FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Internet Access and Use Procedures

Related Policy: FDJJ – 1205.40

I. DEFINITIONS

Chief Information Officer (CIO) – DJJ staff responsible for overseeing the Bureau of Information Technology within DJJ**.**

Firewall – Software residing on the DJJ IT gateway controlling the flow of information through the Internet and Intranet.

Information Security Manager (ISM) – The individual appointed by the Secretary, or his/her designee, to administer the Department's information security program in accordance with s.228.318, F.S. This individual serves as the Department's internal and external point of contact for all information security matters.

Internet Gateway – The physical and logical connections provided by DJJ between the personal computer and the Internet.

Internet Services – Services accessed through the Internet Gateway including, but not limited to, Web Browsers, internet e-mail, FTP, Telnet, and newsgroups. Services such as America On Line (AOL), gmail and Yahoo are also covered by this reference.

Internet User Agreement – A signed acknowledgment that the employee understands his or her responsibility and is aware of the consequences if the Internet policy is not followed.

Intranet – The DJJ internal network that allows employees and other authorized users to access Department related news, resources and information.

Resources – As defined in this policy, computer hardware, software, licenses, software developers, and technical support.

Streaming Media (Service) – Multimedia (e.g. video, audio) that is constantly received by and presented to an end-user while being delivered by a provider.

II. STANDARDS/PROCEDURES

The scope of this policy includes all Department personnel, and employees of providers, contractors, vendors, and third-party organizations utilizing the Department's Internet services.

A. Establishment of Internet Access and Use:

1. The Bureau of Information Technology (IT) shall provide the software necessary to access the DJJ Internet. Use of Internet access software other than that supplied or approved by DJJ IT is prohibited.

2. DJJ Internet Services must go through the DJJ provided Internet Gateway unless approved by the Chief Information Officer.

B. Use and Revocation of Internet Access:

1. Department employees or employees of providers, contractors, and third-party organizations shall not use DJJ Internet services to transmit any proprietary or sensitive (confidential) data, including data that is confidential pursuant to sections 984.06 and 985.04 of the Florida Statutes.

2. Access to the DJJ Internet Services may be revoked, with or without notice, if a Department employee or an employee of providers, contractors, and third-party organizations using the Department's Internet service violates this policy or the "Internet User Agreement."

3. Violation of any provision of this policy by Department employees or employees of providers, contractors, and third-party organizations using the Department's Internet service is cause for disciplinary action up to and including dismissal, civil fines or tort action, and/or criminal penalties under applicable state and federal regulations and laws.

4. Supervisors may request the revocation of an employee's access to the DJJ Internet by submitting a written request to the applicable Bureau Chief or Departmental/Regional Director.

5. If approved, the Bureau Chief or Departmental/Regional Director shall forward the request to the Chief Information Officer and copy the Information Security Manager for revocation of Internet access. Access shall remain revoked until otherwise requested by the employee's Bureau Chief or Departmental/Regional Director.

C. Unacceptable Internet Access and Use:

1. Unacceptable and inappropriate use of the Internet includes, but is not limited to, accessing the following types of non work-related Internet sites or conducting the following types of activities:

   a. Gambling or accessing gambling websites.

   b. Accessing or possessing pornographic, sexually explicit, or sexually oriented material in the workplace or with state equipment. This includes viewing, downloading, copying, faxing, sharing videos, photographs, music, and written material.

   c. Accessing or possessing hate literature, illegal drugs, illegal drug paraphernalia, weapons, hacker websites, gang-related material, or violent material. This includes offensive material concerning sex, race, national origin, religion, age, disability or other characteristics or special classes protected by law, regardless of intent.

   d. Accessing social networking, streaming services, chat rooms, blogs, message boards, political groups, singles clubs, or dating services.

   e. Using state equipment or resources to represent, express opinions, or otherwise make statements on behalf of the Department or any unit of the agency without authorization to do so.

f. Using a state computer to make personal purchases with a state e-mail or to store personal files or using a Department office's physical address for shipping or billing purposes.

g. Conducting any activity that is unlawful or violates Department policy or federal, state, or local laws. This includes using state equipment for commercial purposes or for personal financial gain.

D. Exception Request/Notification: Work-Related Access to Unacceptable Internet Sites:

1. If it is necessary for work-related purposes to access the aforementioned types of websites, a written request/notification is required prior to ***or*** immediately after the site has been accessed

   The following scenarios warrant the submission of a written request or notification to the Chief Information Officer:

   a. Employees needing to access websites currently blocked for work-related purposes must submit a written request to their Manager/Supervisor requesting permission to access the site(s) in question.

   b. Employees needing to access websites that fall into the aforementioned unacceptable categories for work-related purposes must submit a written request to their Manager/Supervisor requesting permission to access the site(s) in question.

   c. Employees who, for work-related purposes, have accessed a website that falls into the aforementioned unacceptable categories must submit a written notification to their Manager/Supervisor immediately after the site has been accessed.

   d. Managers/Supervisors of staff needing to access websites currently blocked for work-related purposes must forward a written request on behalf of their employees to the Chief Information Officer to facilitate staff access.

   e. Managers/Supervisors of staff needing to access websites that fall into the aforementioned unacceptable categories for work-related purposes must forward (on behalf of their employees) and receive prior approval from the Chief Information Officer.

   f. Managers/Supervisors of staff who, for work-related purposes, have accessed a website that falls into the aforementioned unacceptable categories must forward (on behalf of their employees) a written notification to the Chief Information Officer immediately after the site has been accessed.

   g. Managers/Supervisors of staff who, for work-related purposes, have continued past the Department's web filtering application to access a website that falls into the aforementioned unacceptable categories, must forward (on behalf of their employees) a written notification to the Chief Information Officer immediately after the site has been accessed.

E. Limited, Non-Commercial, Personal Use:

1. Employees are permitted limited personal use of the Department's Internet services only during non-work/unpaid hours (e.g., before and after scheduled work hours and during allotted lunch periods), and only if such use does not involve additional expense to the agency, result in loss of productivity or otherwise interfere with official state business.

2. Personal use shall not cause or result in the congestion, delay, or disruption of service to any private or government organizations, systems or equipment.

3. Personal use of the Department's Internet services must not violate any aspects of this or other applicable DJJ, local, state, and federal Internet policies. Please reference the **Unacceptable Internet Access and Use** portion of these procedures for additional details.

F. Violations:

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

III. RESPONSIBILITY AND DUTIES

A. Chief Information Officer

1. Shall ensure a comprehensive risk management program is devised and implemented assuring Internet security risks are identified, considered and mitigated through development of cost effective security controls. The risk management program will include a service access policy defining those services that will be allowed or explicitly denied from the restricted network, how these services will be used, and the conditions for exception to this policy.

2. Shall ensure Internet contingency plans are developed, tested, and maintained. The risk involved with using the Internet makes it essential that plans and procedures be prepared and maintained to:

   a. Minimize the damage and disruption caused by undesirable events; and

   b. Provide for the continued performance of essential system functions and services.

3. Shall ensure audit trails are developed, installed, maintained, and regularly reviewed for unusual system activity.

4. Shall review and approve/disapprove Exception Requests (reference Section II, C) from Managers and Supervisors.

5. Shall notify Managers/Supervisors and facilitate applicable access to websites that fall into the aforementioned unacceptable categories based on his/her approval/disapproval of Exception Requests.

B. Information Security Manager

1. Shall be responsible for implementing the Department of Juvenile Justice Internet policy.
2. Shall be responsible for working closely with the DJJ Network administrator to:
   a. develop audit trails;
   b. review and monitor audit trails on the Internet connection; and
   c. monitor activity on the use of hosts and associated subnets.
3. Shall report any findings of misuse to the Chief Information Officer.

C. DJJ Network Administrator

1. Shall be responsible for working closely with the Information Security Manager to:
   a. develop audit trails;
   b. review and monitor audit trails on the Internet connection; and
   c. monitor activity on the use of hosts and associated subnets.

D. Department Employees and Other Applicable Users

1. Access to the Department's Internet services is reserved for Department employees and employees of providers, contractors, and third-party organizations using the Department's Internet service.
2. Department employees and employees of providers, contractors, and third-party organizations using the Department's Internet service shall sign an Internet User Agreement form stating they have read and understand the DJJ Internet Access and Use Policy.
   a. Department employees shall send their completed and signed, original Internet User Agreement form to the Bureau of Personnel to be filed in their official personnel file.
   b. Non-Department employees shall send their completed and signed original Internet user Agreement to their Contract/Grant Manager for filing and reference.
3. Shall comply with this policy and applicable local, state, and federal Internet policies.
4. Shall report anyone suspected of misuse or attempting the misuse of DJJ Information technology resources to the Information Security Manager, or the Chief Information Officer.
5. Shall immediately report any websites that fall into the aforementioned unacceptable categories (reference page 2, section II, B, 1, a-d for details) that have not been filtered by the Department's web filtering application to the Information Security Manager, or the Chief Information Officer.

IV. ATTACHMENTS

Attachment 1 - Internet User Agreement