MARYLAND Department of Juvenile Services

Successful Youth • Strong Leaders • Safer Communities

POLICY

SUBJECT: **Information Technology Unit Policy**
NUMBER: **IT-502-14**
APPLICABLE TO: **IT Unit employees**

APPROVED: /signature on original/
Sam Abed, Secretary
DATE: 10/27/14

I. POLICY

The Department of Juvenile Services (DJS) Information Technology (IT) unit is responsible for maintaining the integrity and confidentiality of data, as well as monitoring and managing the availability and stability of all applications and services. This policy and its accompanying manual provide DJS IT Unit staff with requirements for the appropriate development, maintenance, and implementation of the Department's information technology infrastructure.

This policy is established to ensure that data, applications and computer systems are protected from unauthorized access, modification, destruction, or disclosure consistent with Maryland Department of Information Technology (DoIT) guidelines for designing, securing, and protecting information technology resources.

II. AUTHORITY

A. MD. CODE ANN., HUM. SERVS. §§ 9-203, -204, -221
B. MD. CODE ANN., STATE FIN. & PROC. §§ 3-402 to -413
C. MD. CODE ANN., CTS. & JUD. PROC. § 3-8A-27
D. MD. CODE ANN., STATE GOV'T §§ 10-1303 to -1305
E. MD. CODE ANN., CRIM. LAW § 7-302
F. Executive Order 01.01.1983.18; Privacy and State Data System Security
G. Maryland Department of General Services - Inventory Control Manual (July 2012) (http://www.dgs.maryland.gov/Documents/inventory/InventoryControlManual.pdf)
H. Maryland Department of Information Technology (DoIT) Information Security Policy, v 3.1, February 2013
I. Executive Order 01.01.2007.01, Standards of Conduct for Executive Branch Employees

J. Standards of Conduct (March 2017)
K. DoIT Mobile Device Security Policy, (October 2011).
L. State of Maryland – Bring Your Own Device – Policy and Rules of Behavior.
M. Maryland Department of Budget & Management – Bring Your Own Device (BYOD) Pilot Program Reimbursement Policy
N. National Institute of Standards and Technology, Computer Security Incident Handling Guide (Special Publication 800-61, Revision 2)

III. DIRECTIVES/POLICIES RESCINDED

None

IV. FAILURE TO COMPLY

Failure to comply with the Department's Policy and Procedures shall be grounds for disciplinary action up to and including termination of employment.

V. STANDARD OPERATING PROCEDURES

Standard operating procedures have been developed.

VI. REVISION HISTORY

DESCRIPTION OF REVISION	DATE OF REVISION
New policy issued updating and combining IT Unit administration policies into one manual.	October 27, 2014
Procedures updated to incorporate the new enterprise model from DoIT	June 2017

MARYLAND Department of Juvenile Services

Successful Youth • Strong Leaders • Safer Communities

PROCEDURES

SUBJECT: **Information Technology Unit Policy**
NUMBER: **IT-502-14**
APPLICABLE TO: **IT Unit employees**

APPROVED: /signature on original/
Lynette Holmes, Deputy Secretary
REVISION DATE: 4/20/17

I. PROCEDURES

Procedures for the IT Unit Policy are delineated in the attached IT Unit Manual.

MARYLAND Department of Juvenile Services

Successful Youth • Strong Leaders • Safer Communities

DJS POLICY AND STANDARD OPERATING PROCEDURES

Statement of Receipt and Acknowledgment of Review and Understanding

SUBJECT: Information Technology Unit Policy
NUMBER: IT-502-14
APPLICABLE TO: IT Unit employees
REVISED: June 2017

I have received and reviewed a copy (electronic or paper) of the above titled policy and procedures. I understand the contents of the policy and procedures.

I understand that failure to sign this acknowledgment form within five working days of receipt of the policy shall be grounds for disciplinary action up to and including termination of employment.

I understand that I will be held accountable for implementing this policy even if I fail to sign this acknowledgment form.

_____ _____

SIGNATURE PRINT FULL NAME

_____ _____

DATE WORK LOCATION

SEND THE ORIGINAL, SIGNED COPY TO VERNELL JAMES IN THE DJS OFFICE OF HUMAN RESOURCES FOR PLACMENT IN YOUR PERSONNEL FILE.

JUNE 2017

DEPARTMENT OF JUVENILE SERVICES

Information Technology Unit

DJS IT Unit Manual

DJS IT UNIT MANUAL

This Manual was initially approved and issued in October 2014. It has been updated in June 2017 to incorporate the new DoIT enterprise model.

FOR HELP WITH INFORMATION TECHNOLOGY ISSUES CONTACT:
DEPARTMENT OF INFORMATION TECHNOLOGY (DOIT)
SERVICE DESK:
PHONE: 410-697-9700
EMAIL: SERVICE.DESK@MARYLAND.GOV

Table of Contents

VISION AND MISSION STATEMENTS

DJS Vision Statement
Successful youth, strong leaders, safer communities.

DJS Mission Statement
By law, the Department of Juvenile Services (DJS or Department) is a child-serving agency responsible for assessing the individual needs of referred youth and providing intake, detention, probation, commitment, and after-care services.

DJS collaborates with youth, families, schools, community partners, law enforcement, and other public agencies to coordinate services and resources to contribute to safer communities.

Information Technology Unit Mission Statement
The mission of the Information Technology (IT) Unit is to provide technology, support and security for all information systems and services needed to achieve the mission and vision of the Department.

INTRODUCTION

The purpose of this manual is to outline the DJS information systems infrastructure, the respective DJS IT Unit members' roles and responsibilities, and to describe security requirements that shall be met to protect the confidentiality, integrity, and availability of the DJS Information Technology systems.

Information security is a departmental responsibility shared by users and administrators of DJS IT systems alike. All users of DJS IT systems shall comply with the DJS *IT Users' Manual*.

The manual is subject to periodic changes as needed.

I. DEFINTIONS

For purposes of this manual, these words and phrases have the following meanings.

1. *Backup*: Copying computer data to a separate electronic media.
2. *Breach of security*: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained in DJS IT systems.
3. *Chief Information Officer (CIO)*: The employee designated by the DJS Deputy Secretary for Support Services to have the responsibility of managing the DJS Information Technology Unit and all aspects of information technology for the Department.
4. *Computer systems*: Mainframes, minicomputers, data communications facilities, local area network (LAN) file servers, microcomputer network nodes, and stand-alone microcomputers (desktops or notebooks/portables).
5. *Confidential information or data*: Non-public information that has been deemed to contain youth or personal information, which if disclosed could result in a negative impact to the State, DJS employees, or youth.
6. *Data center*: A facility used to house computer systems and associated components, such as telecommunications and storage systems.
7. *Demilitarized Zone*: A separate interface in the firewall to protect the internal network from external intrusions.
8. *Department of Information Technology (DoIT)*: The state agency responsible for statewide centralized IT support and services.
9. *Electronic Mail (e-mail)*: The electronic transfer of information including electronic messages and/or attached documents from a sending party to one or more receiving parties via an intermediate data system.
10. *Firewall*: A software or hardware-based network security system that controls incoming and outgoing network traffic based on an applied rule set.
11. *Firewall Administrator*: The individual responsible for managing the activities of the firewall.
12. *Hardware:* Any type of DJS IT equipment, including but not limited to, laptops, smartphones, netbooks, tablets, removable storage devices, air cards, and any mobile computers and devices.
13. *Information Technology Unit*: The group of DJS employees collectively responsible for DJS network, applications, telecommunications, technical support, and all other information-technology related activities.
14. *Internet*: An external, global system of interconnected computer networks.
15. *Intrusion Detection/Prevention (IDP)*: An intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity.
16. *Life cycle*: The period of time during which information technology hardware equipment and software is useful to the State.
17. *Loaner pool*: A collection of wireless equipment available for assignment on a temporary basis to employees with short-term justification to use wireless technology and services.
18. *Local Area Network (LAN)*: A system that interconnects computers or other hardware or

equipment within a limited area using network media, allowing computers to exchange data.

19. *Long-term assignment*: Assignment of a wireless technology from the loaner pool for a period of 31 days or more.
20. *Master listing*: A centralized registry of all wireless technology obtained or held by DJS for use by DJS employees.
21. *Patch*: Software used to fix or update applications and operating systems.
22. *Personal information*: An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:
    a. a Social Security number;
    b. a driver's license number, state identification card number, or other individual identification number issued by a unit of State government;
    c. a passport number or other identification number issued by the United States government;
    d. an Individual Taxpayer Identification Number; or
    e. a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.
23. *Removable storage devices*: A data storage device, typically detachable and rewritable, that allows for the transportation of information away from the originating computer and is used for the storage, backup or transfer of computer files.
24. *Password*: An authorization code to gain access to system resources.
25. *Temporary assignment*: Assignment of a wireless technology from the loaner pool for a period of 30 days or less.
26. *User*: Any person with access to any DJS information system.
27. *Virtual Private Network (VPN)*: A tool that extends a private network across a public network, such as the internet.
28. *Wireless technology*: Any State-issued technology or device with the ability to transfer voice or data to another device without requiring a connection to a publicly switched telephone network (e.g., cellular telephones, pagers, mobile radios, pagers, smart phones, tablets, and cellular modems/air cards).

II. INFORMATION TECHNOLOGY UNIT ADMINISTRATION AND DUTIES

A. The duties of the DJS IT Unit include:
    1. maintaining the integrity, confidentiality, availability, security and accountability of all systems and data in accordance with security guidelines and standards promulgated by DoIT;
    2. ensuring the availability of needed equipment and systems to appropriate staff and others;
    3. monitoring system usage to ensure that access is being provided in accordance with Statewide information security policies;
    4. ensuring that the appropriate system access warnings are provided to users of each

system in accordance with DoIT access control requirements;
5. providing technical assistance to DJS IT users concerning IT matters and promulgating user guidelines for DJS IT systems in conjunction with the Office of Legislation, Policy, & Communications;
6. developing and maintaining the DJS IT master plan;
7. maintaining IT hardware and software assets, including tracking the purchase, configuration, installation, maintenance, and disposal of all IT and telecommunication devices;
8. maintaining a record of all information systems and licensing agreements;
9. providing input, coordination, and an inventory, where necessary, of the procurement and monitoring of building utility services related to computing and communications needs at all DJS worksites;
10. coordinating and maintaining oversight of any applicable contracts or agreements related to DJS IT services;
11. overall responsibility for addressing IT-related breaches of security and confidentiality;
12. identification and implementation of system maintenance and remotely-executed maintenance and diagnostic activities in accordance with manufacturer or vendor specifications and/or organizational requirements;
13. implementing an on-going risk management process for DJS IT systems;
14. participating in annual information systems data security self-audits focusing on compliance with the current DoIT Information Security Policy; and
15. ensuring that security is part of the information planning and procurement process.

III ASSET MANAGEMENT

A. Generally

1. The DJS IT Unit is responsible for requesting and overseeing the purchase, installation, inventory, maintenance, support, and disposal of all IT-related equipment in compliance with this manual, applicable DJS policies and procedures, the Maryland Department of General Services (DGS) Inventory Control Manual, and the current DoIT Information Security Policy.
2. The appropriate DJS IT Unit manager or designee shall approve the installation of all IT-related equipment and telecommunication devices.

B. Procurement and Monitoring of Hardware and Physical Assets

1. Except as otherwise provided in this manual or in statute, regulation, or policy, the IT Procurement Officer is responsible for procuring hardware and physical assets, services, wireless technology, and computer systems.
2. The DJS IT Unit shall implement its procurement function and perform or oversee and verify quarterly audits to ensure the currency of the inventory database.
3. All DJS IT Unit staff are responsible for identifying and reporting superfluous

equipment assignments and unused equipment to the DoIT Helpdesk Services to ensure efficient and effective deployment and utilization of DJS IT Unit assets.

C. **Procurement and Inventory of Software Assets**

1. Except as otherwise provided in this manual or in statute, regulation, or policy, the DJS IT Unit is responsible for procuring and maintaining inventories of all software assets including system software, software development tools, and applications throughout the entire life cycle of the asset.
2. Only properly licensed software packages authorized by the CIO or designee shall be installed on DJS assigned computer equipment. The use or installation of unauthorized or improperly licensed software or programs is strictly prohibited.

D. **Inventory and Availability of Information Assets**

1. The DJS IT Unit shall ensure that information asset manuals, system documentation, and operational and support procedures or resources are available and may be accessed for consultation as needed in conjunction with the manufacturer, developer, or distributor.
2. The DJS IT Unit shall maintain an inventory of information systems as part of its security plan and update and review the inventory annually. The Deputy CIO, in conjunction with the appropriate DJS IT Unit staff, approves of the final inventory.

E. **End of Life Cycle/Equipment Disposal**

1. The DJS IT Unit shall maintain a multiple-year life cycle for all DJS-owned and leased IT equipment to ensure that the equipment is replaced when it becomes obsolete or is otherwise no longer useful.
2. Subject to budgetary restrictions and administrative or operational need, all DJS IT equipment shall be subject to the following life cycle:

Equipment Type	Replacement Cycle
Network infrastructure (routers, switches, media converters)	8 years
Servers	8 years
Desktop computers	5 years
Laptop computers/tablets	5 years
Printers/Fax Machines/Copiers/Scanners	5 years
Telephones	As needed
Smartphones/Cell phones	5 years or pursuant to vendor contract

3. DJS IT staff in conjunction with DoIT staff shall maintain a system of life cycle and equipment disposal documentation requiring appropriate signatures to ensure accountability.

F. **Equipment Sanitization**

DJS IT management shall be responsible for ensuring the sanitization and/or disposal of any hardware or media containing confidential or high-risk data any time the equipment will be transferred or made accessible to an external entity. This shall include the protection and disposal of confidential information in a manner consistent with the DoIT Information Security Policy.

G. **Disaster Recovery Plan**

1. The DJS Deputy CIO is responsible for the maintenance of a DJS IT Disaster Recovery Plan in compliance with the Department's Continuity of Operations (COOP) strategy and the DoIT Information Security Policy.
2. The plan shall be posted and available annually to all members of the DJS IT Unit.
3. The DJS IT Unit shall annually conduct testing exercises and maintain appropriate documentation demonstrating compliance with and integrity of the plan.

H. **Access Controls and Physical Security**

1. Access to data centers shall be physically controlled and restricted.
2. The DJS CIO or his or her designee shall maintain a current list of persons with access to data centers containing confidential information. The list shall be marked on the entryway to secured areas. Persons with approved access shall supervise access to data centers by persons without approved access.
3. Data centers and closets containing DJS IT infrastructure devices and equipment shall be secured where practicable. Access shall be restricted to DJS IT-approved personnel only.
4. All data centers must be capable of protection from known vulnerabilities including fire, water, and electrical failure. This protection includes notification to the appropriate DJS IT Unit and/or DoIT staff in the event of a network-related problem or failure and logging the network status to a central location.
5. Wiring and equipment closets must be equipped with adequate ventilation and a dedicated electrical circuit where practicable.

IV. INFORMATION SECURITY GENERALLY

A. The CIO shall ensure that:

1. all DJS IT Unit staff properly handle, classify, and protect confidential information within DJS IT systems that is processed, stored, or transmitted via any means; and
2. all DJS staff with access to IT systems are provided with requirements for proper confidentiality measures necessary to identify and protect confidential information.

B. The Deputy CIO or their designee shall be responsible for:

1. classifying data pursuant to the current DoIT Information Security Policy; and
2. implementing and maintaining an IT security program.

C. Any DJS IT Unit staff that discovers or is notified of a breach of security of any DJS IT system involving personal information shall immediately inform the CIO, who shall initiate an investigation pursuant to the Maryland Annotated Code, State Government Article, Title 10, Subtitle 13.

V. SUPPORT SERVICES

A. DoIT is responsible for all support services. To aid DoIT's efforts, the DJS IT Unit monitors or participates in the following:

1. administration of agency-wide user support;
2. ensuring that documentation regarding the installation, transfer, repair and disposition of all IT equipment is completed with signatures and dates and retaining these documents in electronic and printed format;
3. inventory of hardware, software, and physical assets including computer, telecommunication, and other technical equipment;
4. maintaining a list of software supported by the DJS IT Unit for user reference;
5. updating the Asset Control database with inventory information;
6. ensuring that all equipment issued to users is maintained and updated in accordance with the Department's technological needs including vendor-recommended patches and service packs;
7. monitoring hardware and software for technological inefficiencies;
8. ensuring proper disposal of all IT-related equipment;
9. reviewing and processing requests for equipment, systems, and services;
10. ensuring proper system configuration and management of user accounts;
11. installation of VPN clients and providing support and training for authorized VPN users;
12. monitoring trends in user Help Desk inquiries and suggesting appropriate remedies in user actions to supervisors;
13. properly labeling computer hardware, installing images on computer hardware,
14. verifying that the standard image has been properly installed, and further preparing hardware for distribution as needed;
15. reviewing system usage logs and monitoring network usage as necessary;
16. ensuring proper functionality of all video surveillance equipment at DJS facilities weekly; and
17. ensuring monthly that security patrol software logs are reviewed to ensure that the appropriate executive staff are notified in the event of non-compliance with established facility security standards.

B. **Equipment Deployment Criteria; Repair and Replacement**

1. Hardware shall be deployed based on:
   a. the assignment of workstations to employees;
   b. equipment needs based on worker assignments as approved by the worker's supervisor;

c. replacement of broken, irreparable or problematic equipment, including equipment that is too costly to repair or no longer warrantied; and
d. replacement of equipment that has reached the end of its established life cycle.

2. Decisions to repair or replace equipment shall be made by the CIO, taking into consideration the equipment's stage in its life cycle or when otherwise cost effective.
3. When equipment is in need of repair, Help Desk staff shall determine whether an equipment warranty or lease agreement covers the repair and shall log a call with the appropriate vendor, lessor, or manufacturer as appropriate.

C. **Help Desk and User Support Response Protocol**

1. The DJS IT Unit shall utilize DoIT's ServiceNow system to monitor/administer user support for IT-related problems and issues. The Help Desk shall be available to users via phone and e-mail during regular business hours and during additional limited times as needed in accordance with internal procedures.
2. The DJS IT Unit staff shall escalate, forward or reassign support tickets to the appropriate division of the DJS IT Unit using a shared ticket as needed, which shall remain active for the duration of the problem.

D. Password Standards

1. DJS-issued hardware and wireless technology shall be configured to prompt the user for a logon ID and password before accessing the desktop.
2. Where involved, staff from the DJS IT Unit shall ensure that all users are uniquely identified and that all passwords meet the construction, usage, and change requirements pursuant to DoIT security standards.
3. Group or shared user IDs are prohibited except automated programmed system authentications.
4. Administrative passwords shall be assigned and managed in accordance with DoIT security guidelines.
5. The DJS IT Unit staff shall ensure prompt termination of all system access for staff separated from State service.

F. **System Access Requests, Approvals, and Denials**

1. Employee system access shall be granted only after:
   a. receipt of an IT System Access Request Form by the employee's supervisor or other appropriate management staff; and
   b. confirmation of the employee's acknowledgment of receipt of the DJS IT Users' Manual.
2. Once approved by the appropriate the DJS IT Unit staff, the employee's supervisor can be contacted and coordinate the employee's access.
3. System access requests shall be denied for the following reasons:
   a. incomplete system access requests;
   b. failure to obtain confirmation that the employee has acknowledged receipt of the IT Users' Manual; or

c. the provided justification does not meet eligibility criteria for system access.

4. Any person from external organizations or entities who require access to any DJS IT system shall be required to submit to the DoIT Help Desk, via the appropriate DJS supervisor or project manager responsible for overseeing the work of the person, the following:
   a. a copy of the current signed contract, intergovernmental agreement, memorandum of understanding or agreement between DJS and the entity with whom the person applying for access is associated;
   b. a copy of the DJS *IT System Request Form* specifying the system(s) or application(s) needed;
   c. a complete and signed copy of the *ASSIST Access Agreement for Organizations* and the *DJS Network Access Agreement for Organizations*;
   d. a signed copy of the *Confidentiality Agreement for Individuals*; and
   e. confirmation that the person has acknowledged receipt of and agrees to comply with the IT Users' Policy & Manual.
5. The DJS IT Unit is responsible for identifying accounts that have not been used for 60 days or longer to be removed or disabled.

G. **Confidentiality Standards**

1. DJS IT Unit staff may not under any circumstances divulge a user's password to anyone other than the user (including supervisors).
2. User passwords may not be transmitted via e-mail when the user account is also identified in the e-mail.
3. Any DJS IT Unit staff observing user practices or actions constituting a risk to confidentiality or information security shall report the action to the user's supervisor and the CIO.

VI. NETWORK SERVICES

A. **Generally**

1. DoIT is responsible for network services; the DJS IT Unit, however, does request, monitor and validate the following:
   a. network hardware and equipment installation, maintenance, and removal;
   b. development and implementation of a system of incident response in accordance with the DoIT Information Security Policy;
   c. configuration of network-related hardware, software, and security assets;
   d. implementation of methodologies to ensure agency-wide network and systems security and integrity, including ensuring that remote network access is available only to authorized users and secured using current security practices and standards;
   e. backup and restoration of all data maintained on DJS networks;

f. response to tier II network-related requests according to established procedures; and
g. ensuring that software patches and updates are available to all users.

B. **Firewall Security**

1. General Procedures
   a. The DJS network shall be protected by a firewall that is managed by DoIT. The firewall will produce log files, which shall be backed up and stored off site in a secured location in an appropriate manner.
   b. The appropriate administrator shall generate reports and make them available to log reviewer monitors for daily reviews. Log reviewer monitors shall report anomalies for investigation as appropriate.
   c. The DJS firewall shall be configured to block all unused ports, limit administrative access to IP addresses or subnets assigned to administrators of the firewall device, maintain comprehensive audit trails, and ensure that publicly-accessed servers are protected against intrusion and attack by configuring a separate network interface designated as a Demilitarized Zone.
   d. An Intrusion Detention/Prevention protection device shall be utilized to provide the DJS network with an extra layer of protection.
2. Configuration of Change Procedures
   a. The Network Administrator shall make all changes to the firewall as necessary.
   b. All changes and testing must be submitted to the CIO as a project plan. The approved project plan will serve as the log of changes and shall be stored on the server with the log files. In the case of an emergency, project plan approval is not required; however, an emergency project plan shall document all changes made and submitted to the CIO within 5 business days of the emergency.

VII. WIRELESS TECHNOLOGY & TELECOMMUNICATION DEVICES

A. **DJS IT Unit Responsibilities**

1. The DJS IT Unit:
   a. assists in developing and implementing policies and procedures to ensure protection of data transmission and storage on mobile devices, wireless technology, and telecommunications devices including removable media;
   b. provides end-user training for the use of wireless technology and telecommunication devices as needed;
   c. maintains a centrally-managed system for wireless technology distribution and installation;
   d. sanitizes wireless technology when returned, exchanged, or disposed; and
   e. implements all other DoIT-recommended wireless technology security measures as applicable and necessary.

B. **Chief Information Officer duties**

1. The CIO or designee shall:
   a. review and approve or disapprove each request for wireless technology equipment and services;
   b. ensure that the most cost-effective device is selected for employees eligible for assignment of a wireless technology;
   c. ensure that wireless technology devices are individually identified with a DJS inventory tag number matched to the device's unique electronic serial number at the time that the wireless technology is assigned to a DJS employee;
   d. maintain a current master listing of all wireless technology issued by the Department that shall include the name and work addresses of each authorized user, the wireless technology number assigned to that employee, and the DJS inventory tag number matched to the device's unique electronic serial number;
   e. develop and implement a protocol for monitoring the use of wireless technology, identifying personal use made on wireless technology devices and directing employees to remit payment to the DJS IT Unit for forwarding to the Accounting Unit for the cost of personal usage;
   f. administer the Department's Bring Your Own Device program; and
   g. establish and manage a loaner pool of wireless technology devices available for temporary use and assignment.

VIII. APPLICATIONS

A. Except as otherwise provided in this manual or applicable DoIT or other information security policy, the Applications division of the DJS IT Unit is responsible for all aspects of customized DJS systems and applications to which DJS staff and other entities have access. The division is also responsible for coordination of access to external systems or applications to which Department staff has access. These include, but are not limited to:
   1. ASSIST;
   2. Small Apps;
   3. Safe Measures®;
   4. METS
   5. Child Safety Net Dashboard;
   6. CHESSIE;
   7. MMIS; and
   8. all DJS and external web applications;

B. All customized programming shall adhere to the requirements set forth in the DoIT Information Security Policy and shall be retained in the Team Foundation Server (TFS). All major applications projects shall follow a systems design life cycle, and their design shall include all security-related requirements.

C. External access to DJS systems and access by DJS staff to external systems or applications shall be subject to compliance with established memoranda of

understanding, inter-governmental agreements, contracts, and applicable law and regulations.

D. Confidentiality of youth and family information shall be preserved in the development and/or implementation of all applications, whether or not the application is designed or hosted by the Department, pursuant to state law and regulations.

E. The DJS Database Administrator is responsible for standby backup and security of the primary database pursuant to the DoIT Information Security Policy.

F. Applications programmers shall ensure that routine maintenance does not compromise security standards built within the application or system.

G. All systems shall be programmed to meet the access control requirements set forth in the DoIT Information Security Policy.

H. The DJS Applications Unit staff shall document significant changes to the coding of application access controls.

IX. VIRTUALIZATION TECHNOLOGIES

A. The DJS IT Unit may utilize virtualization technologies where it is efficient and cost-effective based upon the Department's needs.

B. The assigned staff from the DJS IT Unit responsible for overseeing virtualization solutions shall ensure that the virtual environment is as secure as non-virtualized environments and complies with all relevant State policies, and National Institute of Standards and Technology guidance.

X. POLICY MANAGEMENT

The DJS Deputy CIO or their designee shall ensure that all IT policies, procedures, and directives comply with existing Maryland Department of Information Technology policies and industry standards by participating on the DJS policy committee responsible for reviewing, revising and updating policies annually or as necessary.

XI. FAILURE TO COMPLY

Failure to comply with the DJS IT Unit Policy and Procedures Manual shall be grounds for disciplinary action up to and including termination of employment.

XII. POLICIES & FORMS REFERENCED

1. Mobile Devices and Services Statewide Policy
2. DoIT State of Maryland Information Security Policy
3. DJS Confidentiality Policy
4. DJS Communication with Public and Media Policy
5. IT System Access Request Form
6. Wireless Technology Reimbursement Form
7. Mobile Device Security Policy