September 10, 2002

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NO. 02-03

TO: ALL JOB CORPS NATIONAL OFFICE SENIOR STAFF
ALL JOB CORPS REGIONAL DIRECTORS
ALL JOB CORPS CENTER DIRECTORS
ALL JOB CORPS CENTER OPERATORS
ALL NATIONAL TRAINING AND SUPPORT CONTRACTORS
ALL OUTREACH, ADMISSIONS AND CTS CONTRACTORS

FROM: RICHARD C. TRIGG
National Director
Office of Job Corps

SUBJECT: Network Accounts Management Requirements

1. Purpose. The purpose of this document is to notify Job Corps LAN/WAN users of procedural changes for managing all applications and Job Corps Novell network accounts.

2. Background. Application and Novell network accounts have been managed through a combination of helpdesk calls, email, fax, and recently, through the Job Corps Data Center (JCDC) Security Team. In order to ensure compliance with OIG security requirements and to provide greater accuracy in user ID reporting, the JCDC has developed new procedures for managing all user accounts.

3. Authorities. The procedures included in this document are in accordance with the following authorities:

- Computer Security Act of 1987 (Public Law 100-235)
- OIG audit accountability

4. Guidelines and Requirements. The JCDC will establish procedures to assist staff in acquiring accounts for the use of Job Corps systems and network resources. These procedures are in compliance with federal statutes and current agency and OIG security requirements.

All points of contact (POCs) for centers, OA, CTS and other users will be responsible for tracking and reporting the status of user accounts at their location. The JCDC will provide a

standard format for editing existing user account lists and a standard form for requesting new accounts. This policy applies to all Job Corps LAN-WAN users at the JCDC and at each Job Corps site. The Account Policy, Temporary Account Policy, and Password Policy are defined below:

a. Account Policy. User accounts and passwords should be set up using the following guidelines:

- Set up only one account on a system for each user.
- Delete or suspend accounts immediately when a user leaves Job Corps.

  Set up generic system accounts for system processes. Do not use individual accounts to be shared by more than one user. Center must identify the owner of generic email accounts for email accounts for proxy rights and accountability.
- Limit the number of attempted logins on a system to three.
- Do not build the user ID and password into the workstation startup routine.
- Do not share passwords with anyone. Network administrators and supervisors should assign a temporary password when assisting a user with a problem. The user must change the temporary password the next time they log in.
- Assign a temporary password to a user if they forget their password. The user must change the temporary password the next time they log in.
- Suspend inactive accounts (accounts not accessed within 90 days).
- Require users to change their passwords every 90 days.
- Set password history to a minimum of three.

b. Temporary Account Policy. A temporary account is set up to provide individuals with temporary or restricted access. Network administrators and supervisors should determine whether to install a temporary account and then determine the authorizations needed to access information. Follow these guidelines when setting up a temporary account:

- Set up a temporary account for individuals who only need temporary access to information.
- Never allow a temporary account user (guest) to change the account password.

- Restrict the files and services available for access of the temporary account.

- Protect the temporary account by changing the password frequently, preferably after each temporary user is through using it. For Novell network accounts, the POC should request that JCDC set an expiration date and time when creating the account.

c. Password Policy. Each individual is responsible for any activity using his/her accounts. It is extremely important that users protect their accounts by assigning strong passwords.

- Choose a password that makes sense to only him/her. Obvious choices, like birthdays, anniversaries, people, places, or things that are identifiable with an individual should be avoided.

- Include a combination of letters, numbers, and some special characters ($ # %, etc.) if acceptable by the system. The password must be at least 8 to 10 characters. The longer the password, the more difficult it is to guess.

- Change passwords frequently and do not repeat them.

- Change naming conventions regularly. Rearrange letters, numbers, and symbols each time the password is changed.

5. Management Reviews. Management reviews of current user lists will be conducted annually on a random basis. The audits will be conducted by the JCDC Security Team beginning in September, and will include checking for forms completion and an accurate active user list. Audit review results will be reported to the Job Corps Regional Offices.

6. Standards. The new standards for handling accounts must be implemented by **September 16, 2002**. The guidelines are as follows:

SPAMIS (UNIX), FMS, JCRL, PAIS, Novell Logon, Groupwise, EPMS

- Account Creation, Modification, and Deletion. These procedures include setting up permanent and temporary accounts, modifying accounts, and deleting accounts for friendly separations (i.e. normal retirements and resignations). Users must complete a User Request Form and give the approved form to the POC. The user's supervisor or the center director must approve the request by signing the form before forwarding it to the POC. The POC signs the form, forwards a copy to the Technical Assistance Center (TAC) for processing, and files the original. Requests will not be processed without management and/or POC approval. All unapproved forms will be returned to the requestor.

- Requesting Password Changes/Resets. Users requesting account password changes/resets by JCDC staff must fax a signed request to the JCDC TAC. The JCDC account administrator will contact the user for verification before resetting the password.

- Requesting Account Deletions (for unfriendly separation i.e. staff fired or terminated for reasons other than oderly resignation or retirement). The supervisor or manager should immediately submit an electronic copy of the User ID Request Form to the Account Administrator for processing. The electronic copy should be followed-up with a copy of the signed form.

CIS, CDSS, CTS, and OASIS

- Account Creation, Modification, and Deletion. These procedures include setting up permanent and temporary accounts, modifying accounts, and deleting accounts for friendly terminations. Users must complete a User Request Form and give the approved form to the POC for processing. The user's supervisor or the center director must approve the request by signing the form before forwarding it to the POC. The POC signs the form and processes the request. The POC will file the original form. Requests will not be processed without management approval. All unapproved forms will be returned to the requestor.

- Requesting Password Changes/Resets. All users requesting account password changes/resets at a Job Corps center or site can request a change in person or provide the POC with a signed request.

- Requesting Account Deletions (for unfriendly separation for staff terminated for reasons other than orderly resignation or retirement). The supervisor or manager should immediately submit an electronic copy of the User ID Request Form to the Account Administrator for processing. The electronic copy should be followed-up with a copy of the signed form.

- JCDC Notification of Employee Termination. The POC or center director will notify the JCDC Help Desk by email (helpdesk@jcdc.jobcorps.org) of all employee separations. Notifications will be made within 5 working days after the employee's departure. The JCDC must be notified immediately when an employee departs on unfriendly terms. The JCDC TAC will provide other JCDC employees with user separation information.

9. Action. Addressees are to ensure that a copy of this Instruction is distributed to appropriate staff.

10. Expiration Date. Until superseded.

11. Inquiries. If you have questions or comments regarding account management, please contact Linda Estep at (512) 393-7212, or email to estep@jcdc.jobcorps.org.

Attachments:

CIS User ID Request Form
EPMS User ID/Password Submission Form
FMS User ID Request Form
JCRL User ID Request Form
Network User ID Request Form
OASIS User ID Request Form
PAIS User ID/Password Submission Form
SPAMIS Access Request Form