

<p align="center">GEORGIA DEPARTMENT OF JUVENILE JUSTICE</p>	<p align="center">Transmittal # 17-14</p>	<p align="center">Policy #: 6.8</p>
<p>Applicability {x} All DJJ Staff { } Administration { } Community Services { } Secure Facilities (RYDCs and YDCs)</p>	<p>Related Standards & References: Georgia Technology Authority Policies, Standards and Guidelines</p>	
<p>Chapter 6: INFORMATION TECHNOLOGY</p>	<p>Effective Date: 12/15/17 Scheduled Review Date: 12/15/18 New Policy Administrative Services Division</p>	
<p>Subject: IT SECURITY</p>	<p>APPROVED:</p>  <hr/> <p>Avery D. Niles , Commissioner</p>	
<p>Attachments:</p> <p>A – IT Publications and Standards</p>		

I. POLICY:

Department of Juvenile Justice information technology (IT) resources shall implement a risk based approach to properly secure the enterprise. Each user of IT resources shall be properly trained/educated through a comprehensive Security Awareness Program focused on efficiency, productivity, and guidelines designed to safeguard the agency from vulnerabilities and threats. This policy applies to any resource or area which potentially handles or houses data.

II. DEFINITIONS:

Data Breach: A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Data Loss: The term “lost” does not apply to the loss of data on a hard drive rather it implies the data.

IT DIRECTOR: Director of the Office of Technology and Information Services responsible for technology and security policies as well as it security and technology strategy.

ISO: Department Internet Security Officer responsible for security compliance, audits, and overall program development.

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

IT Security Team: A team comprised of the ISO, IT Director, Assistant IT Director, Chief Application Architect, and the Assistant Deputy Commissioner of Administrative Services.

CHAPTER	Subject	Policy #	Page
INFORMATION TECHNOLOGY	IT SECURITY	6.8	2 of 5

Items not considered an Information Technology Resource: Cable TV distribution systems, LCD panels not connected to a network switch, facility access control systems, and facility automation controls so long as they do not contain a protected class of data.

RFS: Request for Service from GTA\CapGemeni via the BMC Software System known as Remedy.

Security Incident: A violation (breach) or imminent threat of violation of computer security policies.

Security Event: Questionable or suspicious activities that could threaten the security objectives for critical or sensitive data or infrastructure. They may or may not have criminal implications.

Security Class Event: Those events which are considered events under the security umbrella (e.g., denial of service attacks, data theft, or leakage).

Security Breach: An incident that results in unauthorized access to data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

Technology Committee: The Information Technology Committee (ITC) serves as an oversight committee on matters of information technology, information technology security and is responsible for setting the information technology strategic direction of the organization. The committee reviews and recommends department information technology policies and procedures; participates in development of the Strategic Technology Plan; reviews and recommends priorities for the development of applications and for technology requests; and serves as an information-sharing forum. The committee is an advisory to the Executive Committee concerning Instructional and Information Technology direction for the department.

Work Order (WO): Work order within the DJJ Work Order Request System.

III. PUBLICATIONS:

- A. The GEORGIA.GOV standards are included in the Information Security Guide for State of Georgia Government Executives located:

http://portal.georgia.gov/data-sharing-services/sites/portal.georgia.gov.data-sharing-services/files/related_files/site_page/info_sec_guide_for_state_execs.pdf

- B. The national publications and standards, GTA standards, and GTA publications are listed in IT Publications and Standards (Attachment A).

IV. PROCEDURES:

- A. The Georgia Technology Authority (GTA) policies shall be followed unless exemptions have been approved by GTA. Those exemptions shall be approved by the Technology Committee after a review by the ISO.

CHAPTER	Subject	Policy #	Page
INFORMATION TECHNOLOGY	IT SECURITY	6.8	3 of 5

- B. Any additions to GTA policies shall be referenced in an additive policy and referenced within this policy. All subsequent IT Security policies shall be referenced/indexed within this policy as a subordinate to this policy.
- C. National Standards such as NIST 800-53, OWASP, and ISO 9000 shall be used as guides for the development of security controls once they are determined applicable by the IT Security Team and Department Technology Committee. Once determination is in place they shall be included in the Security Controls Implementation Guide.
- D. The Security Controls Implementation Guide:
 - 1. Must be reviewed and approved by the Department Technology Committee;
 - 2. Shall contain notes as to how the control is implemented; and
 - 3. The expected impact should be included with a cost and notes on process.
- E. The ISO shall be responsible for the Security Controls Implementation Guide, its implementation, and the audit of included controls.
- F. The IT Director has the discretion as allowed within federal and state law to bypass security controls when directed by a Deputy Commissioner or an Assistant Deputy Commissioner, to temporarily resolve an outage\access issue, to comply with court orders, or to comply with competing federal or state laws.
- G. In the event any security control is bypassed, the IT Security Team member will be required to log the activity in the associated WO or RFS and seek to quickly resolve the issue causing the bypass.
- H. A WO which has a security component shall have the Security flag checked.
- I. A WO page with a security focus shall be made available for review by the ISO, Auditors, and IT Director or designee.
- J. Security requirements within this policy shall not override in any manner the compliance with federal and state laws.
- K. Passwords are confidential. Staff shall not share or disclose passwords with any other person, within or outside of the Department. Staff may NOT give passwords to OTIS staff for computer repairs. They shall log the staff in so they may accomplish their work. When computer repairs are being accomplished with a logged in computer, the staff member must keep the technician in their site at all times the system is logged in under their user account. The exception is if the computer technician is not logged in using their account, but a local admin account. Accepting the risk, a Deputy Commissioner in cases of emergency can order an override to this on a case-by-case basis.

CHAPTER	Subject	Policy #	Page
INFORMATION TECHNOLOGY	IT SECURITY	6.8	4 of 5

- L. Users are allowed administrative access to their local workstation as approved by the IT Director or designee. Users can be denied administrative level access to their computer provided it is based on specific and compelling reason.
- M. All user and data folders shall be encrypted via Active Directory Group policies or group membership.
- N. All data in transport outside the department's networks must be accomplished through encrypted channels using technologies such as SSH, SSL, #DES, or other standard encryption technology or 128 bit or higher.
- O. Connected VPN's to other organizations networks shall be approved by the IT Director with specific purpose and access to specific resources only. Any VPN shall be preceded by an MOU between the connecting entity and the DJJ. Wholesale access is allowed only for testing and diagnostic purposes.
- P. Recovery of any data on hard disks shall be handled by the IT Support Department in accordance with the IT related department policies. Recovery can be accomplished by providers once a MOU is in place.
- Q. No individual may utilize any personally owned IT resource, including software, on the Department's computers and/or networks without the approval of the IT Director or designee.
- R. Only OTIS employees or agency approved personnel may connect a device to the network. Those approvals must be routed through IT in the form of a work order so that it may be cataloged and routed to the appropriate individual.
- S. If an employee is aware of any breach in information security, including a lost or stolen IT resource, the employee must immediately notify their immediate supervisor and the Department ISO through the employee's chain of command. The employee must also complete an in-house Special Incident Report. (See DJJ 8.5, Special Incident Reporting.) If the suspected breach involves an employee's immediate supervisor, the notification should be made to the next level supervisor.
- T. Anonymous reporting of security events shall be sent through a web link from the intranet page or through a reporting hotline. Anonymous reporting of security events shall be kept captured anonymously and will remain anonymous.
- U. The Department will handle security breaches per procedures required by GTA Policy and the IT Director.
- V. No member of the Technology or Security Team shall report any event to an entity outside of the Department without the prior approval of the Deputy Commissioner or Assistant Deputy Commissioner of Administrative Services.

CHAPTER	Subject	Policy #	Page
INFORMATION TECHNOLOGY	IT SECURITY	6.8	5 of 5

W. Risk Assessments:

1. A risk assessment shall be accomplished and maintained on each technology or data resource. This shall be part of an overall Risk Management Program.
2. That risk assessment shall be updated and maintained when/if the technology or data resource is moved or its use changes.
3. The risk assessment process shall be managed in a total lifecycle approach.
4. The risk assessment process shall be managed by an application with appropriate security controls as directed by the agency ISO.

- X. Security Awareness training shall be conducted on every new employee and annually for all existing employees. The agency shall complete additional security awareness training specific to the agency as an addition to the required GBI security awareness training.

V. **LOCAL OPERATING PROCEDURES REQUIRED: NO**