FLORIDA DEPARTMENT OF JUVENILE JUSTICE POLICY

Secretary: /s/, Simone Marstiller **Date:** 04/26/2019

Subject: Network & Infrastructure Security

Section: FDJJ – 1240.10

Originating Office: Administrative Services

Authority: Section 282.318, Florida Statutes

Related References: Florida Administrative Code (FAC) 74-2
Network User Accounts (FDJJ 1205.50)
Utilization of Information Technology Access Permissions and Resources (FDJJ 1235)
Computer Security Incident Response Team (C-SIRT) (FDJJ 1250)
Central Communications Center (FDJJ 8000)

Purpose: This policy establishes guidelines for evaluating and enforcing compliance with security policies, procedures and standards. The Department of Juvenile Justice shall monitor, control, and protect data, network infrastructure and information technology (IT) resources by using secure software development and system engineering principles.

Offices Affected by the Policy: All offices within the Department of Juvenile Justice and all Department-approved and applicable providers.

POLICY STATEMENT:

DJJ's information technology network and server infrastructure is critical to the Department's mission. When the technology infrastructure is unavailable, critical services cannot be performed. All IT employees and persons accessing DJJ networks or applications must comply with federal and state law and rules in their operation and use of DJJ IT systems or equipment. Appropriate security controls must be in place to support a standard process for reporting, responding to, mitigating, and documenting computer security incidents. To carry out the Department's mission, the technology resources including hardware, software, networks, and data must be protected. Data and resources must be reliable and must be available to those employees and agency providers who have permission to use them. This security of information resources and protection from unauthorized access or improper disclosures are needed to ensure successful DJJ operations. All employees are responsible for protecting the information resources of DJJ.

PROCEDURES/MANUALS:

Network diagram(s) available upon request.

I. Network Access & Privileges

Objective: The Department's network shall be designed, at minimum, to require the following Information System principles:

a. All Department computer users shall have unique user accounts.

b. User accounts must be authenticated at a minimum by a password.

c. Password length of eight (8) or more alphanumeric characters must be specified and implemented on all network user accounts.

d. Password expiration must be set on network accounts. Any exceptions must be approved by the Department's Chief Information Officer.

e. Password-protected screensavers with the automatic activation feature shall be set at fifteen (15) minutes, by the Group Policy Option (GPO) in Active Directory.

f. The agency must ensure accounts with administrative rights are created, maintained, monitored, and removed in a manner that protects IT resources.

g. Administrative account activities shall be traceable to an individual.

h. Service accounts shall be created and used solely for specified services on the network. A service account shall not be used to gain individual access to any service or resource on the network.

i. Access to IT resources shall be granted based on the principles of "least privilege" and "need to know."

j. Only Department-approved software shall be installed on agency computers.

k. The Department shall use software and hardware tools and devices to monitor and protect the integrity of the Department's data and technological infrastructure from known vulnerabilities and unauthorized access (e.g. utilizing a firewall and malware protection tools, along with monitoring, sniffing, and scanning the Department's network).

l. The Department shall implement controls to ensure access to IT infrastructure resources is restricted to authorized users and uses.

m. The Bureau of Information Technology shall ensure separation of duties so that no individual has the ability to control an entire process.

n. The application development team shall implement appropriate security controls when developing applications.

o. The Department shall implement and follow procedures to establish accountability when accessing and/or modifying confidential applications and data.

p. The Department shall monitor for unauthorized access points. Unauthorized access points connected to the Department's network must be removed immediately. The discovery of unauthorized access points shall be reported to the Department's Information Security Manager.

q. Department IT resources shall not be used for personal profit, benefit, or gain.

r. Personal use of the Department's IT resources shall not violate any aspects of this or other applicable DJJ policies or local, state, and federal laws.

s. When authorized by the applicable retention schedule, confidential information, regardless of media type, will be destroyed.

II. NETWORK SECURITY

Objective: To establish secure data transfer among users, hosts, applications, and intermediate and distributed processing facilities.

1. Network Controls – General:

a. Network components shall not be implemented without proper security configuration.

b. Network resources participating in the access of sensitive information shall assume the sensitivity level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

c. All network components under state control must be identifiable and restricted to their intended use.

d. Patches and security updates must be applied in a timely fashion in accordance with [Department] patch management procedures. Logs must be kept documenting the patches and updates that have been installed on each device, including, at minimum, the name of the device, the name of the patch, the version of the patch, and the date of installation.

2. Security at Network Entry and Host Entry:

a. Owners of information resources served by networks shall prescribe sufficient controls to ensure access to network services, host services and subsystems is restricted to authorized users and uses only.

b. Authorization at network entry based on a valid user identification code and authentication (e.g., password) shall be provided under the framework of network services and controlled by the network management program.

3. Security at the Application:

a. Network access to an application containing critical or sensitive data, and data sharing between applications, shall be as authorized by the application owners and shall require user authentication validation.

b. The Department shall implement procedures to establish accountability for accessing and/or modifying confidential data and applications.

c. Application security shall be addressed throughout the application procurement process and/or application development lifecycle.

d. The application maintenance process shall include reviews of application security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

e. The application development team shall implement appropriate security measures and controls to minimize risks to the Department's IT resources, and to achieve the security requirements of the application owner.

f. Application security documentation shall be maintained by the Department and be available to the Information Security Manager.