CHAPTER 1

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

PURPOSE:

The purpose of this procedure is to establish the roles, responsibilities, and communication procedures for the Computer Security Incident Response Team (CSIRT) and Department employees when responding to computer security incidents which may occur within the Florida Department of Transportation (Department). The CSIRT is an objective body with the required technical and procedural skills and resources to appropriately handle computer security incidents. The CSIRT is responsible for identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to management.

AUTHORITY:

Sections 20.23(3)(a) and 334.048(3), Florida Statutes (F.S.)

SCOPE:

This procedure is applicable to all information and technology resources, at all levels of sensitivity, whether owned and operated by or operated on behalf of the Department. Additionally, consultants, outside agency workers, and volunteers shall comply with the ***Department Employee Reporting Responsibilities*** established within this procedure, and are included in any reference to employee throughout this procedure. This procedure establishes the minimum standards for Department CSIRT functions.

REFERENCES:

Section 282.318, Florida Statutes
Section 20.055, Florida Statutes
Rule Chapter 74-2, Florida Administrative Code (F.A.C.)
Security and Use of Technology Resources, Topic No. 325-060-020
Office of the Inspector General (OIG) Audit Process

1.1 DEPARTMENT EMPLOYEE RESPONSIBILITIES

In support of the Department's CSIRT efforts, employees are required to:

(1) Immediately report any breach of security, including but not limited to, unlawful accesses, suspected intrusions, theft, or other actions that compromise the security of technology resources to the FDOT Service Desk.

(2) Cooperate with the CSIRT during investigations of suspected computer security incidents by providing all requested information whether verbal or written to members of the CSIRT in a timely manner.

(3) Respond to final reports from a CSIRT investigation.

(4) Establish any additional security controls that are deemed necessary by the CSIRT as a result of a computer security incident investigation.

(5) Maintain proper security controls and adhere to security guidelines in accordance with ***Topic No. 325-060-020 Security and Use of Technology Resources***; and all other information security standards and procedures.

1.2 CSIRT ROLES AND RESPONSIBILITIES

1.2.1 Role of the CSIRT

The role of the CSIRT is to serve as the first responder to computer security incidents within the Department and to perform vital functions in identifying, mitigating, reviewing, documenting, and reporting findings to management. The CSIRT coordinates with the Chief of Transportation Technology, but is accountable directly to the Secretary.

1.2.2 Responsibilities of the CSIRT

The CSIRT will be responsible for the following activities:

(1) Classifying Department security incidents

(2) Meeting upon notification of a reported computer security incident dependent upon the incident severity level

(3) Conducting a preliminary assessment to determine the root cause, source, nature and extent of damage of the suspected computer security incident with recommended responses as deemed appropriate

(4) Selecting additional support members and subject matter experts as necessary for the reported incident

(5) Maintaining confidentiality and need to know of information related to computer security incidents

(6) Assisting with recovery efforts and providing reports to management

(7) Conduct analysis and document incidents to include findings and corrective actions."

(8) Reporting incidents to AST (Agency for State Technology) and the Cybercrime Office

(9) Maintaining awareness of, and implementing procedures for, an effective response to computer security incidents

(10) Staying current on functional and security operations for the technologies within their individual areas of responsibility

(11) Receiving annual training on cybersecurity, threats, trends, and best practices

1.2.3 CSIRT Meetings

In accordance with ***Rule 74-2.005, F.A.C.***, the CSIRT will meet at least once a quarter to facilitate its activities. Regular CSIRT meetings will be convened by the CSIRT leader and include incident trends and reviews of established processes and escalation protocols.

1.2.4 Conflicts of Interest

Incident Managers are assigned based on the process outlined in CSIRT in cases of a conflict of interest, an alternative incident manager is assigned. Incident managers will not be assigned to an incident if there is a potential for conflict of interest. In the event of a similar conflict of interest involving a core CSIRT member, the conflict must be reported to the designated CSIRT 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.

1.3 CSIRT MEMBER ROLES AND RESPONSIBILITIES

The FDOT CSIRT Core team, includes at a minimum, the Information Security Manager, the Chief of Transportation Technology (CTT), the Chief Information Officer (CIO) and and a member of the Office of Inspector General. If the CSIRT leader determines that the incident requires the additional expertise of a support member, that member will be added to the CSIRT for the duration of the incident resolution. For all Class 3 CSIRT incidents, an FDOT CSIRT Advisory team will be convened. The CSIRT Advisory team will include all CSIRT Core members and be advised by representatives, as needed, from the Office of General Counsel, Personnel Resource Management Office, and Public Information Office.

1.3.1 Role of the Information Security Manager

The Information Security Manager (ISM) will serve as the CSIRT leader. In the event that the ISM is not available during a security event, the CIO will act as the CSIRT leader or designate a CSIRT leader to serve in the interim. The CSIRT leader is responsible for managing the activities of the CSIRT.

The CSIRT leader’s duties will include the following:

(1) Contacting the Chief Information Officer

(2) Convening the CSIRT

(3) Designating CSIRT Incident Manager (CSIRT-IM)

(4) Selecting additional support members as necessary for the reported incident

(5) Managing incidents

(6) Periodically reporting status of incidents to the CIO

(7) Ensuring Class 2 and Class 3 incidents are documented

(8) Ensuring Class 2 and Class 3 incidents are reported to AST-CISO (Chief Information Security Officer)

(9) Conducting a debriefing of lessons learned and reporting to the CIO

(10) Conducting meetings of the CSIRT

(11) Ensuring meetings are documented

(12) Directing CSIRT training on an ongoing basis

(13) Coordinating CSIRT incident research and response activities

(14) Maintaining up-to-date contact information for CSIRT members

1.3.2 Role of the Chief of Transportation Technology

The ISM is responsible for all CSIRT activities and will ensure that the CSIRT operates according to the Department CSIRT procedure as well as all applicable authorities, references, and policies. All decisions relating to incident resolution are the responsibility of the Chief of Transportation Technology (CTT) or designee after conferring with the Secretary. The CTT is responsible for reporting incidents to FDOT executive management.

1.3.3 Role of the Chief Information Officer

The Chief Information Officer (CIO) is responsible for ensuring operational support is available for the resolution and remediation of incidents. This includes providing coordinated oversight between the various OIT sections, establishing priorities, and assisting in the prioritization of future work required based on lessons learned. The CIO will work closely with the CTT to detail the impact of incidents on OIT.

1.3.4 Role of the Office of the Inspector General

Chapter 20.055, F.S., tasks each agency's Inspector General with initiating, conducting, and coordinating investigations related to the programs and operations of each state agency. The Department's OIG will assign a representative to serve on the CSIRT to ensure that CSIRT reviews are properly handled and that reviews that uncover policy violations, fraud, or other abuses are transferred to the OIG for further investigation when appropriate.

The OIG representative will determine if and when law enforcement agencies should be called during the course of an incident review whenever the OIG has reasonable grounds to believe there has been a violation of criminal law. If a CSIRT incident requires the intervention of law enforcement, the OIG will contact law enforcement and develop any required protocols before exchanging investigative information. The CSIRT leader will keep the AST-CISO informed of any referrals to law enforcement and ensure CSIRT members are fully briefed on any interagency incidents. The CSIRT leader and/or designated member of OIG staff may serve as a liaison among law enforcement, AST-CISO, and the CSIRT.

1.3.5 CSIRT Incident Manager

The CSIRT Incident Manager (CSIRT-IM) will be designated by the CSIRT Leader. The criteria for designating a CSIRT-IM will be based upon the technical nature and scope of the incident. For most incidents, this will be an OIT Bureau Chief. In incidents of a highly sensitive or unique nature, the CSIRT leader and/or CIO may designate someone other than an OIT Bureau Chief as the CSIRT-IM.

1.3.6 General Roles and Responsibilities of CSIRT Members

CSIRT members must be familiar with published security guidelines available through the Department's published security policies and procedures. Each CSIRT member will serve as a subject matter expert for the area of the Department they represent. As representatives of their respective areas, each member will ensure that all policies and procedures as well as state and federal laws that apply to their specific area of responsibility are being adhered to during the implementation of this CSIRT procedure. Each CSIRT member should have an awareness of the duties of the other CSIRT members.

Each CSIRT member must also be available (or have a designee available) to respond to security incidents during business and non-business hours in order to mitigate possible incidents and react swiftly to minimize damage to critical infrastructure, computer system(s), networks, and data.

1.4 COMPUTER SECURITY INCIDENT CLASSIFICATIONS

The CSIRT will classify each incident as a Criticality 0, Criticality 1, Criticality 2, or Criticality 3 incident based upon risk-based severity. These classifications allow for consistency for reporting and tracking purposes. If an incident meets several criteria in different rating categories, the incident will be defined based on the highest rating. Criticality 0 are deemed to be observable events that are worth being documented with the understanding they may possibly become incidents.

Examples include but are not limited to anti-malware protection that prevents infection, and an Intrusion Prevention System (IPS) that drops inbound traffic.
The following criteria will be used to determine incident classification:

Criteria	Class 1 – Low/Minimal	Class 2 - Medium	Class 3 – High/Critical
Account Compromise	A single user account is compromised by the same threat source.	More than one user account is compromised by the same threat source.	A user account that deals with personal or confidential information has been compromised with confirmed data loss or exposure.
Breach	Unauthorized disclosure of confidential information has not occurred.	Unauthorized disclosure of confidential information has not been determined.	Unauthorized disclosure of confidential information has occurred.
Business Impact	Incident does not involve mission critical services.	Incident involves mission critical services.	Threat to other Department information technology resources is high.
DoS/DDoS/TDoS	Affected resource(s) is not considered mission critical.	Affected resource(s) has a moderate impact to production.	Affected resource(s) has a severe impact to production.
Loss	Lost hardware that has low monetary value or is not part of a mission critical system.	Lost hardware with high monetary value or that is part of a mission critical system.	Incident investigation and response is transferred to law enforcement.
Malicious Code/Malware	A single endpoint is infected.	Several endpoints are infected.	Widespread infection actively impacting multiple departments or districts.
Misconfiguration	Misconfigured access controls that have minimal impact on resources.	Misconfigured access controls have moderate impact on resources.	Misconfigured access controls have severe impact on resources.
Misuse	Misuse has minimal impact on resources.	Misuse has moderate impact on resources.	Misuse has severe impact on resources.
New/Zero-Day	Minimal impact on resources to the extent of knowledge.	Moderate impact on resources to the extent of knowledge.	Severe impact on resources to the extent of knowledge.
Phishing/Social Engineering	User or resource is affected that does not deal with personal or confidential information.	User or resource is affected and there is the potential for compromise of personal or	User or resource is affected and there is confirmation that personal or confidential information is

Criteria	Class 1 – Low/Minimal	Class 2 - Medium	Class 3 – High/Critical
		confidential information.	compromised.
Policy Violation	Security policy violations determined by the Department that have the potential for minimal impact.	Security policy violations determined by the Department that have the potential to have moderate impact.	Security policy violations determined by the Department that reach the level of requiring a criminal investigation.
Public Interest	Low potential for public interest.	There is the potential for public interest.	There is active public interest in the incident.
Ransomware	Resource is infected but was prevented from spreading.	Resource is infected and spread to a minimal amount of other resources.	Resource is infected and has a severe impact on mission critical resources.
Scan/Probe	Reconnaissance attempts have minimal impact on resources.	Reconnaissance attempts remain consistent.	Reconnaissance attempts are preceded by an attack.
Service Disruption	Incident is within a single business unit.	Incident affects multiple business units within the Department.	Disruption is wide spread across the Department and/or other agencies.
Theft	Stolen hardware that has low monetary value or is not part of a mission critical system.	Stolen hardware with high monetary value or that is part of a mission critical system.	Incident investigation and response is transferred to law enforcement.
Threat Potential	Threat to other information technology resources is minimal.	Threat to other Department information technology resources is possible.	Incident has potential to become widespread across the Department and/or threatens external, third-party information technology resources.
Unauthorized Access	Unapproved access that has not caused damage to resources.	Unapproved access that has caused moderate damage to resources.	Unapproved access that has damaged mission critical resources.

1.4.4 Incident Reclassification

An incident may be escalated or downgraded by any of the following actions:

(1) Decision of the CSIRT leader or designee

(2) Decision of the CTT, CIO, ISM, or IG

(3) Request by Executive Management or the Department's Secretary

(4) Escalation of the magnitude of the event

The reason for the escalation or downgrade must be documented as part of the process.

1.4.5 CSIRT Activation

Activating the CSIRT will be dependent upon the classification of the incident. Activating the CSIRT occurs when members of the team work together by sharing information, steps have already been taken, and previous recommendations for remediation and recovery have been made.

Class	Response	Activate CSIRT?
0	Observable event but not considered an incident at the time.	No
1	Minimal impact to resources	No
2	Moderate impact to resources	Advise
3	Severe impact to resources	Yes

1.4.6 Incident Reporting Timeframes Process

The security incident reporting process must include notification procedures for timely reporting to the AST and Cybercrime Office as established in 943.0415, F.S. The following timeframes shall be followed:

FCS Rating	Initial Notification	Definition of Effect Rating
Minimal	Monthly aggregate	Effect on IT resources managed by internal processes
Low	Weekly	Minimal effect on IT resources
Medium	One business day	Moderate effect on IT resources
High	Within 4 hours	Severe effect on IT resources or delivery of services
Critical	Immediately	Severe effect on IT resources, believed to impact multiple agencies

		or delivery of services

Incident reports will include the following:

(1) Executive summary

(2) Description of the incident

(3) CSIRT members participating

(4) CSIRT findings

(5) Conclusions

(6) Recommendations

After the conclusion of the computer security incident review, any and all new information relevant to the computer security incident must be documented in an amended final report.

1.5 INCIDENT REVIEW PROCESS

Class 2 and Class 3 incidents must involve a review process that is appropriate to the incident, thoroughly documented, and consistent with the Department's review procedures. All members of the CSIRT will document their actions thoroughly and retain copies of their documentation for future use.

1.5.1 Methodologies

The CSIRT will use current best practices in reviews. These practices are intended to ensure the following:

(1) CSIRT reviews are preserved to the extent dictated by the current Department policies and pertinent laws, rules and regulations.

(2) Evidence and its integrity is properly preserved, collected, secured, and documented consistent with the chain of custody requirements as directed by the OIG.

(3) Conclusions can be fully supported by all available evidence.

(4) A full and complete review is conducted, free from contamination and from outside influence.

(5) Appropriate confidentiality is maintained; ensuring information is properly handled and is provided only to those authorized.

1.5.2 Evidence Collection

1.5.2.1 Interviews

The CSIRT must conduct all interviews in a professional manner and document the findings during or immediately after the interview.

1.5.2.2 Evidence

Authorized personnel will collect and preserve evidence and its integrity according to Department procedures and will ensure the appropriate chain of custody. All physical evidence must be secured in a lockable location and all electronic evidence must be secured by appropriate network security. Only the Department-appointed custodian(s) of the evidence will have access to the evidence location, and they will account for the custody of all keys, lock combinations or electronic key cards. All transfers of evidence must be authorized, thoroughly documented and signed for. The evidence custodian(s) must be aware of location and physical security of evidence at all times.

1.6 INCIDENT RESOLUTION

The incident will be closed once the CSIRT delivers the final report to the appropriate parties, including the Department’s Secretary and AST-CISO.

TRAINING:

None.

FORMS:

None.