FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Information Technology Compliance and Enforcement Procedures

Related Policy: FDJJ - 1240

I. DEFINITIONS

Access Points - A device or medium (such as the Internet, public phone line, wireless carriers, or other external connectivity) which allows access to the Department's network.

Central Communication Center – A unit located in DJJ Headquarters that is charged with receiving reports regarding incidents from all DJJ and Provider facilities, programs, offices, or sites operated by DJJ, a provider, or grantee (FDJJ 8000).

Chief Of Management Information Services (MIS) – DJJ staff member responsible for overseeing the MIS Bureau within DJJ; also referred to as the Chief Information Officer (CIO).

Computer Security Incident Response Team (CSIRT) – A group of DJJ staff who are responsible for establishing policies and procedures (FDJJ 1250) for responding to suspected computer security incidents

Confidential Information and/or Confidential Data – Information and/or data that is exempted from disclosure requirements under the provisions of applicable state and federal law, and includes ensuring that information and/or data which is only accessible to authorized users.

Data Integrity Officer (DIO) –DJJ staff responsible for assisting users with maintaining integrity of the data entered in the Juvenile Justice Information System (JJIS), creating JJIS user accounts and assisting with training in use of JJIS.

Firewall – A Computer hardware device used to prevent unauthorized access to internal computer networks. The device also prevents unauthorized outgoing traffic.

Information Owner – The executive business manager responsible for the collection, maintenance, and dissemination of an information set.

Information Resources – The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Information Set – A collection of Department-owned data that is specific to a defined function and or application.

Information Technology (IT) Professional - A member of the Management of Information Systems (MIS) team.

Malware – Any type of malicious software (malware) that is designed to damage or steal information and/or act in an unexpected or undesirable manner. Malware includes but is not limited to rootkits, spyware, Trojan horses, and viruses. Also referred to as malicious code.

Malware Protection – Computer software or hardware devices used to protect computer networks from vulnerabilities, including but not limited to worms, viruses, Trojans spyware and rootkits.

Personal Password – A password that is created and known by only one person and is used to authenticate that person's identity when they access the Department's network.

Provider– Any non-DJJ entity that provides juvenile services under an agreement with the Department

Provider JJIS Access User Agreement – A signed acknowledgement that the provider understands his or her responsibility and is aware of the consequences if the Department of Juvenile Justice policies/guidelines are not followed.

Scanning – Monitoring IT infrastructure (e.g. networks, routers, ports, etc) to detect, assess and correct potential security vulnerabilities.

Sniffing – The process of using an IT tool to capture network data.

User – A person authorized to access and utilize the Department's Information Resources with their personal password.

II. STANDARDS/PROCEDURES

A. General Compliance:

The Department's network shall be designed at minimum to require the following Information System principles:

1. All Department computer users shall have unique user accounts.
2. User accounts must be authenticated at a minimum by a password.
3. Password length of eight (8) or more alphanumeric characters must be specified and implemented on all network user accounts.
4. Password expiration must be set on network accounts. Any exceptions must be approved by the Department's Chief Information Officer.
5. Password-protected screensavers with the automatic activation feature shall be set at a minimun of fifteen (15) minutes.
6. The agency must ensure accounts with administrative rights are created, maintained, monitored and removed in a manner that protects information technology resources.
7. Administrative account activities shall be traceable to an individual.
8. Acccess to information technology resources shall be granted based on the principles of "least privilege" and "need to know."
9. Only Department-approved software shall be installed on agency computers.

10. The Department shall use software and hardware tools and devices to monitor and protect the integrity of the Department's data and technological infrastructure from known vulnerabilities and unauthorized access (e.g. utilizing a firewall and malware protection tools, along with monitoring, sniffing and scanning the department's network).

11. The Department shall implement controls to ensure access to information technology infrastructure resources is restricted to authorized users and uses.

12. The Department shall ensure separation of duties so that no individual has the ability to control an entire process.

13. The application development team shall implement appropriate security controls when developing applications.

14. The Department shall implement and follow procedures to establish accountability when accessing and/or modifying confidential applications and data.

15. The Department shall monitor for unauthorized access points. Unauthorized access points connected to the Department's network must be removed immediately. The discovery of unauthorized access points shall be reported to the Departments' Information Security Manager.

16. Department information technology resources shall not be used for personal profit, benefit, or gain.

17. Personal use of the Department's Information Technology resources shall not violate any aspects of this or other applicable DJJ policies or local, state, and federal laws.

18. When authorized by the applicable retention schedule, confidential information, regardless of media type, will be destroyed.

B. General Enforcement:

Information technology employees shall be granted access to agency information technology resources based on the principles of "least privilege" and "need to know."

1. Periodic audits authorized by the Department's Chief Information Officer and/or the Inspector General will be performed to determine compliance.

2. Department employees shall be held accountable for their account activities.

3. Department employees are responsible for safeguarding their passwords and other authentication methods.

4. Department employees shall not share their passwords, personal identification numbers, or other devices used for identification and authentication purposes.

5. Department employees shall immediately report suspected account compromises according to agency's C-SIRT and CCC incident reporting procedures.

6. Department employees shall not disable, alter, or circumvent agency security measures.

7. Monitoring, sniffing, and related security activities shall be performed by Department employees based on their job duties and responsibilities with the explicit consent of the Department's Chief Information Officer and/or the Inspector General.

8. Department computer users shall not circumvent agency computer security measures.

9. Department information technology resources shall not be used for any activity which adversely affects the availability, confidentiality and/or integrity of the Department or its data or resources.

10. Privately-owned devices (e.g., MP3 players, thumb drives, printers, routers) shall not be connected to Department resources without prior, documented authorization and approval from the Department's CIO.

C. Mobile Devices:

1. User authentication shall be required on all mobile computing devices, where technology permits.

2. Encryption shall be required on all mobile devices, where technology permits.

3. Mobile computing devices shall require user authentication.

4. Mobile computing devices shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minute increments.

D. Violations:

1. Violations of this policy or any of the Department's other Information Resource policies may result in revocation of user access, disciplinary action, up to and including immediate dismissal, and/or potential criminal prosecution under Chapter 815, Florida Statutes, or other applicable law.

III. RESPONSIBILITY AND DUTIES

A. Department Head and Chief Information Officer shall ensure:

1. Every staff member, contractor, vendor or provider reads this policy prior to using the Department's information resources and acknowledges doing so by signing a Statement of Understanding (Attachment 1), which will be appropriately filed in each official personnel file (DJJ employees), appropriate contractor's file or authorized access file. Suggest all receipts for the policy be kept by personnel since it could be a subject of taking away access.

2. Information technology professionals enforce portions of this policy within the scope of their capability by establishing policies, generated reports and using various tools and techniques to protect the integrity of the Department's data and technological infrastructure (e.g. utilizing a firewall and malware protection tools, along with monitoring, sniffing and scanning the department's network).

3. Periodic audits are performed for compliance and enforcement.

B. Agency computer users:

1. Shall ensure that their passwords are strong and in compliance with the implementing procedures of this policy.
2. Shall be held accountable for all actions performed under his/her assigned username and password.
3. Shall be responsible for safeguarding their passwords.
4. Shall not attempt to use another employee's username or password under any circumstances.
5. Shall not attempt to circumvent the Department's security measures by any means.
6. Shall contact their immediate supervisor or local DIO if their account needs to be reset. Direct account lockouts to the JJIS Help Desk

C. Information Owners

1. Department information owners shall be responsible for classifying information as confidential.
2. Information owners shall be responsible for authorizing access to information.
3. Access to confidential data shall be controlled by applicable user agreement forms and specific system access permissions.

D. Contractors

1. The Department shall establish procedures to ensure contracts and agreements involving the use of information technology resources guarantee contractor compliance with the agency information technology security policies and procedures.

E. Providers

1. Each provider (individual users) must read and sign the Provider JJIS Access User Agreement acknowledging his or her understanding of applicable Department policies.
2. Each provider (entity providing services to the Department) must execute compliance with Department security policies, prior to accessing the Department's network and/or information technology resources.

IV. ATTACHMENTS

Statement of Understanding

Provider JJIS Access User Agreement