Florida Fish and Wildlife Conservation Commission **Internal Management Policies and Procedures (IMPP)**		
	TITLE Mobile Device Use and Management	IMPP 3.12
		EFFECTIVE DATE 08/08/2017
	APPLICABILITY ALL MEMBERS	RESCINDS/AMENDS
REFERENCES: **AUTHORITY:** FLORIDA STATUTE CHAPTER 282; FLORIDA STATUTE CHAPTER 815; FLORIDA ADMINISTRATIVE CODE RULE 74-1; FLORIDA ADMINISTRATIVE CODE RULE 74-2; CRIMINAL JUSTICE INFORMATION SERVICES SECURITY POLICY		
IMPP OWNER: OFFICE OF INFORMATION TECHNOLOGY		

POLICY

In accordance with the above statutes and rules, the Florida Fish and Wildlife Conservation Commission (FWC) establishes this mobile device use and management policy, to effectively and efficiently make use of mobile device technologies, while protecting the integrity and confidentiality of sensitive data, applications, and the availability of information technology (IT) services for the FWC.

This policy will also enable the FWC to comply with security policies, processes, and procedure requirements as defined in Florida Administrative Code Rule 74-2.

This policy establishes rules and guidelines for the management of mobile device technologies in the enterprise IT environment, to protect the integrity and confidentiality of sensitive data, applications, and the availability of IT services for the FWC. This policy applies to all employees, consultants, vendors, contractors, and volunteers utilizing mobile device technology for accessing FWC IT resources.

Contents:

3.12.1 DEFINITIONS

A. Availability - the principle that authorized users have timely and reliable access to information and information technology resources.

B. Authentication – the process of verifying that a user is who he or she claims to be, such as a password, passcode or personal identification number (PIN).

C. Bring Your Own Device (BYOD) – BYOD describes the practice of allowing personal mobile devices to be used for agency business.

D. Choose Your Own Device (CYOD) - model in which an organization provides its employees with a limited choice of mobile computing devices that may be used to access organization resources. A more controlled and manageable version of BYOD model.

E. Computer Security Incident Response Team (CSIRT) – agency cross-divisional team responsible for receiving, reviewing, and responding to computer security incident reports and activity.

F. Confidentiality - the principle that information is accessible only to those authorized.

G. Critical Process - a vital or key agency process that, should it fall victim to fraud, cyberattack, or unauthorized activity, can seriously impact the agency's ability to fulfill its mission.

H. 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.

I. Information and Communication Technology (IT) Resources - data processing hardware, software and services, data, communications, supplies, personnel, facility resources, maintenance, and training.

J. Integrity - the principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

K. Personally Identifiable Information (PII) - any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

L. Malware – malicious software; general term used by computer professional to mean a variety of forms of hostile, intrusive, or annoying software or program code.

M. Mobile Device Management (MDM) – the ability to centrally secure, monitor, manage and support mobile devices deployed across service providers and enterprise connecting to agency IT resources. Centralized functionality includes, but is not limited to:

a. Firmware over-the-air updates
b. Diagnostics
c. Remote configuration and provisioning
d. Security
e. Network Usage and Support
f. Software Installation
g. Troubleshooting and Diagnostics Tools
h. Mobile asset tracking and management
i. Remote Wipe
j. Logging and Reporting
k. Remote Control and Administration

N. Mobile Devices – Mobile devices are small handheld or wearable devices or computers. Examples of these devices are smartphones, tablets, laptops, and other portable devices which can access IT resources.

O. Remote Wipe – Use of software to destroy data on a mobile device remotely.

P. Risk – the likelihood that a threat will occur and the potential impact of the threat

Q. Stakeholder – a person, group, organization, or state agency involved in or affected by a course of action related to state agency-owned IT resources.

R. Wireless Network – A means to access the network and public internet, over the air, without the need to connect to a physical wired network.

3.12.2 SCOPE

Mobile devices have become an integral part of the IT infrastructure. Mobile devices may be owned by the employing entity or personally owned by the employee. In some cases, the use of personally owned devices, selected from a pre-approved list (CYOD), to conduct work-related tasks may be allowed. Mobile devices, unlike traditional desktop computing configurations, are typically not physically connected to the agency's computing environment or network and can be used from any place in the world to connect to the agency's computing environment over the publicly accessible Internet. Convenience and availability are the major advantages of using mobile devices; however, these attributes also present additional risks to the agency. Specifically, the use of mobile devices increases the risk of:

- Information interception, resulting in a breach of sensitive data, enterprise reputation, adherence to regulation, and legal action.
- Malware propagation, which may result in data leakage, data destruction, data corruption, and unavailability of necessary data.

This policy covers all mobile devices used to access agency wireless networks, resources, data, and applications.

This policy will be reviewed annually to ensure compliance with legal and financial requirements remains reflective of the current technological landscape and address current and future business needs.

3.12.3 General Guidelines

A. The decision to provide a mobile device or allow a personally-owned mobile device will be based on a documented business need and executive or management approval.

B. The decision to approve the use of a given app, on an FWC-provided mobile device, will be based on a documented business need and executive or management approval.

C. FWC reserves the right to disconnect mobile devices or disable agency services without notification for both FWC-provided and personally-owned mobile devices.

D. Signed acceptance of this mobile device policy, and the Mobile Device User Agreement is required.

3.12.4 Requirements

A. Device Configurations – The following applies to both FWC-provided mobile devices as well as personally-provided mobile devices.

1. All Mobile devices connecting to FWC resources must comply with IMPP 3.7 IT Resource Usage Policy.
2. MDM tools will be installed and activated on all mobile devices before accessing FWC resources.
3. Mobile devices will adhere to agency authentication criteria (see IMPP 3.3 Password Policy).
4. Users should recognize that their use of, or access to, data provided by or through FWC networks may be monitored by FWC at any time. Users should presume that personal activity and data put on an agency-owned device may also be monitored by the agency.
5. Users must ensure that the use of any software on the device for work purposes doesn't violate the license agreement for the software.
6. All mobile devices, both personally owned and agency provided, will meet minimum hardware and software requirements as described in the Mobile Devices Specifications Document, found in the OIT Portal.

B. Mobile Device Security – The following applies to both FWC-provided mobile devices as well as personally-provided mobile devices.

1. Users are responsible for ensuring the physical security of mobile devices connecting to FWC resources.
2. Mobile devices must not be left in plain view in an unattended vehicle, even for a short period of time, and must not be left in a vehicle overnight.
3. Mobile devices must always be physically secured when not in the user's possession. If mobile devices are left unattended for any extended period, user must secure them in a locked environment outside of plain view (i.e. vehicle glove box or trunk).
4. FWC will use an MDM solution to secure mobile devices and enforce policies remotely. Before connecting mobile devices to FWC resources, the device must be set to be manageable by FWC's MDM solution.
5. Any attempt to contravene or bypass the MDM implementation will result in immediate disconnection of the device from FWC resources.

6. Criminal Justice Information (CJI) must not be stored on the devices, as defined in Section 4.1 of the Criminal Justice Information Services Security Policy.
7. FWC business related PII data must not be stored on mobile devices.
8. Forensic investigation could occur on any device used to access FWC resources in the event of an information security investigation.
9. Employees must immediately report lost or stolen mobile devices by following CSIRT policy and procedures (IMPP 3.8) or by contacting the IT Help Desk.
10. FWC will have the authority and ability to have a device remotely erased/wiped of FWC data if lost or stolen, or if the device owner is terminated or separates from the agency.

C. Personally-owned Mobile Devices (CYOD)

1. Personal mobile devices, prior to connecting to agency IT resources, require the end user to agree to and sign the Mobile Device User Agreement, and have proper FWC approval.
2. Personal mobile devices will be analyzed by the IT department to ensure that proper settings and encryption are enabled prior to access being allowed to the agency IT resources.
3. Personal mobile devices used to access agency resources, will comply with all policies covered under A and B above.

3.12.5 ENFORCEMENT

A. Violation of this policy may result in disciplinary action appropriate to the violation up to and including termination as outlined in the Commission's disciplinary standards.

B. The Office of Information Technology (OIT), with assistance from the program areas, will be responsible for monitoring compliance.

3.12.6 FORMS

FORM NUMBER	FORM TITLE
None	Mobile Device User Agreement

Approved: **Eric Sutton** Date: **08/08/2017**
Nick Wiley, Executive Director or Designee

History: Est.: 08/08/2017