SECTION: **3.3**

SUBJECT: **Password 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 to ensure protection and security of its electronic files and data. This policy sets the standards and structure of user names and passwords to protect FWC's data resources. All personnel who have or are responsible for a user account within the Florida Fish and Wildlife Conservation Commission network are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish standards for the use and creation of strong passwords, password protection, and the frequency of change of those passwords for FWC user accounts, and ensure all users of Florida Fish and Wildlife Conservation Commission Information Technology resources are made aware of this policy and the possible consequences of non-compliance with any part of this policy.

Contents:

General guidelines:

3.3.1 Definitions

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

B. Confidential Information – Information that is exempted from disclosure requirements under the provisions of applicable state or federal law, e.g., Chapter 119, Florida Statutes, the Florida Public Records Act.

C. Dictionary Attack - Refers to the general technique of trying to guess some secret by running through a list of likely possibilities, often a list of words from a dictionary. It contrasts to a brute force attack in which all possibilities are tried.

D. High risk application – the loss of confidentiality, availability or integrity

might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one of more of its primary functions, resulting in major damage to organizational assets, major financial loss or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

E. Information Technology, Information Technology Resources, Information Resources, Information Technology System – Includes any transmission, emission, and reception of signs, signals, writing, 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 this agency and political subdivisions of this agency.

F. Low risk application – the loss of confidentiality, availability or integrity might cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced, resulting in minor damage to organizational assets, minor financial loss or minor harm to individuals.

G. Moderate risk application – the loss of confidentiality, availability or integrity might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced, resulting in significant damage to organizational assets, significant financial loss or significant harm to individuals that does not involve loss of life or serious life threatening injuries.

H. Network or Networking Resources – Media which allow transfer of information between computers and provide design, programming, development and operational support for local area networks (LAN's), wide area networks (WAN's) and other networks. Networks support client/server applications, telephony, audio and video.

I. Password and Strong Password – A protected word or string of characters which serves as authentication of a person's identity ("personal password"), or which may be used to grant or deny access to private or shared data ("access password"). Passwords are used for various purposes. Some of the more common uses include: user-level accounts, web accounts, email accounts, and screen saver protection.

Strong passwords are the agency standard. They have the following characteristics:

- Contain eight or more characters
- Include both upper and lower case letters (e.g., A-Z, a-z)
- Contain digits (e.g., 0-9), punctuation characters and other special characters (e.g. ~, `, !, @, #, $, %, ^, &, *, (,), _, -, +, =, {, }, [,], |, \, :, ;, ", ', <, , >, ., ?, /)
- They are <u>NOT</u> words in common usage (including slang, dialect, jargon, etc.)
- They are <u>NOT</u> based on personal information, names of family, etc. One way to create a strong password that can be easily remembered

is to base it on a phrase, called a password phrase. For example, “This is one way to remember your password,” therefore the password could be “Tilw2Ryp.” In this example some letters were changed to numeric values, making the password strong and more complicated to ‘guess.’ The preceding is only an example and should not be used.

J. User Name (also called user id, login name, logon or user account) - A unique name for each user of a computer service which can be accessed by more than one user. Users may need to identify themselves for accounting, security, logging and resource management. Usually a person must also enter a password in order to access a service. Once the user has ‘logged’ on, the operating system will often use an identifier, e.g. an integer, to refer to them rather than their user name.

3.3.2 Scope

The scope of this policy includes all individuals who have or are responsible for a user account on any system that resides in the Florida Fish and Wildlife Conservation Commission network of computing and/or networking resources - employees, contractors, consultants, temporaries and volunteers. All user-level passwords, (e.g., email, desktop computer, etc.) which allow access to any FWC Information Resource must meet the requirements of this policy.

3.3.3 Requirements

A. Each user of a system that can be accessed by multiple users shall be assigned a unique user name and password.

B. Users are required to create strong passwords. Please refer to the definition of “strong” password in IMPP 3.3.1.

C. Passwords must be changed at least every 60 days for high risk applications, every 90 days for moderate risk applications, and every 180 days for low risk applications. Users will be notified automatically during logon when their password is about to expire.

D. Passwords shall not be stored in readable format on any system

E. User identification shall be authenticated before the system grants that user access to automated information.

F. A user’s access authorization shall be immediately removed from the system when the user’s employment is terminated or the user transfers to a position where access to the system is no longer required.

G. Consultants and contractors shall have their access rights carefully controlled and will be terminated immediately upon expiration of contracts

H. In situations where an employee, consultant or contractor is terminated under adverse conditions (such as termination of employment or reassignment), unsupervised system access shall be denied.

I. Users who need a password to be reset or changed by the Office of Information Technology or one of its service providers, such as DMS Enterprise Information Technology Services, shall follow the procedures posted on the OIT intranet website or call the OIT Helpdesk at 850-487-8438 for assistance.

J. If a password is, or is suspected to be, compromised, users shall report the incident to their supervisor.

K. Supervisors shall report all password-related incidents to the agency Computer Security Incident Response Team (CSIRT) via the OIT Helpdesk at 850-487-8438, or via email notifications to: CSIRT@myfwc.com.

3.3.4 Password Protection Guidance

A. Passwords for agency accounts should be different from non-agency access passwords (e.g., personal ISP accounts, etc.). Where possible, the same password should not be used for various agency access needs. For example, one password should be selected for workstations and separate passwords selected for web access.

B. Passwords should never be left in plain sight.

C. Passwords should not be shared with anyone, including administrative assistants, information technology professionals or supervisors. All passwords are to be treated as sensitive confidential information.

D. Passwords should not be inserted into email messages or other forms of clear text (plain text) messaging. Passwords should be secured by other means when delivered electronically.

3.3.5 Enforcement

A. The agency will conduct periodic security audits and evaluations of the agency's security program, the systems audit logs, and the processes and procedures utilized to monitor compliance with this policy.

B. All individuals who utilize Florida Fish and Wildlife Conservation Commission information technology resources, including contractors, consultants and temporary employees are required to read and acknowledge a Statement of Understanding concerning this policy, which is attached for reference. When an individual logs on to the network, a reminder that this policy applies to his/her usage of the network will be displayed. Clicking "OK" to proceed will serve as documentation that the user has read and understands this policy.

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

History: Est.: 03/2006; Rev: 09/2010; 06/27/2011

Approved

Gregory L. Holder — **Executive Director or Designee**

June 27, 2011 — **Date**

Statement of Understanding
for
Florida Fish and Wildlife Conservation Commission
Password Policy

All individuals who utilize Florida Fish and Wildlife Conservation Commission information technology resources, including contractors, consultants and temporary employees are required to read and acknowledge the following Statement of Understanding. If for some reason an electronic acknowledgment of understanding is unavailable at network log on, the form can be printed, signed and filed in an employee's personnel file. If a printed form is used, a copy of the signed form will be provided to the individual signing the statement. **For more information please contact the Florida Fish and Wildlife Conservation Commission, Office of Information Technology.**

I have read the Florida Fish and Wildlife Conservation Commission Password Policy and agree to abide by it as consideration for my continued employment by the Florida Fish and Wildlife Conservation Commission. I understand that violation of any part of this policy may result in disciplinary action, up to and including termination of employment.

_____ _____
Signature Date