FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Computer Security Incident Response Team (CSIRT) Procedures

Related Policy: FDJJ – 1250

I. DEFINITIONS

Breach – A confirmed event that compromises the confidentiality, integrity, or availability of information or data.

Chief of Information Technology (IT) – DJJ staff responsible for overseeing the Bureau of Information Technology within DJJ, also referred to as the Chief Information Officer (CIO).

Computer Security Incident – Any event resulting in the Department's computer systems, networks or data being viewed, manipulated, damaged, destroyed, or made inaccessible by an unauthorized activity. See the **Severity Level** definitions for specific information incident classifications.

Confidential Information and/or Confidential Data – Information and/or data exempted from disclosure requirements under the provisions of applicable state and federal law, and includes ensuring information and/or data is accessible only to those authorized to have access.

Confidentiality – The principle that information is accessible only to those authorized.

Contract/Grant Manager – DJJ staff responsible for contract or grant management, including adherence to the guidelines identified in the CSIRT policy and procedures by reporting known computer security incidents involving DJJ's data and/or information technology resources.

Data Integrity Officer (DIO) – DJJ staff responsible for assisting information technology resource users, maintaining the integrity of the data within the Juvenile Justice Information System (JJIS), creating JJIS user accounts, and assisting with conducting JJIS training. This includes following the guidelines identified in the CSIRT policy and procedures for reporting known computer security incidents involving DJJ's data and/or information technology resources.

Denial of Service (DoS) – An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

Department-Approved Software – Software reviewed and deemed acceptable by the Department of Juvenile Justice's (DJJ) Bureau of Information Technology (IT)for use with its information technology resources.

Department-Managed Device – A device not owned by the Department, but for which the Department ensures the hardware and software used are in compliance with Department standards.

Event – An observable occurrence in a system or network.

Incident – A violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing a specific incident is about to occur.

Information Security Manager (ISM) – The person designated to administer the DJJ's information resource security program and plans in accordance with section 282.318(2)(a)1, Florida Statutes, and the Department's internal and external point of contact for all information security matters.

Malicious Code – A virus, worm, Trojan horse, or other code-based entity that infects a host.

Malware – Malicious software.

Provider – Any non-DJJ entity that provides a service for youth under the care of the Department.

Scans and Probes – Unauthorized and/or repeated probes (also referred to as service and port scans). This includes Scans and Probes that are persistent, significant, and/or attempt to avoid detection.

Severity Levels – The CSIRT classifies computer security incidents based on four levels of severity (.i.e. Level 3, Level 2, Level 1, and Level 0.

a. Severity Level 3 (High)- Successful penetration or denial of service attacks detected with significant impact on operations. Widespread instances of a new computer virus not handled by anti-virus software. This severity should be used if significant risk of negative financial or public relations impact may result.

- Significant and immediate threat to human safety.
- Significant adverse impact on a large number of systems and/or people.
- Potential large financial risk or legal liability to the agency.
- Loss of confidential and/or sensitive data (Data Breach).
- Adverse impact on a critical enterprise system or service.
- High probability of propagating to a large number of other systems and causing significant disruption.

b. Severity Level 2 (Medium)- Moderate to significant numbers of system probes detected, penetration, or denial of service attack attempts with limited impact on operations, or larger instances of known computer viruses that can be handled by anti-virus software. This severity may also include isolated instances of a new computer virus not handled by anti-virus software.

- Adverse impact on a moderate number of systems and/or people.

- Adverse impact on a non-critical enterprise system or service.
- Adverse impact on a sub-departmental scale system or service.
- Disruption of a building or departmental network segment.
- Moderate risk of propagating and causing further disruption.
- Lost or stolen device where loss of sensitive data is unknown.

c. Severity Level 1 (Low)- Small numbers of system probes detected on internal systems or an isolated virus that can be handled by anti-virus software.

- Adverse impact on a very small number of non-critical individual systems, services, or people.
- Disruption of a very small number of network devices or segments.
- Little risk of propagation and further disruption.
- Isolated incidents involving minor issues with individual users or non-critical systems.
- Individual lost or stolen devices not containing sensitive data.

d. Severity Level 0 (Negligible)- Events that may or may not be considered "security incidents" based on the individual agency policy but may be indicative of a security issue. This information will be potentially useful in establishing intelligence related to a baseline of normal activity and facilitating the identification of abnormal behavior

State Office of Information Security (OIS) – The State of Florida information security office that guides, coordinates, and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities so that effective security controls can be implemented.

Theft or Loss of Confidential Data – Confidential information pertaining to youth under the care of the Department, personal health in terms of HIPPA security rules and reporting procedures, data and personally identifiable information in terms of Section 817.5681 Florida Statues.

Theft or Loss of Information Technology Devices and Resources – Information Technology Devices and/or Resources including those outlined in the Department's Mobile Device Policy (FDJJ 1230) that are stolen or lost, or are known to contain sensitive data or are utilized by DJJ to hold sensitive data.

Threat – Any circumstance or event that has the potential to adversely impact a state agency's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

Unauthorized Access – Attempts (either successful or failed) to gain unauthorized access to (or use of) a system or its data especially when the data files and information are considered sensitive or confidential.

II. STANDARDS/PROCEDURES

A. Composition of CSIRT:

1. The CSIRT shall be comprised of three core members: an individual from the Office Inspector General (OIG), the Department's Information Security Manager (ISM), and the Chief Information Officer (CIO).

2. The ISM shall act as the Team Leader with management responsibility for the activities of the CSIRT, except the authority to conduct an investigation.

3. In addition to the three core team members, staff from the following areas shall be included as needed: Office of General Counsel, Office of Public Information, Bureaus of Personnel, Finance & Accounting, and Information Technology functional specialists.

4. Team support members shall not be full-time members of CSIRT, but shall be added to the team for the duration and resolution of a specific incident when the Team Leader determines that an incident requires their expertise.

B. Computer Security Incident Reporting:

1. All DJJ employees and provider staff having access to Department equipment and information systems shall report all computer security incidents to the ISM.

2. For computer security incidents requiring termination of access to Department information systems (employees or provider staff), IT staff and/or DIOs shall assist in that process.

3. The escalation and the reason for the escalation by CSIRT must be documented as part of the process. An incident may be escalated from a Severity Level 1, to a Severity Level 2 incident in any of the following ways:

   a. Decision of the CSIRT Team Leader or designee;
   b. Determination of the CIO, ISM, or OIG;
   c. Additional related events (i.e. emergence of a distributed, coordinated attack as an example); and
   d. Request by Executive Management or Department Secretary.

C. Investigative Process:

1. Section 20.055, Florida Statutes, grants authority for investigations of each Department to the Office of the Inspector General (OIG). The Inspector General has the authority to conduct and/or coordinate investigative activities and may, at his/her discretion, refer or assign the actual conduct of an investigation to the CSIRT. The OIG, in this case, will continue to supervise, coordinate, and direct the investigation.

Note: The IG has the authority under Section 20.055, Florida Statutes, to conduct any and all investigations independent of the CSIRT process, where such investigations are deemed necessary by the OIG.

2. In all CSIRT-delegated investigations, a formal investigative process shall be used, appropriate to the incident, consistent with each Department's investigative procedures and documented following Department's guidelines.

3. All members of the CSIRT investigating team shall document their actions thoroughly, retain a copy of their notes for future use (i.e., as an expert witness in resulting litigation or criminal proceeding), and submit a copy to the team for use in preparing the final report.

4. The Office of the Inspector General (OIG) will be in charge of all investigations, and will retain all records, notes, and reports for the investigative process in accordance with Department records retention schedules.

5. CSIRT members may only assist in the investigation of an incident at the direction of the OIG.

D. Report Process:

1. All Severity Level 2 and Severity Level 3 incidents must be reported to the OIG for the initial review, and to the OIS, in a format defined and required by OIS.

2. The CSIRT is responsible for reporting their findings to executive leadership, including the CIO, at the conclusion of an incident. This report shall include the following:

   a. **Executive Summary** – Include a description of the incident, methods of investigation and general conclusions.

   b. **Detailed Conclusions** – Include one section for each conclusion drawn by the CSIRT. These sections describe how the CSIRT arrived at the conclusion, lists exculpatory evidence that may prove contradictory, and evidence that supports the conclusion. Log entries can show a chain of events that support the CSIRT's conclusion.

   c. **Recommendations** – The report should conclude with the CSIRT's recommendations for avoidance of future or repeat incidents.

E. Continuity of Operations Plan (COOP):

1. Incident handling by the Department's CSIRT is closely related to COOP planning as well as support and operations. The Department's CSIRT may be viewed as a component of contingency planning because it provides the ability to react quickly and efficiently to disruptions in normal processing.

F. Violations:

1. Violations of this policy or any of the Department's Information Technology Resource policies or procedures may result in the revocation of access/permissions, disciplinary action up to and

including immediate dismissal, and/or potential criminal prosecution under Chapter 815, Florida Statutes, or other applicable federal, state or local laws or policies.

III. RESPONSIBILITY AND DUTIES

A. Responsibilities of the CSIRT:

1. Report incidents to the OIS.
2. Convene as required upon notification of a reported computer security incident.
3. Respond to activities that might interrupt the IT services of the area for which the team is responsible during duty and non-duty hours.
4. Assist with recovery efforts, document incidents, and provide regular reports to the CIO.
5. Classify Department security incidents.
6. Maintain awareness of and implement procedures for effective response to computer security incidents.
7. Stay current on functional and security operations for the technologies within their area of responsibility.
8. Follow the direction of the CIO**,** or designee**,** during incident response activities.
9. Maintain confidentiality of information related to computer security incidents.
10. Select additional support members as necessary for the reported incident.

B. Duties of the CSIRT:

1. Conduct a preliminary assessment of a security incident to determine the root cause, source, nature, extent of damage, and recommended response.
2. Manage the release of information to the media in coordination with the Department's Communication Office.
3. Prepare a report of findings, root causes, lessons learned, and recommended actions for executive leadership review.
4. Carry out the directions of management as communicated through the CIO.

Note: The Department's CSIRT does not make policy decisions or take action following an investigation. The CSIRT receives its direction from the Department's CIO, but is accountable directly to the Department Secretary in consultation with the OIS. In addition, all investigative activities will be performed by or at the direction of the Department's OIG.

C. Information Security Manager (ISM)/CSIRT Team Leader:

1. Convene the CSIRT.
2. Contact with the CIO.
3. Conduct meetings of the CSIRT.
4. Report periodically status of incidents to the CIO.
5. Manage Severity 1/0 incidents.
6. Ensure all Severity Level 2 and Severity Level 3 incidents and applicable information are reported to the (OIS).
7. Coordinate non-investigative team activities.
8. Compile the final report and recommendations of the CSIRT regarding specific incidents.

D. Office of Inspector General:

1. Convene investigations.
2. Ensure investigative procedures are followed using the guidelines outlined by Section 20.055, Florida Statutes.

E. Office of General Counsel:

1. Provide legal advice to the Department as appropriate.

F. Platform Specialists (Network Security):

1. Network Security representative shall contain the incident locale as appropriate.
2. Respond to all activities that might interrupt any critical information technology services owned and managed by the Department. This includes those systems both inside and outside the Department's firewall (e.g., Web Servers, Routers, all regional field office servers).
3. Review tracking logs and report any unusual or suspicious activities.
4. Report any unusual behaviors of the critical systems.
5. Be prepared to brief the CSIRT on operations procedures.
6. Protect evidence of incident according to the Department' guidelines and instructions from the core team.
7. Assess and report damage to computer system and/or data to CSIRT.
8. Aid in the determining the scope of an intrusion.

9. Assist in identifying the point of access or the source of the intrusion.
10. Make recommendations to close the source or point of access of the intrusion.

G. Finance & Accounting:

1. Brief the team on financial procedures as needed.
2. Conduct financial reviews (i.e. financial losses from theft) as requested.
3. Report findings to the CSIRT.

H. Personnel:

1. Advise the CSIRT core members on personnel policies and procedures.
2. Make recommendations for handling sensitive employee information.

I. Communication Office:

1. Act as a single point of contact for the media.
2. Review any press releases before they are distributed to the media.
3. Obtain legal advice before any interview or press release is given to the media.
4. Obtain approval from the OIG that interviews or press releases will not interfere with investigations.
5. Inform all other affected users to refer any media inquiries to the Communication Office

J. Contract/Grant Manager:

1. Shall report any known computer security incidents involving providers and DJJ's data and/or information technology resources to the Department's ISM.

K. Data Integrity Officer (DIO):

1. Shall report any known computer security incidents involving providers and DJJ's data and/or information technology resources to the Department's ISM.

IV. ATTACHMENTS: N/A