FLORIDA DEPARTMENT OF JUVENILE JUSTICE POLICY

Secretary /s/, Christina K. Daly **Date:** 5/1/2017

Subject: Computer Security Incident Response Team (CSIRT)

Section: FDJJ – 1250

Originating Office: Administrative Services

Authority: Section 282.318, Florida Statutes – Security of Data and Information Technology Resources Government Information Security Reform Act (PUBLIC LAW 106–398, APPENDIX 114 STAT. 1654A–269)

Related References: Florida Office of Information Security – Agency for Enterprise Information Technology, Computer Security Incident Response Team Agency Guidelines;
Florida Administrative Code, Rule 74-2, Florida Information Resource Security Policies and Standards;
FDJJ 1205.30 - Information Resource Security Standards & Guidelines;
FDJJ 1225 - User Password Policy; and
FDJJ 1230, Mobile Devices Policy

Purpose: This policy establishes guidelines for the Florida Department of Juvenile Justice's Computer Security Incident Response Team (CSIRT) for the purpose of reporting, responding to, mitigating, and documenting computer security incidents, which occur within this agency and applicable providers.

Offices Affected by the Policy: All offices within the Florida Department of Juvenile Justice (DJJ) and applicable service providers.

POLICY STATEMENT:

- The Governor's Information Technology Security Initiative requires each state agency to establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents by identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to agency management. This policy establishes the CSIRT for the Department.
- Pursuant to Chapter 282.318(4)(d), Florida Statutes, all State of Florida agencies shall report network security incidents, including data breaches, to the applicable governing agency or agencies.
- All state of Florida agencies shall follow the severity and reporting guidelines set by the applicable governing agency or agencies.

- The Department's CSIRT shall establish roles, responsibilities and communication procedures for the purpose of reporting, responding to, mitigating, and documenting computer security incidents, which includes but is not limited to the identification, classification, and notification of computer security incidents.

- CSIRT membership shall include an individual from the Office of Inspector General (OIG), the Department's Information Security Manager (ISM), the Chief Information Officer (CIO), the Office of General Counsel, the Office of Public Information, the Bureaus of Personnel, Finance & Accounting, and a Data Integrity Officer (DIO).

- All Department employees and applicable providers shall report suspected computer security incidents (as referenced in the CSIRT Procedures document) to the agency's ISM, who will disseminate that information to the CIO, OIG, and other governing agencies as applicable.

PROCEDURES/MANUALS:

Procedures for this policy are accessible at the Department Policies internet page:
http://www.djj.state.fl.us/partners/policies-resources/department-policies/by-office