MARYLAND Department of Juvenile Services
Successful Youth • Strong Leaders • Safer Communities

# POLICY

**SUBJECT:** **Information Technology Users' Policy**
**NUMBER:** **IT-501-14**
**APPLICABLE TO: All DJS Employees**

**APPROVED**: /signature on original/
**Sam Abed, Secretary**
**DATE:** 4/3/14

## I. POLICY

The Department of Juvenile Services (DJS) Information Technology unit (IT) is responsible for maintaining the integrity, confidentiality, availability and accountability of all applications and services with support from Maryland Department of Information Technology (DoIT). This policy provides DJS employees with guidelines in the appropriate use and responsibilities when using IT resources.

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

## II. AUTHORITY

A. Md. Code, Human Services Article, §9-203, §9-204, and §9-221
B. Md. Code, State Finance and Procurement Article, §3-402 through §3-413
C. Md. Code, Cts. and Jud. Proc., §3-8A-27
D. Annotated Code of Maryland, Criminal Law Article, §7-302
E. Executive Order 01.01.1983.18; Privacy and State Data System Security
F. Maryland Department of General Services - Inventory Control Manual (http://www.dgs.maryland.gov/Documents/inventory/InventoryControlManual.pdf)
G. Maryland Department of Information Technology (DoIT) Information Security Policy, v 3.1, February 2013
H. Executive Order 01.01.2007.01, Standards of Conduct for Executive Branch Employees
I. DJS Standards of Conduct and Disciplinary Process (March 2017)
J. DoIT Mobile Devices and Services Statewide Policy (2/20/10)
K. State of Maryland – Bring Your Own Device – Policy and Rules of Behavior
L. Maryland Department of Budget & Management – Bring Your Own Device (BYOD) Pilot Program Reimbursement Policy

## III. DIRECTIVES/POLICIES RESCINDED

None

## IV. FAILURE TO COMPLY

Failure to comply with the Secretary'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 combining all IT policies for users of DJS IT systems into one manual. | June 2013 |
| Manual updated to implement the State's "Bring Your Own Device" initiative. | March 2014 |
| Revised procedures 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 Users' Policy**
**NUMBER:** **IT-501-14**
**APPLICABLE TO: All DJS Employees**

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

## I. PROCEDURES

Procedures for the IT Users' Policy are delineated in the attached IT Users' Manual.

# DJS POLICY AND STANDARD OPERATING PROCEDURES

## Statement of Receipt and Acknowledgment of Review and Understanding

**SUBJECT: Information Technology Users' Policy**
**NUMBER: IT-501-14**
**APPLICABLE TO: All DJS Employees**

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

# IT Users' Manual

## IT USERS' MANUAL

This Manual was initially approved and issued in June 2013. It has been updated in:

- March 2014 to include procedures to implement the state's Bring Your Own Device initiative; and
- 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 the DJS IT Users' Manual is to provide users of DJS information systems, equipment and services, including employees, volunteers, and contract employees, with written documentation of security requirements and procedures by which users must abide to protect the confidentiality, integrity, and availability of DJS data and equipment.

All DJS employees, volunteers, and contract personnel are responsible for:

- Implementing statewide and internal policies and understanding their responsibilities for protecting the IT assets of DJS and the state of Maryland;
- Using IT resources only for intended purposes as defined by policies, laws and regulations of DJS and the state of Maryland; and
- Being accountable for their actions when using any DJS IT information system.

The manual is subject to periodic changes, as needed. All users shall be notified by the DJS Policy Unit of any revisions to the DJS IT Users' policy or manual.

# I. DEFINITIONS

1. *Business call:* A telephone call directly related to the operation of DJS.
2. *Chief Information Officer (CIO)*: The employee designated by the Deputy Secretary for Support Services to have the responsibility of managing the Information Technology Unit and all aspects of information technology for the Department.
3. *Computer systems*: Mainframes, minicomputers, data communications facilities, local area network (LAN) file servers, microcomputer network nodes, and stand-alone microcomputers (desktops or notebooks/portables).
4. *Confidentiality*: Information that is deemed private, privileged or sensitive and is prohibited from disclosure to any person except in accordance with law.
5. *Electronic Mail (email):* 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.
6. *Hardware:* Any type of DJS IT issued device (laptop, smartphones, netbooks, removable storage device, and air cards).
7. *Internet:* An external, global system of interconnected computer networks.
8. *Intranet:* An internal computer network system that uses internet technology to share information, operational systems, or computing services within an organization.
9. *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.
10. *Long-term assignment:* Assignment of a wireless technology from the loaner pool for a period of 31 days or more.
11. *Mobile computers:* Laptops and tablets.
12. *Mobile Device:* All wireless computer equipment including air cards, cell phones, laptops, tablets or pagers.
13. *Personal call:* A telephone call not directly related to the operation of DJS and outside the scope of employment responsibility of the person making or receiving the call.
14. *Removable storage devices:* A data storage device that is typically detachable and rewritable and is used for the storage, back-up or transfer of computer files.
15. *Prohibited Sites:* Internet sites and activities to which access is forbidden. These sites include, but are not limited to, sites relating to non-business related chat rooms, social media, on-line gaming, streaming radio, sexually explicit, pornographic or nude images or content in any form, on-line gambling, and any unlawful online activities, such as hacking.
16. *Spam:* The widespread distribution of unsolicited email.
17. *Telecommunication Device:* A handheld device that communicates via cellular or wireless technology, including cell phones, pagers or two-way radios.
18. *Temporary assignment*: Assignment of a wireless technology from the loaner pool for a period of 30 days or less.
19. *Users*: Any person with access to any DJS information system.
20. *Wireless technology:* Any 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, mobile radios, pagers, smart phones, tablet, and cellular modems/air cards).

## II. GENERAL GUIDELINES FOR IT USERS

A. All users shall abide by the DJS IT Users' Manual as well as the *Mobile Devices and Services Policy* and the *State of MD Information Security Policy.*

B. The primary use of DJS information systems, services and equipment shall be limited to official business use only or personal use in the event of an emergency.

C. Users should take all necessary safeguards, including encryption, to protect a youth's right to privacy when transmitting information via email or the internet. All users who send encrypted authorized confidential information shall notify the recipient of the password via phone when necessary. (*Note: the penalty for disclosing confidential information may result in disciplinary action and/or criminal penalties according to the DJS Confidentiality Policy.*)

D. All information communicated electronically by the user over DJS information systems or work-related information communicated by using a personal device in conjunction with the Bring Your Own Device (BYOD) program is subject to state laws, regulations, policies and procedures.

E. Users shall return all devices issued by the DJS IT Unit to the DJS IT Unit upon request or when separated from employment and obtain a copy of the *Equipment Property Release Form* signed by an IT employee and the user.

F. When a DJS employee leaves DJS service,
   1. The employee shall return all devices issued by the IT Unit and complete a *Property Checklist Form;* and
   2. the supervisor must complete and submit the *IT Change Request Form* to the DoIT Service Desk indicating the last day the employee requires system access.
   3. Users shall submit a signed acknowledgment of receipt of this DJS IT Users' Manual acknowledging their understanding of the Manual and obligations as a condition of gaining access to DJS computer systems, including by way of participation in the BYOD program.

## III. SYSTEMS ACCESS AND SECURITY

A. DJS supervisors will request access for their employee to the DJS Information Technology (IT) supported applications and systems by submitting the *IT System Access Request Form* along with a signed acknowledgment of receipt of this *IT Users' Manual* to the DoIT Service Desk as an email attachment where it will be processed.

B. The IT Unit will create an account for approved access to systems and services that users need to perform their job functions.

C. The DoIT Service Desk staff shall assist users with logging onto the systems for the first time and changing their passwords to meet the Password Standards as defined by the *State of MD Information Security Policy*.

D. All staff from external organizations or agencies that require access to any IT system must complete the *IT System Access Request Form,* submit a signed acknowledgment

of receipt of this *IT Users' Manual*, and abide by the procedures established by the IT Users' Manual and the *DJS Confidentiality Policy.*

# IV. HARDWARE AND SOFTWARE

A. DoIT is responsible for the procurement, installation, support, replacement and disposal of all IT related devices.

B. All requests for non-standard equipment or software shall be submitted in writing to the DJS Chief Information Officer (CIO) justifying the need. Non-standard hardware and software requests require approval from the CIO.

C. Only authorized and properly licensed software packages that are installed by an IT technician can be used on state owned and issued computer equipment. The use of unauthorized or improperly licensed software or hardware is strictly forbidden.

D. Approval of requests for non-standard software does not guarantee DJS IT support. The user will be responsible for obtaining support for any non-standard software from the vendor.

E. Knowingly running or installing a program intended to damage or to place excessive load on a computer system or network (including computer viruses, Trojan Horses, and worms) is forbidden.

F. Mobile computer users will need to report to a DJS office, at least monthly, to connect to the network to receive security patches, virus, Windows, and client updates.

G. Workstations and laptops will be configured to prompt the user for a logon ID and password before accessing the desktop.

H. A password protected screen saver should be activated if the workstation or laptop is left idle for 45 minutes.

I. The use of removable storage devices is acceptable. Users shall not store any personal information on any removable storage device where DJS information also is stored. Any confidential information stored on such devices shall be encrypted and labeled as confidential.

J. All information stored on DJS IT related devices is the property of DJS and may be subject to disclosure for public information act requests or monitoring by DoIT Staff.

K. Users shall:

1. maintain reasonable care of all hardware and may not alter, repair, or misuse equipment;
2. report hardware and software problems or damage to the DoIT Service Desk;
3. report stolen or missing assigned IT devices by submitting a completed *Missing or Stolen Personal State Property Form* and a copy of the completed Police Report to the DoIT Service Desk;
4. turn off or lock their mobile computer, when the mobile computer is left unattended; and
5. ensure that the mobile computer is physically secured when not in use by placing the computer in a locked office, a desk or cabinet drawer, or not leaving the computer in their car unattended.

# V. WIRELESS TECHNOLOGY & TELECOMMUNICATION DEVICES

## A. Requesting a Telecommunication or Wireless Device

1. Users shall request telecommunications or wireless devices by completing and submitting the following to their supervisor:
   a. *Request for Wireless Technology Equipment Form*;
   b. Signed acknowledgment of receipt of this *IT Users' Manual;* and
   c. Signed acknowledgement of *Employee Acknowledgement of Agency Mobile Devices and Services Policy* Form.
2. The Supervisor shall forward the approved *Request for Wireless Technology Equipment Form* and the above documents to the DJS CIO.
3. The DJS CIO or designee will review the request and either approve or disapprove the request.
4. The IT Unit shall obtain the users' signature on an *Equipment Property Release Form* upon the user's receipt and return of the equipment.

## B. Assignment of Devices (DJS employees only)

1. The following DJS employees shall be eligible for long-term assignment of a wireless technology or telecommunication device:
   a. Employees who are away from their assigned office on state business for a significant part of their normal work day and have a frequent and recurring need to communicate with others;
   b. Employees who must be accessible outside of ordinary business hours for emergency response, restoration of services, or enhanced safety of DJS clients or employees;
   c. Employees who are responsible for management of constituent services; and
   d. Employees who are integral to the Department's decision-making process.
2. DJS employees ineligible for long-term assignment of a wireless technology or telecommunication device may be eligible for temporary assignment from the DJS loaner pool upon approval by the employee's supervisor. The assignment will be based on achievement of work efficiency, safety, emergency response capability, or other good cause.
3. Supervisors shall review the usage report every month for each DJS employee within their supervisory responsibility who is assigned a wireless technology or telecommunication device and inform or remind, as needed, the employee of the wireless technology or telecommunication device use restrictions and obligations set forth in this policy and procedure; and take necessary disciplinary action for misuse of wireless technology or telecommunication device.
4. An employee's eligibility for assignment of a wireless technology or telecommunication device may be revoked and terminated when a pattern of misuse is identified. For approved and prohibited usage, see Sections VII.A. and VII.B.
5. The employee may also be subject to disciplinary action up to and

including termination from employment for misuse of wireless technology or telecommunication devices.

6. Mobile (two-way) Radios.
   a. Employees using a mobile radio are responsible for safeguarding them at all times.
   b. Employees shall report a damaged mobile radio to the Shift Supervisor who shall notify the DoIT Service Desk.
   c. Employees shall report a lost or stolen mobile radio to the Shift Supervisor who shall report the loss or theft to the DoIT Service Desk by submitting a completed *Missing or Stolen Personal State Property Form* and a copy of the completed Police Report to the DoIT Service Desk.

**C. Reimbursement for Use of State-Issued Wireless Devices or Telecommunication Devices**.

1. A DJS employee shall limit their use of a state-issued cellular telephone for non- business related calls to 30 minutes per month and reimburse the State for non- business related calls if the total duration of the employee's non-business related calls exceeds 30 minutes per month. Employees who fail to reimburse the Department for non-emergency personal use may be subject to disciplinary action up to and including termination.
2. Employees who use their own personal cellular telephone to conduct state business and who do not participate in the BYOD program may be reimbursed for legitimate business calls at a rate specified in the *Wireless Technology Reimbursement Form*.

**D. Bring Your Own Device (BYOD) Program Reimbursement Eligibility and Requests to Participate**

**1. Eligibility and Requests to Participate**

   a. Participants must be in positions with a demonstrated business need for a State-issued mobile device as determined by the CIO or his or her designee.
   b. Employees shall request to participate in the BYOD program by completing and submitting the following to their supervisor:
      1) a completed IT System Access Request Form indicating the make, model, and phone number of the personal device to be used;
      2) a signed acknowledgment of receipt of this IT Users' Manual; and
      3) a signed acknowledgment of receipt of the State of Maryland Bring Your Own Device – Policy and Rules of Behavior.
   c. The supervisor shall forward the approved *IT System Access Request*; Form and the above acknowledgments to the DJS CIO.
   d. The DJS CIO or designee will review the request and either approve or disapprove the request. The CIO or designee will determine whether the services required include voice only or voice and data.
   e. Employees currently assigned a mobile device must surrender his or

her currently assigned device and provide proof of a personal device with the required services and features to meet the business need.

**2. Participation**

a. Participation in the BYOD program is optional for eligible employees. An employee choosing to participate must meet any requirements set forth by the DoIT related to BYOD participation and any other applicable DJS policy. Staff who elect to participate in the program must do so for a minimum of six months.

b. Employees participating in the BYOD program are required to maintain a working device and are responsible for replacement of damaged or broken devices.

c. Participating employees must allow any security measures to be installed on the personal device as required by DoIT and the IT Unit.

d. The participating employee is responsible for all fees related to mobile services contract changes and cancellations and the costs of maintaining, repairing, and/or replacing the mobile device.

e. DoIT will not provide support services for any issues encountered on a personal mobile device. Employees shall resolve all issues with their service provider or mobile device vendor or manufacturer

**3. Reimbursement Guidelines**

a. Subject to section b. below, participating employees will receive reimbursement in accordance with rates posted on the *Wireless Technology Reimbursement Form* for use of their personal devices for business purposes not to exceed the established amounts, regardless of actual costs incurred in using and maintaining the personal device.

b. Reimbursement amounts are calculated so as not to exceed expenses the participating employee actually incurs in maintaining the device. Reimbursement payments shall not exceed reimbursement levels set by the State.

c. Where applicable, reimbursement for voice and/or data shall be at the service level provided when the employee had a state-issued device.

d. The amount of reimbursement received by a participating employee shall be restricted to no more than one voice and one data plan per month.

**4. Reimbursement Process**

a. Submission of expense report. Participating employees shall complete a State of Maryland Expense Account form (GAD X-5) identifying the expense as "Mobile Device" and shall submit the form according to the standard expense reimbursement process. The expense account form must be accompanied by the required documentation below and be approved by the employee's supervisor. Expense reports for mobile

device reimbursement shall be submitted on a quarterly basis.

b. Required documentation. Participating employees must submit copies of their monthly device bills showing that the device is activated and has the required reimbursable features (voice, data, etc.). The employee's name or device telephone number must be listed on the bill.

c. Payment. Reimbursement payments to participants do not constitute an increase to base pay and will not be included in the calculation of any salary adjustments or be treated as compensation for any purpose.

**5. Non-Reimbursement E-Mail Participation**

a. Employees without a demonstrated business need for a State-issued mobile device as determined by the CIO or his or her designee may use personal devices for direct access to their state email account. Employees shall request access by completing and submitting the following to their supervisor:

1) a completed IT System Access Request Form that indicates the make and model of the personal device to be used and that states "non- reimbursement participation in the BYOD program;"

2) a signed acknowledgment of receipt of this DJS IT Users' Manual; and

3) a signed acknowledgment of receipt of the *Mobile Device Security Policy.*

b. The supervisor shall forward the approved *IT System Access Request* Form and the above acknowledgments to the DJS CIO.

c. The DJS CIO or designee will review the request and either approve or disapprove the request.

d. Employees must adhere to the BYOD Participation section above.

e. Employees are not eligible for reimbursement using mobile devices under this section.

# VI. ELECTRONIC MAIL, INTERNET AND INTRANET

A. General Guidelines for Email, Internet and Intranet Use

1. Users' email addresses, email passwords, equipment and all messages that are created, sent or received using DJS' email systems are the property of the state and may therefore be subject to audit and may be used in legal or disciplinary actions.

2. Users with access to the internet using state-issued equipment shall limit any non- work related internet access to a maximum of 30 minutes per day and access may be further limited, prohibited entirely, or restricted by a user's supervisor and/or DJS executive staff.

3. Users shall communicate electronically as they would in a public meeting and in a professional manner that reflects positively on the user, the Department and the state of Maryland, and in accordance with the *DJS Communication with Public and Media Policy* and *DJS Standards of Conduct.*

4. Any access to or attempt to access prohibited sites using state-issued equipment may be grounds for disciplinary action.
5. Access to DJS internet services on state-issued equipment may be revoked with or without notice if a user violates this policy and its procedures. In addition, a user may be subject to disciplinary and/or criminal proceedings.

# VII. ACCEPTABLE AND PROHIBITED USAGE

## A. Appropriate Usage

1. DJS-issued technology and personal devices used for work-related purposes in conjunction with the BYOD program shall be used for communications that serve legitimate business functions and purposes of the Department and the state of Maryland.
2. Examples of appropriate use include, but are not limited to:
   a. Communication with federal, state, or local government personnel, vendors, and other private businesses;
   b. Communication and information exchange for professional development or to maintain knowledge or skills;
   c. Activities involving public policy associations, government advisory agencies, or standards activities; and
   d. Communication for administrative purposes.

## B. Prohibited Usage

Users shall not use DJS-issued technology for:

1. Any illegal or unethical purposes;
2. Downloading or installing any programs;
3. Engaging in "chat room" conversations that are non-business related;
4. Completing any communication that does not accurately indicate the true authorized originator and recipient of DJS email communications;
5. Attempting to gain access to secure web sites or information by bypassing the site's security measures (commonly known as “hacking”);
6. Creating or transmitting threatening, defamatory, fraudulent, annoying, harassing or otherwise inappropriate messages, even as a prank;
7. Downloading or streaming radio broadcasts, music, videos, or voice, and large graphic files;
8. Engaging in any illegal or wrongful conduct, including communications violating any laws or regulations, copyrights, patent protections, license agreements, or other intellectual property rights of third parties;
9. Intentionally interfering with or disrupting network users, services, or equipment;
10. Private or personal for-profit activities such as consulting for pay, sale of goods, charity fundraising or solicitation of non-state business;
11. Sending chain letters, spam, letter bombs, advertisements, or commercial solicitations;
12. Viewing or attempting to access prohibited images and sites where any minors (as defined in state or federal laws) are inappropriately depicted including, but not limited to, any sexual depiction, or

graphic images of violence against youth or demeaning/dehumanizing of youth; such actions shall be grounds for immediate termination from the Department and the user may be subject to criminal proceedings;

13. Viewing or emailing pornographic or sexually explicit materials;
14. Playing computer games or gambling;
15. Mass mailing of personal or non-business related announcements unless approved for publication by the DJS Chief Information Officer;
16. Granting any unauthorized person access to the DJS email systems; granting access to another user's electronic mailbox, or retrieving, reading, copying, or altering the contents of another user's mailbox without first obtaining the user's permission;
17. Saving password information locally when prompted for system authentication;
18. Forging or sending forged emails or attachments;
19. Using a wireless technology or telecommunications device while operating a vehicle except when provided with "hands free" technology, (*Note: phone calls without a headset, texting, and using laptops in vehicles, etc. are prohibited by state law*);
20. Connecting to unsecured public Wi-Fi networks (such as Starbucks, Dunkin' Donuts, book stores, hotels, airports); and
21. Using the internet for non-business related purposes in excess of 30 minutes per day.

**C. Reporting of Prohibited Usage**

1. Each user shall report any employee for prohibited usage of email and the internet to the employee's supervisor.
2. The supervisor shall investigate, confirm any prohibited usage, and impose the appropriate disciplinary action.
3. The supervisor shall report any confirmed prohibited usage to
   a. their Regional Director, Facility Superintendent, or if applicable, their Deputy Secretary, and
   b. the Office of the Inspector General (OIG).

## VIII. RIGHT TO MONITOR

A. DJS reserves the right to review, intercept, and monitor any electronic communication including users' phone calls or internet activity through the Department's communication systems and disclose the activities to Executive Staff and/or the OIG.

B. All emails originated or received by DJS systems or accounts are subject to disclosure for public information act requests according to MD Annotated Code, Cts. And Jud. Proc. §3-8A-27.

C. DJS reserves the right to seize a user's state-issued work station and equipment to evaluate it for inappropriate or illegal activity.

## IX. PRIVACY AND CONFIDENTIALITY

A. The use of passwords for security does not guarantee privacy. Messages and information transmitted and stored on DJS systems are not necessarily private. Even when a message or material is erased, it may still be possible to retrieve.

B. All external email messages that contain confidential information shall be encrypted or password protected, and forwarded with the following message attached: *"This electronic transmission may contain confidential or privileged information. If you believe that you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it. Thank you."*

## X. RECORDS MANAGEMENT

Locally stored files are not automatically saved to the DJS network; therefore, DJS users are responsible for regularly copying their working files and critical documents from their local hard drive (C: drive) to the DJS network (e.g., H: drive or other shared drive). DoIT Services will back up the network drives daily.

## XI. POLICY MANAGEMENT

The DJS Deputy CIO will ensure all DJS IT policies comply with existing MD DoIT policies and industry standards by participating on the DJS policy committee responsible for reviewing, revising and updating policies annually or as necessary.

## XII. FAILURE TO COMPLY

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

## XIII. POLICIES/DIRECTIVES RESCINDED

None

## XIV. POLICIES & FORMS REFERENCED

1. Mobile Devices and Services Statewide Policy
2. State of MD 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