



POLICY & PROCEDURE

SUBJECT: Data Security
NUMBER: IT-02-09
APPLICABLE TO: All DJS employees
EFFECTIVE DATE: September 2, 2009

APPROVED: /S/ signature on original
Donald W. DeVore, Secretary

1. 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. This policy was 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.

2. AUTHORITY

- a.** Annotated Code of Maryland, State Finance and Procurement Article, §3-401 through §3-413 and §3-701 through §3-705.
- b.** Annotated Code of Maryland, Human Services Article, §9-202, §9-203, §9-204, §9-221, §9-227, and §9-229.
- c.** Annotated Code of Maryland, Criminal Law Article, §7-302.
- d.** COMAR 14.18.04
- e.** Executive Order 01.01.1983.18.Maryland Department of Information Technology (DoIT)
 - 1) Security Roles and Responsibilities Standard and Network Security Standard
- f.** Maryland Department of General Services
 - 1) Records Management Manual (January, 1993)
 - 2) Inventory Control Manual
(<http://www.dgs.maryland.gov/overview/ISSSD.htm#inventory>)
- g.** Maryland State Department of Juvenile Services Policies
 - 1) Firewall Policy
 - 2) Virtual Private Network Policy
 - 3) Wireless Device Policy End of Life Cycle Policy
- h.** FIPS Pub 199 - Federal Information Processing Standards (February, 2004)
- i.** NIST (National Institute of Standards and Technology)
 - 1) SP800-30 Risk Management Guide for Information Technology
 - 2) SP800-41 Guidelines for Firewalls and Firewall Policies
 - 3) SP800-45 Guidelines for Electronic Mail Security

- 4) SP800-55 Security Metrics Guide for Information Technology Systems
- 5) SP800-100 - Information Security Handbook

3. **DEFINITIONS**

- a. *Accountability*: A system's ability to determine the actions and behavior of a single individual within a system and to identify that particular individual.
- b. *Computer systems*: Mainframes, minicomputers, data communications facilities, local area network (LANs) file servers, microcomputer network nodes, and standalone microcomputers (desktops or notebooks/portables).
- c. *Confidentiality*: A restriction from disclosure, intentionally, to unauthorized persons, processes or devices.
- d. *Employee*: Individual employed either full time or part time by DJS on a permanent or contractual basis.
- e. *Password*: An authorization code to gain access to system resources.
- f. *Portable storage devices*: Any device that allows for the transportation of information away from the originating computer.
- g. *Users*: DJS employees and staff from any entity, agency or organization that has entered into a contract, Intergovernmental Agreement (IGA) or Memorandum of Understanding (MOU) with DJS to access the DJS IT system.

4. **PROCEDURES**

- a. **Password Security**
 - (1) DJS supervisors will request access to the various IT supported applications and systems by submitting the IT System Access Request Form to the Help Desk where it will be processed.
 - (2) The IT unit will create an account for users and assign and approve access to the systems and services that the users will require to perform their respective job function.
 - (3) The IT Help Desk staff shall assist users with signing onto the systems(s) for the first time and changing their passwords to one that meets the Password Standards as defined by DoIT. These standards will be regularly reviewed by the IT Security Officer to ensure compliance with the DoIT Password Standards.
 - (4) IT unit managers will provide the Chief Information Officer (CIO) with administrative passwords to applications, network devices (routers, switches, firewalls, etc), workstations / laptops. These passwords must also be kept in the off-site storage as backups.
 - (5) When an employee leaves DJS service, the *Separation/Termination Procedure (Attachment 1)* must be followed with all documentation and sign-offs submitted to the Data Security Officer.
 - (6) All staff from organizations or agencies who require access to the DJS IT system must complete and abide by the procedures established by the following agreements:
 - a. Confidentiality Agreement for Individuals or Confidentiality Agreement for Organizations;
 - b. DJS Electronic Mail, Internet and Intranet use policy; and

c. IT System Access Request Form.

b. Workstations and Laptops

- (1) The IT unit is responsible for the procurement, installation, support, replacement and disposal of all IT related devices.
- (2) The IT unit will provide all DJS employees with the equipment needed to perform their job duties.
- (3) Workstations and laptops will be set up with virus protection software that will be configured to receive the current virus definition updates from the network.
- (4) Laptop users will need to report to a DJS office to connect to the network for the updates at least monthly.
- (6) Only authorized and properly licensed software packages that are installed by an IT technician can be used on State microcomputer equipment.
- (7) The use of unauthorized or improperly licensed software and programs is strictly forbidden.
- (8) Workstations and laptops will be configured to prompt the user for a logon ID and password before accessing the desktop.
- (9) A password protected screen saver should be activated if the workstation or laptop is left idle for forty-five (45) minutes.
- (10) Users of DJS IT systems are responsible for reporting hardware and software problems to the IT Help Desk.

c. Wireless Communications Devices

- (1) Wireless communications devices are requested by completing and submitting Appendix 2 (*Request for Wireless Technology Equipment*) from the Wireless Technology Policy to the DJS IT unit.
- (2) The Deputy CIO of Telecommunications will review the application and either approve or disapprove it.
- (3) DJS employees are held responsible for the terms of the Wireless Technology Policy and must sign the receipt of the policy. The Property Release form must be signed upon receipt of the equipment.
- (4) DJS employees must return all devices to the IT unit upon separation from DJS services.

d. Portable Storage Devices

- (1) The use of portable storage devices is limited to the IT Technical Support staff.
- (2) Technical staff must store removable storage devices containing software and files in a locked cabinet.

e. Personally owned devices

- (1) Devices that are the property of DJS will be installed by an IT Technician.
- (2) Non-DJS equipment is prohibited from connecting to the DJS network.

f. Physical Security

- (1) All DJS data centers must be secured. A list of DJS employees with

- access to data centers must be maintained by the DJS Security Officer.
- (2) The Building Access systems must be installed as described in a secured location with UPS backups and adequate ventilation. The server must have a method of performing backups to an external device that is stored off-site.
 - (4) Access to all data centers is restricted to IT approved staff only.
 - (5) All data centers shall have devices installed to protect the data center from known vulnerabilities including fire protection, water/flood protection, and electrical failure. These devices must alert the DJS IT Network manager and the IT Help Desk in the event of a network related problem or failure and log the network status to a central location.
 - (6) Access to closets containing IT infrastructure devices should be secured where possible. Only IT- approved personnel should have access to the equipment.
 - (7) Wiring closets and equipment closets must be equipped with adequate ventilation, dedicated electrical circuit (where possible) and backup power. All equipment shall have the capability of notifying the IT unit Help Desk and Network Manager when a network related problem or failure occurs.
 - (10) IT unit manager or designee must approve the installation of all IT and telecommunication devices.
 - (12) When left unattended, workstations or laptop computers should be either turned off or locked.
 - (12) DJS employees are responsible for reporting to the IT Help Desk equipment that has been stolen, vandalized or in need of repair.

g. Network Security

- (1) The DJS IT unit will ensure the availability of remote access to the DJS network system to all DJS employees.
- (2) The DJS IT unit will ensure the security of all its network system enterprise by implementing all DoIT network security policies and guidelines.
- (3) The DJS IT unit will ensure the security of all its network system enterprise by implementing the following DJS approved polices:
 - a. DJS Firewall Security policy (IT-01-09).
 - b. DJS Wireless Technology policy (IT-01-05);
 - c. DJS Electronic mail, Internet and Intranet use policy (IT-01-08);
and
 - d. DJS Virtual Private Network (VPN) policy (IT-02-08).
- (4) The DJS IT unit will ensure that the operating system for all network equipment has the most current relevant patches, fixes and service packs installed.

h. Asset Control Standards

- (1) The IT unit is responsible for the purchase, installation, maintenance, support and disposal of all IT-related equipment in compliance with the Maryland Department of General Services Inventory Control Manual and the DJS End of Life Cycle Policy.
- (2) The IT unit is responsible for maintaining an Asset Management Database

that tracks all IT equipment from purchase to disposal.

- (3) Each regional IT technician is responsible for Asset Control in their assigned region. Each regional IT technician will be responsible for:
 - a. Ensuring that all documentation regarding the installation, transfer, repair and disposition of all IT equipment is completed with signatures and dates; these documents are to be retained in electronic format with the hardcopy filed in a secured filing cabinet;
 - b. Ensuring that all IT equipment is properly labeled with DJS Property Inventory stickers;
 - c. Updating the Asset Control database with the inventory information; and
 - d. Ensuring that all equipment is properly disposed.
- (4) The IT unit will maintain proof of all software and licensing agreements

i. Records Management

- (1) The IT unit will maintain electronic documents and remove records according to the records retention schedule established by the DJS unit that created the record.
- (3) The IT unit will transfer permanent electronic data according to the unit's record retention schedule to the Maryland State Archives in accordance with COMAR 14.18.04.

j. Policy Management

- (1) The Data Security Officer will ensure all IT policies are in compliance with existing MD DoIT and industry standards by conducting an annual review of policies and updating when needed.

k. Disaster Recovery Plan

- (1) The IT unit will implement an approved IT Disaster Recovery Plan. This plan contains critical documentation and procedures that are needed to recover IT Systems in the event of a disaster.

5. DIRECTIVES/POLICIES AFFECTED

- a. Directives/Policies Rescinded - **None**
- b. Directives Referenced:
 - a. DJS Firewall Security policy (IT-01-09).
 - b. DJS Wireless Technology policy (IT-01-05);
 - c. DJS Electronic mail, Internet and Intranet use policy (IT-01-08); and
 - d. DJS Virtual Private Network (VPN) policy (IT-02-08).

6. LOCAL IMPLEMENTING PROCEDURES REQUIRED

Yes

7. FAILURE TO COMPLY

Failure to comply with a Secretary's Policy and Procedure shall be grounds for disciplinary action up to and including termination of employment.

Appendices –

1. Equipment Property Release form (policy\disposal)
2. Separation/Termination Procedure