FLORIDA DEPARTMENT OF JUVENILE JUSTICE POLICY

Secretary /s/ Christina K. Daly **Date:** 6/12/2017

Subject: Utilization of Information Technology Access Privileges and Resources

Section: FDJJ 1235

Originating Office: Administrative Services

Authority: Florida Administrative Code, Rule 71A-1 (Information Resource Security Policies and Standards)

Related References: Network User Accounts (FDJJ 1205.50)

Purpose: This policy establishes standards for the utilization of the Department's Information Technology (IT) resources and access privileges to guard against unauthorized use and abuse. Nothing in this policy shall be construed as limiting the access of the Auditor General to Departmental records, systems, or networks in the performance of a properly authorized audit or examination pursuant to Chapters 11 and 119, Florida Statutes. Nothing in this policy shall be construed to impair the public's access rights under Article I, Section 24 of the Florida Constitution, and Chapter 119, Florida Statutes.

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

- **POLICY STATEMENT:** Information Technology (IT) staff are assigned administrative privileges in order to do their jobs. These privileges shall only be used in the performance of assigned duties.
- Suspected or known IT misuse or computer incidents shall be reported to the Chief Information Officer, Information Security Manager, and the Central Communications Center (CCC) as an incident.
- IT staff shall not conduct independent investigations and shall only assist in investigations at the request the Office of Inspector General in conjunction with a reported incident, or as directed and approved by Executive Level Leadership, the Office of General Counsel, or the Chief Information Officer.

Note: 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 at his/her discretion.

- Access to DJJ IT resources is available to assist employees and provider staff in the performance of their assigned and authorized duties. This policy strictly prohibits employees and provider staff from using their authorized access to perform tasks outside of their assigned duties. This includes but is not limited to:
  - Unauthorized creation and use of network and/or E-mail accounts; including forging or spoofing E-mail headers and the distribution of malware;
  - Unauthorized access, viewing, deletion, modification, and/or disclosure of E-mail messages, files, records, materials, and/or data, including employee records, medical information, or juvenile data;
  - Compromising servers, computers, or any IT related resources for unauthorized use;
  - Altering and/or circumventing established protocols, procedures, and security practices for personal, unauthorized and/or non work-related use; and
  - Altering the authorized configuration of DJJ computers without the written consent of the Chief Information Officer.
  - No privately owned devices shall be connected to state-owned systems without the written consent of the Chief Information Officer.
- All Department employees and provider staff are responsible for maintaining system security and integrity, to the extent of his/her assigned duties.
- All Department employees and provider staff shall immediately report any known or suspected instances of misuse and abuse of IT access and/or resources to the Chief Information Officer.
- All Department employees and provider staff shall use IT resources and access privileges in the performance of their assigned and authorized duties in support of DJJ and/or State of Florida business.
- All Department employees and provider staff are prohibited from using their access privileges or the Department's resources to access, disclose, or transmit material deemed to be in violation of any federal, state, or local law or rule, or Department policy.
- All Department employees are granted access to IT resources based on the principles of "least privilege" and "need to know." Reference FDJJ 1205.30, Information Resource Security Handbook, Section X. Glossary of Terms for a detailed definition.
- Non-IT employees of the Department are prohibited from modifying (i.e., adding, removing, changing) the security privileges of file folders on the DJJ Network without prior written approval from his/her manager.
- The altering of the standard authorized configuration of DJJ computers without prior approval is prohibited. Non-Standard software can only be installed on DJJ computers with prior approval from the Chief Information Officer.
- Administrative privileges shall be requested in writing and approved by the Chief Information Officer before privileges are granted.
- Administrative privileges shall only be granted when needed to perform specific duties which cannot be done by any other access type.

- The use and activities of those with elevated administrative privileges shall be reviewed periodically and audited by the Chief Information Officer (or designee) to ensure said privileges used in accordance with assigned duties and responsibilities.
- Violation of any provision of this policy is cause for disciplinary action, up to and including dismissal.

PROCEDURES/MANUALS: N/A