FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Network User Accounts Procedures

Related Policy: FDJJ - 1205.50

I. DEFINITIONS

Authorized Access - That which relates to an employee's duties at the Department of Juvenile Justice (DJJ) and for whom authorized written approval has been given.

Chief of Management Information Systems (MIS) – DJJ staff responsible for overseeing the Bureau of MIS within DJJ, also referred to as the Chief Information Officer (CIO).

Computer Resources - Computer hardware, software, licenses, applications and technical support (Management Information System staff).

E-mail – Electronic mail messages sent to users on the local or wide area network or to anyone on the Internet who has an e-mail account.

Information Security Manager (ISM) – An individual appointed by the Secretary or his 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.

User Account or Network account - The DJJ method of granting a user authorized access to secured file servers and networked printers.

II. STANDARDS/PROCEDURES

A. Granting Access to DJJ Information Systems:

1. To obtain a network user account for a new DJJ employee, the employee's supervisor shall submit the **NETWORK USER ACCOUNT REQUEST FORM** to the appropriate Management Information System (MIS) employee (e.g., Regional Leader, local MIS staff).

2. This form shall include the signatures of the employee, his or her supervisor, and MIS staff creating the account.

3. After the account is created, the MIS staff will complete the form and send the original form to the Information Security Manager.

4. The Information Security Manager shall keep these files in accordance with applicable records management laws, rules and policies.

5. Standard account creation shall consist of personal E-mail and network accounts.

6. Each account shall identify the authorized individual for whom it was created. DJJ shall not create accounts that are non-specific or generic in nature.

7. Administrative permissions shall be requested in writing and approved by the Chief of Management Information Systems (CIO) before permissions are granted.

8. Administrative permissions shall only be granted when needed to perform specific duties, which cannot be done by any other access type.

9. The granting of and removal of administrative permissions shall be monitored and tracked in the form of a spreadsheet and/or database, which will be maintained, by the CIO and/or ISM.

10. All exceptions to this standard for the creation of accounts shall be pre-approved by the Department's Chief Information Officer/MIS Bureau Chief.

B. Terminating Access to DJJ Information Systems:

1. To terminate an employee's network user account, the immediate supervisor or Provider Director or designee shall complete and submit a **USER ACCOUNT DELETION FORM** to the appropriate MIS employee (e.g., Regional Leader, local MIS staff) within twenty-four (24) hours of an employees' termination of employment.

2. MIS staff shall disable accounts within one business day of receiving a **USER ACCOUNT DELETION FORM** from the Supervisors of the terminated employees.

3. DJJ Supervisors shall request access to the departing employee's network files and/or E-mail messages via the **USER ACCOUNT DELETION FORM** *before* the account is permanently deleted.

4. Accounts shall remain disabled for 30 days, at which time MIS will permanently delete the account.

5. Following permanent deletion, the MIS staff deleting the account shall send the original **USER ACCOUNT DELETION FORM** to the Information Security Manager.

6. The Information Security Manager shall keep these files in accordance with applicable records management laws, rules and policies.

7. All exceptions to this standard of terminating accounts shall be pre-approved by the Department's Chief Information Officer/MIS Bureau Chief.

C. Auditing User Accounts:

1. Each month, MIS Regional Leaders shall obtain from Personnel a report of DJJ terminations and new hires. This report shall be used to conduct an audit of user accounts.

2. The MIS Regional Leaders shall identify individuals with user accounts who are listed on the personnel termination report. Action shall be taken to verify that these individuals are

authorized, active contractors or employees of DJJ. If active status cannot be verified, the user account shall be terminated.

3. The results of this audit shall be submitted on a quarterly basis by the MIS Regional Leaders to the Chief Information Officer with a copy to the Information Security Manager.

D. Other Network User Account Requirements:

1. All new account requests shall be made to Management Information System by delivering the **NETWORK USER ACCOUNT REQUEST FORM** to the supporting MIS staff at least one week prior to the requested account activation date.

2. MIS staff shall initially set passwords for new accounts. It shall be the employee's responsibility to determine a proper password for subsequent changes (to their password) in accordance with the Department's Password Policy (FDJJ – 1225). The initial password will expire, and must be changed after the first login.

3. Passwords shall expire every 90 days. It is the user's responsibility to reset his/her password.

4. Network user accounts shall have a minimum password length of eight (8) characters.

5. Valid network account owners shall log into the DJJ network (using their username and password) at least once every thirty (30) days to avoid account deletion due to non-activity.

6. When a user needs their password reset, their supervisor (or supervisor's designee) shall send an E-mail to the MIS Help Desk requesting the password change.

7. The owner of the account for which the password has been reset shall not be allowed to use a recent password in setting up a new password. The system will record the previous twenty-four (24) passwords used and not accept them as a valid entry.

8. After a pre-determined number of unsuccessful logon attempts, the network user account shall be locked.

9. When a network user is locked out of their account, the user must call the MIS Help Desk and request their account be unlocked.

10. An employee's passwords shall be kept confidential. A supervisor or co-worker may not, for any reason, request an employee to divulge their passwords. If another person knows an employee's password, it is the employee's responsibility to change it.

11. An employee's current supervisor shall request remote access to the DJJ network. This request must be in the form of a written memorandum to the MIS Bureau Chief. The request shall include documentation that explains why remote access is required for this employee. After review and approval by the MIS Bureau Chief, MIS will establish remote access and notify the employee and their current supervisor.

12. Staff shall maintain different passwords for their DJJ and non-DJJ accounts, personal accounts, and other State of Florida accounts, if any.

13. Staff shall not modify (i.e., add, remove, change) the security permissions for file folders on the DJJ Network without prior written approval from his/her manager.

14. Any exceptions to the aforementioned standards shall be pre-approved by the Department's Chief Information Officer/MIS Bureau Chief.

E. Provider Network Access:

1. A **NETWORK USER ACCOUNT REQUEST FORM** must be completed for provider staff working in DJJ owned/operated facilities that need access to the DJJ network.

2. The form shall be completed and signed by the applicant provider staff and the Provider Director or Designee (authorizing supervisor signature).

3. The Provider Director or Designee shall submit the completed form to the applicable DJJ staff (i.e. Contract/Grant Managers, etc.) for review, who will then submit the form to the appropriate Management Information System (MIS) employee (e.g., Regional Leader, local MIS staff) if access to the DJJ network is to be granted.

4. After creating the network account MIS will forward the original **NETWORK USER ACCOUNT REQUEST FORM** to the Information Security Manager.

5. The Information Security Manager shall keep these files in accordance with applicable records management laws, rules and policies.

6. Reference the Provider Access to Juvenile Justice Information System (JJIS) Policy and Procedures documents (**FDJJ - 1205.60**) for information on provider access to the Department's Juvenile Justice Information System (JJIS).Non-Active Network Accounts:

1. MIS will disable network accounts and move them to the "Stale Accounts" organizational unit in Active Directory after 30+ days of non-activity.

2. MIS Regional Leaders will send a Non Active Account e-mail notification to the immediate Manager/Supervisor in question to verify the validity of the account and the cause of non-activity.

3. Manager/Supervisor shall respond to MIS within 30 days of receiving the Non Active Account Notification.

4. If non-activity is due to military service or medical/administrative leave, MIS will notate the reason in the "description" field of Active Directory. A standard description (for example "Inactivity due to XXXXX" i.e. Military Duty, ADMIN, FMLA, etc.) will be used for listing the reason in the description field.

5. If the Manager/Supervisor does not respond within 30 days of receiving the Non Active Account Notification the accounts will be deleted after 90 days of non-activity.

6. All accounts—regardless of reasoning—will be deleted after 90 days (3 months) of non-activity.

7. If 90 days/3 months of non activity is due to an ongoing investigation, the accounts will be deleted ***but*** all applicable e-mail, shared folder documentation/data, and computer images will be saved in the form of a .pst file and/or DVD, as directed by the IG, if necessary—prior to account deletion.

8. If a network account is deleted due to non-activity, the user's Manager/Supervisor will have to submit a new Network User Access Agreement form for the person in question if he/she is in fact an active DJJ employee that needs to have network access.

III. RESPONSIBILITY AND DUTIES

A. DJJ Staff:

1. Each staff member shall be responsible for the use of network accounts and computers provided to them by DJJ, including data backup and password maintenance.

2. Network accounts shall only be used by the user to whom they are assigned to conduct and support DJJ and/or State of Florida business.

3. Network users shall sign off the system when he/she is finished accessing the desired information.

4. Network users shall choose passwords that are not easily guessed or deduced by others. (Number/order change only)

5. Non-MIS Departmental employees are prohibited from modifying (i.e., adding, removing, changing) the security permissions for file folders on the DJJ Network without prior written approval from his/her manager. (New)

6. Network users who suspect that their computers or network accounts have been compromised shall immediately change their passwords and report the suspected activity to Management Information Systems (MIS).

B. DJJ Supervisors:

1. Shall be responsible for obtaining a network account for employees under their direct supervision. All requests for network accounts shall be initiated via submission of a **NETWORK USER ACCOUNT REQUEST FORM.** The form must be received by MIS at least one week prior to account activation date.

2. Shall insist that staff under their supervision do not use another staff's network user account.

3. Shall not request disclosure of passwords to subordinates' accounts.

4. Shall be responsible for notifying supporting MIS staff within twenty-four (24) hours of employees' termination of employment with the Department. Notification shall be done via the **USER ACCOUNT DELETION FORM.**

5. Shall ensure that staff under their direct supervision log into the DJJ network at least once every thirty (30) days so that valid accounts are not disabled/deleted due to non-activity.

6. Shall be responsible for consulting with supporting MIS staff to periodically review the network and systems access privileges for employees under their direct supervision. Managers/Supervisors shall submit a Network User Account Request form and other applicable forms to MIS in order to modify the network and systems access privileges of their employees when necessary.

7. Shall be responsible for consulting with supporting MIS staff to periodically review the network and systems access privileges for employees under their direct supervision. Managers/Supervisors shall submit a Network User Account Request form and other applicable forms to MIS in order to modify the network and systems access privileges of their employees when necessary.

C. DJJ Providers:

1. Responsibilities and duties for DJJ Providers are defined in the Provider Access to Juvenile Justice Information System (JJIS) Policy and Procedures (FDJJ 1205.60).

2. Contractors, vendors or providers, and third parties who need access to the Department's information resources shall also be required to comply with Provider Access to Juvenile Justice Information System (JJIS) Policy and Procedures (FDJJ 1205.60).

D. MIS Staff:

1. MIS staff shall ensure prompt creation, auditing and deletion of network accounts.

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

IV. ATTACHMENTS

Attachment 1 - Network User Account Request Form

Attachment 2 - User Account Deletion Form