SECTION: **3.8**

SUBJECT: **Computer Security Incident Reporting and Response Policy**

AUTHORITY: **Executive Director; Chapter 282.318, Florida Statutes - Security of Data and Information Technology Resources; Chapter 71A-1, Florida Administrative Code - Florida Information Technology Resources Security Policies and Procedures; Chapter 817.5681, Florida Statutes – Notification Requirements for Breaches of Security of Personal Information**

Policy:
To ensure all computer security incidents related to information technology resources and the communications network are promptly reported by Florida Fish and Wildlife Conservation Commission (FWC) workers and the appropriate Agency response is performed.

Purpose:
The purpose of this policy is to establish reporting and response procedures for all computer security incidents. The FWC's information technology resources must be protected against disruptions of the communications network and the destruction, improper modification, improper use or unauthorized disclosure of FWC information. Every person with access to the FWC network is responsible for knowing and following the guidelines for reporting computer security incidents. Failure to comply with policies and procedures shall result in disciplinary action up to and including dismissal. Appropriate incident response may include convening the Computer Security Incident Response Team (CSIRT), referrals to the Office of the Inspector General (OIG) for investigations or law enforcement involvement and notification requirements for breaches of security of personal information in the agency's records.

Contents:

3.8.1 Definitions:

A. Breach notification (as defined in section 817.5681 FS) – includes:

1. **Written notice**
2. **Electronic notice**, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code s.7001, General Rule of Validity, or if the person or business providing the notice has a valid email address for the subject person and the subject person has agreed to accept communications electronically.
3. **Substitute notice**, if the person demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:
   - **a.** Electronic mail or email notice when the person has an electronic mail or email address for the subject persons.
   - **b.** Conspicuous posting of the notice on the web page of the person, if the person maintains a web page.
   - **c.** Notification to major statewide media.

B. Computer Security Incident – any action or activity – accidental or deliberate – that causes the destruction, improper modification, improper use or unauthorized disclosure of confidential agency information or compromises the integrity of the agency's data or information resources. Examples of activities which would constitute an incident include unauthorized access to or disclosure of confidential information, denial of service attacks and loss or stolen devises with stored confidential information. An example of activity which would not constitute an incident would include receipt of a spam e-mail by a small number of FWC workers.

C. FWC Worker - Any person authorized to use the FWC information technology resources including employees, contractors, volunteers, trainees and other persons who perform work for FWC, whether or not they are paid by the agency.

D. Incident – See Computer Security Incident.

E. Incident Reporting Form –See the Office of Information Technology (OIT) SharePoint site at: OIT's *SharePoint site*, click on *Report a Computer Security Incident,* and complete the required form.

F. Information technology resources (ITR) - FWC computer hardware, software, networks, devices, connections, applications and data.

G. Personal information (as defined in section 817.5681 FS)– an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

1. Social security number
2. Driver's license number or Florida Identification Card number
3. Account number, credit card number or debit card number, in combination

with any required security code, access code or password that would permit access to an individual's financial account.

Personal information does not include publically available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

3.8.2 Scope: This policy applies to all information and information resources, whether owned and operated by or operated on behalf of FWC. It applies to all individuals who have an FWC user account on any FWC system, including employees, contractors, consultants, temporaries and volunteers.

3.8.3 Description of the Incident Reporting & Response Process

Step 1 – Incident occurs

Step 2 – FWC worker reports incident, using the Incident Reporting Form

Step 3 – Incident received by Information Security Manager (ISM) and preliminary classification is made

Step 4 – If the reported incident is out of scope of the CSIRT or the incident is clearly a class 1 incident, ISM takes appropriate action. This may include referral to OIT technical personnel. Response is communicated to FWC worker who reported the incident, if appropriate. Class 1 incidents are documented, logged by ISM and closed upon completion of action.

Step 5 – If incident is not clearly a class 1 incident, ISM convenes CSIRT core team and appropriated support members, for classification of incident and determination of appropriate response (i.e., OIG investigation, OIG referral to law enforcement, determination of breach of personal information or other action).

Step 6 – ISM reports class 2 and 3 incidents to Agency for Enterprise Information Technology's Office of Information Security (AEIT OIS) within 24 hours of incident report.

Step 7 – ISM documents CSIRT action plan, tracks incident until completion of action, conducts a debriefing of lessons learned and closes the incident.

3.8.4 Incident Reporting Responsibilities of all FWC Workers

All incidents shall be reported by FWC workers using the Incident Reporting form, located at *Report a Computer Security Incident.*

3.8.5 Classification and Logging of Incidents

A. Classification of Security Incidents

Computer security incidents are classified based upon risk severity, using seven criteria: data classification, legal issues, business impact, expanse of service disruption, threat potential, public interest and policy infraction. If an incident meets criteria in different severity ratings, the incident shall be classified in highest category.

B. Class 1 Incident: Low Severity Rating

A Class 1 incident is any incident that has a low impact to Commission information technology resources and is contained within the Commission.

The following criteria define Class 1 incidents:

- **Data classification**: Unauthorized disclosure of confidential information has not occurred.
- **Legal issues**: Lost or stolen hardware that has low monetary value or is not part of a mission critical system.
- **Business impact**: Denial of service incident does not involve mission critical services.
- **Expanse of service disruption**: Incident is within a single business unit.
- **Threat potential**: Threat to other information technology resources is minimal.
- **Public interest**: Low potential for public interest.
- **Policy infraction**: Security policy violations determined by the Commission.

C. Class 2 Incident: Moderate Severity Rating

A Class 2 incident is any incident that has a moderate impact to agency information technology resources and is contained within FWC.

The following criteria define Class 2 incidents:

- **Data classification**: Unauthorized disclosure of confidential information has not been determined.
- **Legal issues**: Lost or stolen hardware with high monetary value or that is part of a mission critical system.
- **Business impact**: Incident involves mission critical services.
- **Expanse of service disruption**: Denial of service incident affects multiple business units within FWC.
- **Threat potential**: Threat to other information technology resources is possible.
- **Public interest**: There is a potential for public interest.
- **Policy infraction**: Security policy violations determined by the agency.

D. Class 3 Incident: High Severity Rating

A Class 3 incident is any incident that has impacted or has the potential to impact other state information technology resources and/or events of public interest.

The following criteria define Class 3 incidents:

- **Data classification**: Unauthorized disclosure of confidential information has occurred outside FWC.
- **Legal issues**: Incident investigation and response is transferred to law enforcement.

- **Business impact**: Threat to other agency information technology resources is high.
- **Expanse of service disruption**: Denial of services disruption is wide spread across FWC and/other agencies.
- **Threat potential**: Incident has potential to become wide spread across the agency and/or threatens external, third-party information technology resources.
- **Public interest**: There is active public interest in the incident.
- **Policy infraction**: Security policy violations determined by the agency.

E. Change in Classification

An incident may be escalated (classification severity increased) or downgraded (classification decreased) in the following ways and the reasons for doing so shall be documented in the incident documentation:

1. Decision of the CSIRT leader or designee.
2. Decision of the Chief Information Officer (CIO), ISM or OIG.
3. Request by senior management or the Executive Director.
4. Escalation of the magnitude of the event.

3.8.6 Computer Security Incident Response Team (CSIRT)

The formation of a CSIRT will establish roles, responsibilities and procedures for responding to FWC computer security incidents.

A. Composition of Team

1. The core of the CSIRT is the Chief Information Officer (CIO), the Information Security Manager (ISM) and the designated representative from the Office of the Inspector General (OIG).
2. The ISM will act as team leader. Responsibilities of team leader include:
   a. Convene CSIRT.
   b. Select appropriate support members, as necessary, for the reported incident.
   c. Contact the CIO.
   d. Conduct meetings of the CSIRT.
   e. Ensure meetings are documented.
   f. Direct team training on an on-going basis.
   g. Periodically report status of incidents to the CIO.
   h. Manage incidents.
   i. Ensure Class 2 and Class 3 incidents are reported to the AEIT OIS.
   j. Ensure class 2 and Class 3 incidents are documented.
   k. Coordinate team incident research and response activities.
   l. Conduct a debriefing of lessons learned and report to the CIO.
3. The CSIRT should have representatives from the following areas:
   a. Legal Office
   b. Office of Human Resources
   c. Public Information Officer/Community Relations Office
   d. Office of Information Technology (technical experts on servers, network devices, databases, applications, etc., as appropriate)

e. Finance & Budget Office
f. Law Enforcement
g. Other areas required for a specific incident, for the duration of the incident.

4. In cases where an incident may have originated from an employee or employees who report directly or indirectly to the CIO, the team will report a conflict of interest to the CIO. The CIO will implement a temporary alternative reporting structure to the Executive Director or designee.

5. In the event that a similar conflict of interest involved a core team member, that conflict must be reported to the designated team leader and to the CIO immediately. The CIO will determine the appropriate course of action based upon the circumstances surrounding the incident and the nature of the conflict of interest.

B. Team Expertise & Responsibilities

1. Chief Information Officer (CIO)
a. Overall responsibility for the CSIRT
b. Resolve any conflict of interest issues.
c. Ensure appropriate CSIRT practices relative to statute, rule, OIS guidelines, and agency policy. The CIO will ensure that the CSIRT operates according to FWC CSIRT procedures, as well as, all applicable authorities, references and policies.

2. Office of the Inspector General (OIG) Representative
a. Senior member
b. Convene investigations, following FWC investigative procedures.
c. Notify FDLE or appropriate law enforcement agency of incidents where there are reasonable grounds to believe a criminal violation has occurred and serve on liaison team with law enforcement agency, OIS, FWC ISM and FWC Law Enforcement.

3. Information Security Manager (ISM)
a. Coordinate the notification to users affected by the incident.
b. Coordinate technical tasks required by the review.
c. Provide an analysis of the incident including root causes.
d. Serve on liaison team with outside law enforcement, OIS, FWC Law Enforcement and the OIG
e. Compile the final report and recommendations of the CSIRT.

4. Legal Office
a. Brief members on legal issues such as privacy, search and seizure, Fourth Amendment and wiretap.
b. Advise members regarding protection of individual rights.
c. Advise Public Information Officer as necessary.
d. Act as liaison with outside legal counsel.

5. Office of Human Resources
a. Advise the core members on personnel policies and procedures.
b. Make recommendations for handling sensitive employee information.

c. Ensure that employees' rights are appropriately protected.

6. Public Information Officer (PIO)/Commuity Relations Office
- **a.** Act as a single point of contact for the media.
- **b.** Inform impacted users to refer all media inquiries to the PIO.

7. OIT Technical Specialists
- **a.** Respond to all activities that might interrupt any critical information technology services owned and managed by FWC. This includes those systems both inside and outside the agency's firewall (i.e., servers, network devices, databases, applications).
- **b.** Report any unusual or suspicious activities.
- **c.** Brief the CSIRT on operational procedures as needed.
- **d.** Contain the incident as appropriate.
- **e.** Protect the evidence of the incident according to the agency's guidelines and instructions of the core team.
- **f.** Assess and report to CSIRT any damage to systems and data.
- **g.** Assist in identifying the scope of the incident.
- **h.** Make recommendations to mitigate the incident.

8. Finance and Budget Office
- **a.** Brief the team on financial procedures.
- **b.** Conduct financial reviews if necessary.
- **c.** Report findings to CSIRT.

9. Law Enforcement
- **a.** Brief the team on law enforcement issues.
- **b.** Assist OIT with protection of evidence of the incident and preserving the chain of custody.
- **c.** Serve on liaison team with OIG, outside law enforcement, OIS and ISM, to track incidents reported to outside law enforcement by the OIG, where there are reasonable grounds to believe a criminal violation has occurred.

C. CSIRT Responsibilities

1. Classify FWC security incidents.

2. Convene upon notification of a reported Class 2 or Class 3 computer security incident.

3. Conduct a preliminary assessment to determine the root cause, source, nature and extent of damage.

4. Recommend response to a computer security incident.

5. Select additional support members as necessary for the reported incident.

6. Maintain confidentiality of information related to incidents.

7. Assist with recovery efforts and provide reports to the CIO and senior management.

8. Document incidents, including recommended actions and lessons learned.

9. Report incidents to the AEIT OIS.

10. Maintain awareness of and implement procedures for effective response to computer security incidents.

11. Stay current on functional and security operations for the technologies within these areas of responsibility.

D. Team Training and Simulation Exercise Requirements

1. Members should be familiar with this CSIRT procedure, published AEIT guidelines, the *Information Security Rule* and the relevant statutes associated with this policy.

2. FWC should conduct periodic simulation exercises of the CSIRT to offer initial training to CSIRT members and their backups and annual refresher training thereafter. An *After Action Report* should be written by the Information Security Manager following each exercise to describe what happened, lesson learned and how the CSIRT response can be improved.

3.8.7 Incident Review Process and Determination of Appropriate Action to be Taken

A. Convening CSIRT

1. The CSIRT will be convened at least once a quarter, for regularly scheduled meetings.

2. CSIRT will be convened to review all Class 2 and Class 3 incidents and determine the appropriate action to be taken.

3. CSIRT reviews will ensure the following:

a. Subject's rights are preserved to the extent dictated by FWC policies and pertinent laws, rules and regulations.

b. Evidence and its integrity is properly preserved, collected, secured and documented consistent with the agency's chain of custody procedures.

i. Evidence is collected only by authorized personnel.

ii. Evidence is secured in a lockable location.

iii. Only the agency-appointed custodian will have access to the evidence location and will account for the custody of all keys, lock combinations or electronic key cards.

iv. As evidence is transferred, the new recipient must sign for all transfers of evidence and the transfer must be authorized and documented.

v. Evidence custodian must be cognizant of physical security measures at all times.

vi. Network security will be in effect for all electronic evidence.

c. Conclusions can be fully supported by all available evidence.

d. A full and complete review is conducted, free from contamination by outside influences.

e. Appropriate confidentiality is maintained, ensuring information is properly handled and is provided only to those with a need to know.

f. Interviews are conducted in a professional manner and will be documented during or immediately following the interview.

B. Referral to the Office of the Inspector General (OIG) for IG Investigation

Section 20.055, Florida Statutes, grants authority for investigations within each agency to the agency IG. The OIG has the authority to conduct and/or

coordinate investigative activities. CSIRT reviews which uncover policy violations, fraud or other abuses should be transferred to the OIG and CSIRT documentation will show that as the incident final disposition.

C. Referral to Law Enforcement (OIG to coordinate)

1. The OIG will determine if and when law enforcement agencies should be called during the course of an incident review.
2. The OIG will contact the appropriate law enforcement agencies and develop any required protocols before any exchange of investigative information.
3. The CSIRT leader will keep the AEIT OIS informed of any referrals to law enforcement.
4. The CSIRT leader or designated OIG representative on the CSIRT may coordinate activities with any engaged law enforcement agencies.
5. The CSIRT leader or designated OIG representative on the CSIRT will ensure the CSIRT is fully briefed on any inter-agency incidents or primary data center incidents.

3.8.8 Reporting to Agency for Enterprise Information Technology's Office of Information Security (AEIT OIS), FDLE and FWC Management

A. The CSIRT leader will report a summary of Class 1 incidents to the AEIT OIS quarterly, in the prescribed format.

B. The CSIRT leader will report all Class 2 and Class 3 incidents to the AEIT OIS within 24 hours, using the AEIT Reporting Form.

C. If the incident affects operations of the FDLE's Florida Crime Information Center (FCIC) or the federal criminal justice network (CJNet), the CSIRT leader will also notify FDLE's CJIS Information Security Officer, using the current CJIS incident reporting procedures.

D. At the conclusion of the incident, the CSIRT leader will report the team's findings to FWC management and to the AEIT OIS. At a minimum, this report should include:

1. Description of the incident
2. CSIRT members participating
3. CSIRT findings
4. Conclusions
5. Recommendations

E. After the review has concluded, all new information will be included in an amended report.

F. After the final report is delivered, the incident is closed.

3.8.9 Determination of Breach of Personal Information and Notification Requirements

If the CSIRT review determines that unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person as a result of this incident, the CSIRT will notify FWC senior management. The

CSIRT recommendations will recommend the appropriate breach notification that needs to be done and the responsible FWC Office(s) that will need to perform the breach notification.

3.8.10 Documentation and Closeout of Incident

A. As reported incidents are received by the ISM, they will be logged and numbered sequentially, using the fiscal year as a prefix. For example, the first incident in fiscal year 2010-11 will be numbered as 2010-11-001 or the third incident in 2011-12 will be numbered as 2011-12-003.

B. At a minimum, the incident reporting form and final report (including amendments) shall be maintained as documentation of the incident.

C. The log and documentation for each incident will be maintained on a confidential Information Security directory and retained according to the relevant records retention schedule.

Established: 09/2010; Revised: 6/27/2011

APPROVED

Gregory L. Holder — **June 27, 2011**

Executive Director or Designee — **Date**