FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: User Password Procedures

Related Policy: FDJJ - 1225

I. DEFINITIONS

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

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 Technology Professional – A member of the Information Technology team.

Personal Password – A password created and known by only one person and is used to authenticate that person's identity.

User – Person employed by the Florida Department of Juvenile Justice, including permanent employees (SES, CS, SMS) as well as temporary staff ***or*** employees of third party organizations using the Department's Information Resources who are authorized to access and utilize the Department's Information Resources for official business with a personal password.

II. STANDARDS/PROCEDURES

A. General Password Construction:

1. Passwords are used for various purposes. Some of the more common uses include: user-level accounts, E-mail accounts, web accounts, and other applications (e.g. JJIS). Everyone should be aware of how to select strong passwords. The following explains how to create a strong, desirable password.

2. Strong passwords have the following desirable characteristics:
   a. Are **eight (8)** or more alphanumeric characters.
   b. Contain both upper and lower case characters (e.g., a-z, A-Z).
   c. Have digits and punctuation characters, as well as letters (e.g. 0-9, !@#$%^&*(/?);.

3. Weak passwords have the following poor, undesirable characteristics:
   a. The password contains less than eight (8) characters.
   b. The password is a word found in a dictionary (English or foreign).
   c. Are words in any language, slang, dialect, or jargon.
   d. Are based on personal information, such as names, pets, birthdays, address, family, phone number, etc.
   e. The password is a common usage word, such as:
      (1) Computer terms and names, commands, sites, companies, hardware, or software.

(2) Acronym or slang for a college or team, such as: "FSU," "Gator," "Nole," or any derivation of this.

f. Any of the above spelled backwards;
g. Any of the above preceded or followed by a digit (e.g. 1secret, secret1); or
h. Word or number patterns like **aabbcc**, **qwerty**, **zyxwvuts, 12321**, etc.

B. General Password Standards:

1. Passwords shall be changed at least every 90 days.

2. Passwords should be encrypted or secured by other means when delivered electronically.

3. Passwords shall meet strong General Password Construction criteria as stated above.

4. Passwords shall be kept confidential.

5. A supervisor or co-worker may not, for any reason, ask anyone to divulge his or her password.

6. If another person knows a user's password, it is the DJJ staff and contract provider's staff responsibility to change their password immediately.

7. Passwords shall never be written, recorded or stored by any means.

8. DJJ staff and contracted provider's staff are encouraged to create strong passwords that can be easily remembered. One way to do this is to create passwords based on a song title, affirmation, or other phrase. For example, the phrase might be: 'This is one way to remember" and the passwords could be **Tis1w2R**, or some variation of this phrase. (NOTE: Do not use any of the examples given as passwords).

C. Password Protection Standards:

1. Passwords for DJJ staff and contracted provider's staff to DJJ accounts shall be different from other non-DJJ access passwords (e.g., personal ISP account, benefits, etc). Where possible, do not use the same password for various State accesses needs. For example, select one password *for* the DJJ network and separate passwords to access other computer applications, programs, and/or databases.

2. Passwords shall not be shared with anyone including administrative assistants, information technology professionals or supervisors. All passwords are to be treated as sensitive confidential information.

3. Individual user accounts for DJJ staff and contracted provider's staff shall each have a unique user ID and password.

4. Passwords for DJJ staff and contracted provider's staff shall not be stored in readable format on any system.

5. If an account or password is, or is suspected to be compromised, DJJ staff and contracted provider's staff shall report the incident to their supervisor.

6. Any exceptions to the aforementioned standards must be pre-approved by the Department's Chief Information Officer.

III. RESPONSIBILITY AND DUTIES

A. Agency Head and Chief Information Officer shall ensure:

1. Every DJJ employee and employees of providers, contractor or vendors, utilizing DJJ IT resources read this policy prior to using the Department's Information Resources and acknowledges so doing by signing a Statement of Understanding (Attachment 1), which will be appropriately filed in each employee's official personnel file, appropriate provider, contractor or vendor's files.

2. Information Technology Professionals enforce the parts of this policy that is within the scope of their capability (e.g., system generated policies).

3. Periodic audits are performed for compliance.

B. Agency Computer Users:

1. Shall ensure their passwords are strong and in compliance with the implementing procedures of this policy.

2. Shall be held accountable for their account activities.

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 agency computer security measures by any means.

6. Shall contact their immediate supervisor or local DIO if their account is locked or needs to be reset.

7. Shall keep their account active by using their username and password to log into the Department's network at least once every thirty days.

C. Supervisors/DIO:

1. Shall contact the Help Desk to request password resets on behalf of their employees and/or the provider staff they manage. Temporary passwords will be sent electronically to the requesting Supervisor/DIO, which will require the user to change the temporary password immediately.

2. Shall ensure employees under their supervision (or the provider staff they manage) keep their accounts active by using their username and password to log into the Department's network at least once every thirty days.

IV. ATTACHMENTS

Statement of Understanding (Attachment 1)