife Conservation Commission Internal Management Policies and Procedures (IMPP)		
	TITLE	IMPP
	Information Technology Resource Usage	3.7
	APPLICABILITY	EFFECTIVE DATE
	All Staff	11/9/2022
		RESCINDS/AMENDS
		11/12/2021
REFERENCES: CHAPTER 119, FS; CHAPTER 282.318, FS; 60GG-2, FLORIDA INFORMATION TECHNOLOGY STANDARDS; IMPP's 1.7, 1.8, 3.2, 3.3, 3.4, 6.1, 6.34 AUTHORITY: CHAPTER 282.318, FS; 60 GG-2, FLORIDA INFORMATION TECHNOLOGY STANDARDS, EXECUTIVE DIRECTOR		
IMPP OWNER: OFFICE OF INFORMATION TECHNOLOGY		

POLICY

The Fish and Wildlife Conservation Commission (FWC) has an extensive electronic communications network that serves as a valuable tool for conducting business. This document establishes policy and guidelines to ensure the proper use of the information and information technology resources contained within this network and to safeguard all information that is stored, transmitted, or received through the system. Additionally, this policy addresses devices and methods that are utilized to communicate FWC business whether or not it flows through the FWC network.

The network consists of the FWC email system, FWC intranet and internet websites and supporting applications, VPN, wired and wireless connections, database systems, videoconferencing, Internet access, telephone service using voice over IP communications and any supporting network infrastructure. Collectively, these systems are referred to as the FWC network. All communications (including, but not limited to email content, internet sessions, voice over IP connections, data, and information storage, etc.) conveyed by or contained within these systems are subject to this policy.

This policy is intended to comply with [Chapter 282.318](#), Florida Statute and [Chapter 60GG-2](#), Florida Administrative Code (F.A.C.) and to establish standards for connecting to the FWC network or utilizing FWC information technology resources in any manner, from any location, and/or for any reason. Every person with access to the FWC network is responsible for knowing and following the guidelines for electronic communication use outlined here. Failure to comply with policies and procedures in this IMPP may result in disciplinary action up to and including dismissal.

This policy is developed in support of the Florida Information Technology Resources Security Policies and Procedures, [Chapter 60GG-2](#), F.A.C. This rule recognizes the value of state information technology resources and data and the need to protect the confidentiality, integrity, and availability of these resources. Data and resources must be reliable and must be available to those who are authorized to use them.

The purpose of the Florida Information Technology Standards:

1. Document a framework of information security practices for state agencies to safeguard the confidentiality, integrity, and availability of Florida government data and information technology resources.
2. Define minimum standards to be used by state agencies to categorize information and information technology resources based on the objectives of providing appropriate levels of information security according to risk levels.
3. Define minimum management, operational and technical security controls to be used by state agencies to secure information and information technology resources.
4. FWC may find it necessary to employ compensating security controls when the FWC is unable to implement a security standard, or the standard is not cost-effective due to the specific nature of a system or its environment. After the FWC analyzes the issue, a compensating control may be employed if the FWC documents the analysis results and senior management documents the acceptance of the risk associated with employing the compensating control. All related documentation shall be retained by the FWC Information Security Manager. This documentation is confidential, pursuant to Section 282.318, Florida Statutes, except that such information shall be available to the Auditor General and the Agency for Enterprise Information Technology.

Contents: 3.7.1: Definitions

3.7.2: Scope

3.7.3: Access and Monitoring Activities

3.7.4: Standards

3.7.5: Examples of Unacceptable Use

3.7.6: Additional Guidelines for Managers and Users

3.7.7: File Management and Records Retention

3.7.8: Enforcement

3.7.1 - DEFINITIONS

- A. Administrative Convenience Records** - Reproductions of record (master) copies, prepared simultaneously or separately, which are not designated as the official copy.
- B. Authentication** - The process of verifying that a user is who they purport to be.
- C. Authorized FWC Personnel** – Those individuals whose official duties include making determinations of findings in personnel matters or those responsible for network security. In the event of personnel misconduct, it includes the immediate and/or chain of command supervisor(s) subject to senior management consent. In cases related to fraud, waste, abuse, or violation of laws, it includes the Inspector General and General Counsel (see IMPP 1.8, *Office of Inspector General*).

- D. Computer use and confidentiality agreement** - An individual's acknowledgement of the FWC policies and procedures (see IMPP 6.34, *Employee Conduct, Demeanor and Conflict of Interest* and the related *IMPP Acknowledgement Letter*); this agreement includes adhering to the provisions of this IMPP 3.7 and the individual's acknowledgement of accountability and compliance. For non-FWC personnel, the FWC Help Desk will provide a copy of IMPP 3.7 to any other user at the time of issuance of their network ID and password with the individual's implied acknowledgement occurring on their use of any of FWC's information technology resources.
- E. Confidentiality** - Information which is defined by Florida or federal law as being accessible only to those authorized to have access. Under the Florida Public Records law, Chapter 119, Florida Statutes, this information may be exempt from disclosure or confidential and exempt from disclosure.
- F. Incident Reporting Procedures** – Those procedures adopted in compliance with the Agency for Enterprise Information Technology in accordance with [Chapter 282.318, F.S.](#). Visit the Office of Information Technology (OIT) [Computer Security Incident SharePoint](#) and complete the required form.
- G. Information Technology Resources (ITR)** - FWC computer hardware, software, networks, communication devices, applications, databases, and data.
- H. Least Privilege** – The practice of granting the minimum set of access rights to data and information resources that are required for an individual to perform their job responsibilities.
- I. Malware** - Malicious software.
- J. Need to Know** – The practice of only sharing information with those individuals who have a specific need to have the information to perform their job duties and meet their responsibilities.
- K. Objectionable material** - material including, but not limited to images, text or documents that depict, describe, or evidence nudity, obscenity, sexually- explicit activity, gambling or prejudice based on race, religion, gender, marital status, ethnicity, color, ancestry, sexual orientation, or national origin.
- L. Sniffing** – Monitoring and capturing network data.
- M. Transitory Messages** - Records that are created primarily to communicate information of short-term value. "Transitory" refers to short-term value based upon the content and purpose of the message, *not* the format or technology used to transmit it. Examples of transitory messages include, but are not limited to, reminders to employees about scheduled meetings or appointments; announcements of office events such as holiday parties or group lunches; and recipient copies of announcements of FWC-sponsored events such as exhibits, lectures, workshops, etc. Transitory messages are not intended to formalize or perpetuate knowledge and do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.
- N. User** - Any person or process authorized to use FWC information technology resources including, but not limited to employees, contractors, consultants, volunteers, trainees, and other persons who perform work for the FWC, whether or not they are paid by the FWC.

O. Warning Banner - Message displayed prior to or upon connection to a resource informing the user that activities may be monitored, or access is restricted.

P. Workstation - A device used to perform work related duties.

3.7.2 - SCOPE

This policy applies to all Users who have or are responsible for a user account on any system that resides in the FWC network of computing and/or networking resources. It applies to all messages, documents, data, images, and information conveyed by or contained within the FWC network -- in any form -- including correspondence, attachments, bulletin boards, discussion or reference databases and archives. Additionally, the scope applies to any public record created by an FWC employee, contractor or volunteer outside of the network.

3.7.3 – ACCESS AND MONITORING ACTIVITIES

Users that access and use the FWC network provide consent for Authorized FWC Personnel to access electronic communication messages and all systems or other resources for which the User is authorized. Users shall be granted access to FWC information and information technology resources based on the principles of “Least Privilege” and “Need to Know”.

FWC information owners shall be responsible for authorizing access to information and periodically reviewing access rights, based upon the level of the information’s risk, account change activity and error rates. For functions susceptible to fraudulent or other unauthorized activity, the FWC shall ensure separation of duties, so no individual can control the entire process.

If fraud, waste, abuse or violation of laws, policies or procedures is reported, the Office of the Inspector General (OIG) will specifically authorize access and/or monitoring activities before monitoring activities commence. This applies to business and personal messages transmitted over the FWC network. Every email sent or received in the FWC email system will be automatically archived. Users should have no expectation of privacy regarding any activities conducted over the FWC network.

3.7.4 - STANDARDS

A. Compliance with Applicable Laws, Policies and Procedures

1. Every User is responsible for complying with FWC security policies and procedures when performing FWC work or when using FWC information technology resources.
2. Every User is responsible for complying with all applicable State and Federal rules and laws.

B. Computer Use, Confidentiality Agreement and Security Training

Every user accessing FWC's Information Technology Resources (ITR) acknowledges, in writing, their responsibilities regarding adherence to computer use in this IMPP, the proper handling of exempt, and confidential and exempt information reflected in IMPP 1.7, and adherence to all FWC policies and procedures by completing an FWC *IMPP Acknowledgement Letter* at the time of initial employment. For non-FWC personnel accessing FWC's ITR, the FWC Help Desk will provide a copy of IMPP 3.7 at the time of issuance of their network ID and password with the individual's implied acknowledgement occurring on their use of any of FWC's ITR.

Users shall complete initial security awareness training within 30 days of reporting to work and on an annual basis thereafter.

C. Use of FWC Information Technology Resources

1. Access to FWC information technology resources is reserved for FWC- approved Users.
2. Authorized FWC Personnel shall have sole discretion to determine whether a use is personal or business.
3. Personal use must not interfere with the normal performance of a User's duties.
4. Personal use must not consume significant amounts of FWC information technology resources.
5. Users must obtain authorization before taking information technology equipment, software, or information away from an FWC facility. Mobile computing devices and software issued to Users and information to which Users have authorization to access may be taken away from FWC facilities for business purposes.
6. Computing devices shall only be issued to and used by FWC-authorized Users.
7. Only FWC-approved software shall be installed on FWC computing devices.
8. Only FWC-owned or FWC-managed mobile storage devices are authorized to store FWC data.
9. Users utilizing mobile computing devices used with exempt or confidential require encryption and the User shall ensure that all appropriate content is encrypted.
10. To prevent loss of data, Users must ensure that the only copy of FWC data is not permanently stored on a workstation or mobile device.
11. Non-FWC owned devices (e.g., computers, cellphones, tablets, MP3 players, thumb drives, printers) shall not be connected to FWC information technology resources without documented Chief Information Officer (or designee) authorization.
12. Users shall take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

13. Users shall immediately report lost or stolen mobile computing devices according to FWC's Incident Reporting Procedures (Also see 3.7.7, *Misuse of the Electronic Communications Network*).
14. Remote location access to ITR is covered in IMPP 3.2, *Remote Access Policy*.
15. Access by means of wireless access devices is covered in IMPP 3.4, *Wireless Communications Policy*.
16. Users are prohibited from creating new social media/networking websites or accounts on behalf of the FWC without prior authorization from the division/office director or their designee and the Community Relations Office (CRO.)
17. Users are prohibited from creating new cloud service provider accounts without prior authorization from the Office of Information Technology (OIT).
18. Users are prohibited from storing on any FWC devices or media any objectionable material.

D. Authentication

1. Users shall have unique user accounts.
2. Users shall be held accountable for their account activities.
3. FWC ITRs must be authenticated at a minimum by a strong password (see IMPP 3.3 *Password Policy*).
4. Users are responsible for safeguarding their passwords and other authentication methods.
5. Users must not share their FWC accounts, passwords, personal identification numbers, smart cards, identification badges or other devices used for identification and authentication purposes.
6. Users shall immediately report suspected account compromises by submitting a [Computer Security Incident Response](#) form.
7. Users shall immediately report lost smart cards or other devices used for identification and authentication purposes by submitting a Computer Security Incident Report form.

E. Privacy

1. Users shall have no expectation of privacy as it relates to information technology resource use.
2. Authorized FWC Personnel may inspect all files stored on the FWC network or computer systems, including removable media.
3. Authorized FWC Personnel may monitor the use of state ITR.
4. Use of state ITR constitutes consent to monitoring activities whether a warning banner is displayed or not.

F. Email

It is a requirement for all Users, who use email to perform their FWC responsibilities, to have an FWC email account. The FWC email system shall be used by all Users when conducting any FWC business by email so that a complete record of FWC email communications is retained in the email archives.

If there is a situation where the FWC email system cannot be used and work-related emails are sent using an FWC User's personal email account (i.e., law enforcement working undercover, emails sent to foreign addresses that are blocked by the FWC email system, etc.), these emails should be forwarded or copied to the User's FWC email account.

Volunteers, typically, do not have an FWC email account and may use their personal email accounts to communicate volunteer activity and work schedules. The FWC supervisor should be copied on any volunteer emails involving FWC business. If a volunteer's duties require extensive email communications, their supervisor may request an FWC email account for the volunteer. The supervisor is also responsible for ensuring the FWC email account is promptly terminated when the volunteer's duties end.

Users are always responsible for using the FWC computer resources in a professional, ethical, and lawful manner. It is recommended that personal email be kept separate from work email. Please note that all email messages are subject to monitoring and review and may be subject to disclosure through a public records request.

- 1. Acceptable Personal Email Use:** The email system may be used for the following type of activities if they do not conflict with policy guidelines or are otherwise prohibited herein:
 - a. Emergencies
 - b. Sending and receiving short messages.
 - c. Forwarding personal email to a non-FWC account.
- 2. Unacceptable Personal Email Use:** Personal use of the email system shall, not:
 - a. Interfere with the work performance of the User or his/her colleagues.
 - b. Have an undue impact on the operation of FWC's computer systems related to the transfer of information, resource capacity or introduction of viruses.
 - c. Violate any provision of this policy including:
 - i. Distribution of malware
 - ii. Forging email headers and disguising his/her identity.
 - iii. Propagating "chain" letters of any kind
 - iv. Auto-forwarding FWC email to a non-FWC email address
 - v. Use in conducting private business practices.
 - vi. Objectionable material.
- 3. Personal Use of the Email System is a privilege and may be revoked at any time.**

4. **Size of Email Messages (personal or work related):** Due to the considerable increase in email message volume, size and the related impact on long-term storage for enterprise message archiving and network traffic, all email Users are cautioned to limit the size and number of attachments/background materials. Additionally, Users are urged to create documents for attachments that are smaller (e.g., announcements should be less than 25MB in size with more restricted use of complex graphics which typically expand the content size. If complex/large documents or attachments are necessary to communicate an email's intent, consider using FWC's SharePoint facilities or OneDrive to save these documents/attachments and only refer to them by providing a link in the email to their SharePoint or OneDrive location.

5. Exempt or confidential information shall not be sent by email unless encrypted.

G. Internet: The Internet may be accessed for personal use under the following constraints. Users are permitted to briefly visit non-prohibited Internet sites or use email for personal reasons during non-work hours (supervisor approved breaks, lunch periods, or before/after work) subject to the limitations contained within this policy. Personal use of the Internet is a privilege which FWC provides for the convenience of its Users and is not a right of employment. Usage must not interfere with the User's job duties or compromise the functionality of FWC's network. Excessive personal use may constitute abuse of the privilege and may subject the User to disciplinary action. Personal use strictly prohibits FWC resources being used for private business practices. Users are always responsible to use FWC computer resources in a professional, ethical, and lawful manner.

1. Sound discretion and good judgment must be used in viewing non-work-related sites and personal use must be limited so that FWC business can be continued without undue interruption or delay.
2. **Acceptable Personal Internet Use:** The Internet may be used for the following type of activities if they do not conflict with policy guidelines or is otherwise prohibited herein:
 - a. Conducting personal research
 - b. Making on-line purchases
 - c. Surfing or browsing the web.
 - d. Visiting non-prohibited websites including those dealing with health matters, weather, news, business or work-related topics, community activities, career advancement, and personal enrichment
3. **Unacceptable Personal Internet Use:** Personal use of the Internet shall not:
 - a. Interfere with work performance.
 - b. Have an undue impact on the operation of the FWC network or computer systems related to the transfer of information, resource capacity, or introduction of viruses.

- c. Violate any provision of this policy including non-work-related access to the following prohibited websites:
 - i. Those websites with objectionable material.
 - ii. High bandwidth websites such as Internet radio, Internet TV, music/movie download, Internet streaming movies, online gaming etc., since these streaming/gaming sites can have enormous network performance impact to the entire FWC community.

4. Personal use of the Internet is a privilege that may be revoked at any time.

H. Workstation Security

- 1. Users shall not disable, alter, or circumvent FWC workstation security measures.
- 2. Users shall logoff or lock their workstations prior to leaving the work area.
- 3. Workstations shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.

I. Software

- 1. Only FWC-approved software authorized by OIT shall be installed on FWC-owned computers.
- 2. Illegal duplication of software is prohibited.

J. Hardware

No internal hardware changes shall be made to FWC ITR without OIT approval.

K. Network

- 1. Transmission of exempt or confidential information over the network shall be encrypted.
- 2. Monitoring, sniffing and related security activities shall be performed only by Authorized FWC Personnel, based on job duties and responsibilities.

3.7.5 – EXAMPLES OF UNACCEPTABLE USE

The following sections provide examples of activities which Users are prohibited from doing when using FWC ITR unless such User is conducting an authorized investigation or is specifically authorized by the OIG.

A. Unacceptable Use – Internal and External

- 1. Sending messages that are neither professional in nature nor in compliance with IMPP 6.34 *Employee Conduct, Demeanor, and Conflict of Interest* and the guidelines outlined in the Executive Director's presentation on *Leadership and Behavior Expectations*.

2. The expression of personal beliefs or philosophies that conflict with FWC policies or any government laws, ordinances, or regulations, unless the expression is defined as “Personal Opinion, Not FWC Official Position” and does not demean another individual. However, Users should be aware that expressions of personal opinions (IMPP 6.34) regardless of the method of communication that undermine FWC’s position may subject the User to discipline.
3. The unofficial dissemination of information or opinions about any aspect of FWC that is derogatory (via chat rooms, social media, emails, or other forums.)
4. FWC ITR shall not be used for personal profit, benefit, or gain, monetary or other.
5. Objectionable material shall not be stored on any FWC computers, mobile devices, network, external storage devices, or any other FWC storage media.

B. Additional Prohibitions and Requirements for Internet Access

1. All internet access shall utilize an FWC approved network.
2. The unauthorized use or possession of password cracking, network scanning programs, or other Internet security tools are strictly forbidden.
3. Users may not attempt to circumvent established FWC Internet security measures.

3.7.6 – ADDITIONAL GUIDELINES FOR MANAGERS AND USERS

Supervisors with responsibility for Users having access to the FWC network shall ensure those individuals are aware of the *Information Technology Resource Usage Policy*.

- A. When anyone under a supervisor’s control resigns, is terminated or transfers to another position, it is critical the supervisor immediately submit a New/Modify/Departed user form on the OIT SharePoint site. This will ensure that User’s access is immediately terminated or transferred.
- B. Supervisors are also responsible for reporting any status changes involving any third-party relationships they manage to ensure access privileges are removed when no longer needed. In no event should any FWC network ID be transferred to another User or agent.
- C. If any FWC User believes circumstances warrant accessing the contents or monitoring the use of an FWC network ID, please notify the OIG.
- D. Each User is responsible for reporting any unauthorized network/information access, tampering or prohibited/unauthorized activities according to FWC’s Incident Reporting Procedures (Also see 3.7.7, *Misuse of the Electronic Communications Network*).

3.7.7 – FILE MANAGEMENT AND RECORDS RETENTION

All Users are responsible for maintaining their electronic files in accordance with Records Management policies and procedures, including the handling of exempt or confidential and exempt information (see IMPP 1.7, *Commission Records*).

Unmanaged and unidentified electronic communication records residing on FWC computers and servers can impact FWC's ability to document and reconstruct FWC decision-making processes.

If appropriate, a User should discuss their D/O's specific records retention schedules with their immediate supervisor. Specific questions may be referred to FWC's Records Management Liaison Officer. The Records Management Liaison Officer may aid in preparing record retention schedules and facilitating approval.

Record schedules apply to records regardless of their format. This includes emails, text messages, and instant messages. Records created or maintained in electronic format fall into two categories, transitory and non-transitory, and shall be retained in accordance with the minimum retention requirements presented in these schedules. FWC does not permit the transmission of non-transitory electronic messages using any electronic messaging system unless approved by this policy or OIT for FWC use. OIT shall review any potential electronic messaging system to ensure that the system allows OIT to maintain and store the information to be made available upon request. Currently, the only approved electronic messaging systems are the FWC email system and MyFWCAAlert, the FWC's official Emergency Notification System.

Examples of unapproved messaging systems are:

- Instant messenger (including but not limited to AOL IM, Yahoo IM, Apple iMessage, WhatsApp, Line, WeChat, Jami, etc.)
- Personal email accounts (including but not limited to Gmail, Hotmail, Yahoo) except as approved by section 3.7.4 F.
- Social Media Messaging (including but not limited to Facebook, Twitter, Snapchat, Instagram etc.) unless approved by (CRO) and OIT.

Text messaging relating to agency business is not permitted on non-agency issued devices. Text messages on FWC issued devices are only authorized to be sent through the phone's standard messaging application. Third-Party applications for text messaging are not permitted. Messages through Apple iMessage are not permitted. Methods of messaging other than "traditional text messaging" are not able to be retained and therefore their use is prohibited.

All Electronic messaging of a non-transitory nature, which includes, but is not limited to non-transitory text messaging, shall be through FWC ITR and retained in accordance with retention schedules as set forth in *General Records Schedule GS1-SL for State and Local Agencies*, and General Records Schedule GS2 For Law Enforcement, Correctional Facilities and District Medical Examiners, and FWC specific Retention Schedules by Customer.

Users should be aware of the types of records stored in their email mailbox and archives. Electronic records covered by record retention schedules or related to policies and procedures must be maintained in accordance with such schedules/ policies. Preferably such will occur in electronic databases outside the scope of the email system and on the FWC network. By doing so, documents will be maintained and preserved by the Network Services Section using their standard backup procedures. If an FWC User chooses not to follow these procedures, the User shall archive this type of information on an FWC computer hard drive and maintain physical media backup copies (i.e., CDs/DVDs, USB storage devices, OIT approved cloud storage providers) so that data recovery is possible in the event of a hard drive failure.

3.7.8 – ENFORCEMENT

Misuse of FWC's ITR and the electronic communications network, or any other violation of this policy, may result in disciplinary action that could include termination as outlined in FWC's disciplinary standards.

FORMS

FORM NUMBER	FORM TITLE

Approved: Thomas H. Eason
Eric Sutton, Executive Director or Designee

Date: November 9, 2022

History: Est.: 08/11/2008; Rev 09/2010; 07/01/2011; 05/15/2013, 11/21/2021, 11/9/2022