I. POLICY:

The Office of Information Technology shall oversee the use of information technology resources to ensure the use of resources is in support of the Department’s mission and guide the organization strategically with respect to use, operation, and implementation of technology following industry standards of practice.

II. DEFINITIONS:

Information Technology Resources: Desktop, laptop, and handheld computers and tablets, jump/flash drives used on Department computers, printers, scanners, data networks and servers, internet, e-mail, numerous applications including but not limited to mobile platforms and software programs, cellular telephones, Guard Plus, DJJ agency website, wireless and electronic and video communications devices and CCTV.

Items not considered an Information Technology Resource: Two-Way radios, CCTV systems not connected to a network switch. Cable TV distribution systems, LCD panels not connected to a network switch, facility access control systems, and facility automation controls.

Information Security Officer (ISO): Person responsible for security compliance, audits, and overall program development.

Technology Committee: Committee made up of select technology savvy individuals in the agency to participate in the technology governance, planning, and technology operation processes.

III. PROCEDURES:

A. The Director of the Office of Technology and Information Services (OTIS) will serve as the Chief Information Officer for the Department and will be represented with other agencies as the Chief Information Officer (CIO).
B. The IT Director will establish standards and procedures governing all information technology (IT) resources deployed within DJJ, including determination of the types and models of resources that will be deployed and the manner in which they will be configured.

C. The IT Director must approve all IT resources used by DJJ. Those resources must be acquired in accordance with approved Georgia Technology Authority (GTA), approved State Purchasing procedures, and OTIS procurement procedures. All IT resources will be configured in accordance with established standards and installed by OTIS and/or persons approved by the IT Director or designee.

D. DJJ under direction of the IT Director may remove, replace, or reconfigure its IT resources without notice to the user, provided that the procedures set forth by the IT Director are followed. Absent a specific procedure, changes may be made with the approval of the IT Director.

E. With the approval of an Assistant Commissioner or respective Deputy Commissioner, the IT Director may direct the monitoring of all digital transmissions to and from the internet, including e-mail and text messages, internal network communications, or any other outside network. DJJ may examine all of its system configurations, as well as the files on those systems, to protect its resources from virus infections, unauthorized access, misuse, to respond to complaints of abuse (e.g., harassment), or to maintain data integrity. No monitoring can be accomplished without prior approval.

F. Wholesale monitoring is not approved by anyone within DJJ. All activity monitoring must be accomplished only on specific named individuals.

G. The IT Director will ensure that Information Security Procedures are properly maintained in a reasonable manner. They shall also be applicable to provide for the confidentiality, availability, and integrity of information assets. Policies shall be modified to incorporate relevant industry standards including compliance with Federal and State Security Policy and Procedures.

H. The IT Director shall be responsible for all IT, security, and communications related policies in coordination with the agency Technology Committee. This shall include remaining current with national technology standards and versioning.

I. The ISO is responsible for adherence to all security and compliance requirements with GTA security policy. The ISO shall coordinate such actions with GTA and the state ISO.

J. The Strategic Technology Plan and related plans will be the responsibility of the IT Director with coordination with the agency Technology Committee.

IV. LOCAL OPERATING PROCEDURES REQUIRED: NO