US DEPARTMENT OF LABOR

Office of Job Corps

# Account Management Policies and Procedures

**1.0 Purpose**

Federal policy requires that access controls be implemented to provide reasonable assurance that computer resources (data files, application programs, and sensitive work areas and sensitive equipment) are protected against unauthorized access. This policy specifically addresses access to the Job Corps Network, data files and application programs.

**2.0 Scope**

This policy and the associated procedures should be implemented Job Corps-wide and should apply to all Job Corps employees with access to the Job Corps Network and Job Corps applications.

**3.0 Policy**

Job Corps Center/Agency Management and Points of Contact (POC) are responsible for ensuring that access to all Job Corps information resources is documented and approved. Access to Job Corps Information Technology (IT) resources should be documented and approved based on the segregation of duties established for each Job Corps site. Job Corps access should be established based on segregation of duties and least privilege. The following procedures and guidelines should be followed when requesting, approving, establishing, modifying, and deleting user accounts and access to IT data and systems.

**3.1 Job Corps Standard Naming Convention for User Accounts**

- For all Job Corps accounts -- The standard naming convention for user IDs must be used for new and existing Job Corps accounts.

- This naming convention is "lastname.firstname" and if a duplicate name exists, then "lastname.middleinitial.firstname" must be used. If there is a duplicated last name, middle initial, and first name, then the middle name must be spelled out using as many letters as necessary until a unique user ID is established.

**3.2 Approving and Creating Accounts**

The following approval process will be followed when establishing and modifying accounts.

The requesting manager must:

- Complete the proper User ID Request Form as required for each system based on the appropriate segregation of duties. The link to access Job Corps User ID Request Forms is

http://jcweb.jobcorps.org/Pages/Forms.aspx.  Ensure that the user identified on the form has read and signed the "User Responsibility" section of the User ID Request Form.

- Provide the user with a security briefing related to the access and use of the specific system.   All new users must take the Security Awareness orientation training within 60 days of their hire date.

- The manager, POC, or Human Resource personnel should present the new user with a copy of the Job Corps Rules of Behavior document prior to approving access to the system.  A copy of the Job Corps LAN-WAN Rules of Behavior can be obtained at http://jcweb.jobcorps.org/Pages/JCNetSecDocs.aspx. New users must review, sign and date the rules of behavior and a copy should be delivered to the POC and kept on file.  This process must be completed before access to the system is granted.

- Forward the request to the local POC for processing.

The Point of Contact (POC) must:

- Use the Job Corps Standard Naming Convention identified in 3.1 for all Job Corps accounts.

- For accounts established by the POC – Verify that the access that is being requested is in compliance with the segregation of duties guidelines, sign the form, and create the account.  If an account cannot be established in compliance with the segregation of duties policies and procedures, mitigating controls must be implemented to ensure that proper management reviews are conducted.  If a mitigating control is used, it must be approved in accordance with policy prior to its establishment.

- For accounts established by the Job Corps Data Center (JCDC) – Verify that the access that is being requested is in compliance with the segregation of duties guidelines, sign the form, and fax a copy of the form to the JCDC Technical Assistance Center (TAC) at (512) 804-2053.

- The process flow and table in Section 10.0 should be used as a guide for requesting account creations, modifications, and deletions.

- Keep the form on file for a period of one year beyond the separation date of the user.

- Do not process a request that does not have management's approval.

### 3.3 Permanent Accounts

Permanent accounts are set up to provide authorized users with access to Job Corps resources/systems for the duration of employment with Job Corps (unless otherwise specified). The following guidelines should be followed when establishing permanent accounts.

- Set up only one account on a system for each user.

- Assign a temporary password when creating the account and make it mandatory that the user change the temporary password at the time of the first log on.

- Use the Job Corps Standard Naming Convention identified in 3.1 for all Job Corps accounts.

### 3.4 Temporary Accounts

Temporary accounts are set up to provide individuals with temporary access to systems for the duration of a work assignment or project. The following guidelines should be used when setting up a temporary account:

- Set up only one account on a system for each user.

- Assign a temporary password when creating the account and make it mandatory that the user change the temporary password at the time of the first log on.

- Use the Job Corps Standard Naming Convention identified in 3.1 for all Job Corps accounts.

### 3.5 Super User/Administrator Accounts

Super User/Administrator accounts are set up to provide system administrators (POCs) with the capability of creating end-user accounts. The following guidelines should be used when setting up Super User/Administrator accounts:

- Super User/Administrator accounts should only be established by administrators at the JCDC.

- Administrators assign a temporary password when creating the account and make it mandatory that the user change the temporary password at the time of the first log on.

- Administrators set no more than three super user accounts for each system per agency.

- Administrators have each Super User sign the Administrator Agreement. A copy of the agreement will be provided by the JCDC Administrator at the time that the account is established.

- Use the Job Corps Standard Naming Convention identified in 3.1 for all Job Corps accounts.

## 3.6 Student Accounts and Use

Individual student accounts must not be established for student's use on the Job Corps Administrative Network. Student accounts may only be created on the Job Corps Student Network. Additionally, students must not be allowed to use Job Corps employee accounts at any time under any circumstances. Remember sharing of user accounts is prohibited on all Job Corps systems. All student accounts must follow the Job Corps Standard Naming Convention.

## 3.7 Protecting Accounts

Each individual is responsible for all activities performed using his/her account. Federal guidelines require that employees use the following guidelines to protect their accounts and safeguard against unauthorized activities:

- Do not share passwords with anyone.

- Select passwords that are complicated, not easily guessed. A user should choose a password that makes sense to only him/her. Obvious choices like birthdays, anniversaries, people, places, or things that are identifiable with the individual should be avoided.

- Change passwords frequently and do not repeat them.

- Passwords are required to contain 6 alpha with one being an upper case, 1 numeric, and 1 special character in addition to the following:
  o Minimum length – 8 characters
  o Maximum length – none
  o Allowable characters – Alphanumeric and special characters including: {, }, [, ], (, ), <, >, :, ', ", ?, /, |, `, ~, !, @, #, $, %, ^, &, *, _, -, +, =

- Do not allow anyone to log on to your account or to use your account once you have logged on. Users must be authenticated in a manner that allows accountability to be maintained for actions performed.

- Users requesting account password changes/resets by the JCDC TAC must contact the TAC at (800) 598-5008. The JCDC Account Administrator must contact the user for verification before resetting the password.

- 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 form.

- Users should log on and change their password immediately after the account or access is established.

System Administrators (including POCs) are responsible for ensuring that Job Corps system security controls are in place to enforce the following safeguards:

- Users and passwords should be individually owned. This means that each user should only be assigned one account and password, and that accounts should not be set up as shared accounts.

- User accounts should not be established until they are ready to be used.

- Passwords should be set to change every 90 days.

- Assign a temporary password to a user who forgets his/her password. The user must be prompted to change the temporary password the next time s/he logs in.

- Passwords should be required to be complicated enough to disallow the use of common words and phrases. Passwords are required to contain 6 alpha with one being an upper case, 1 numeric, and 1 special character in addition to the following:
  o Minimum length – 8 characters
  o Maximum length – none
  o Allowable characters – Alphanumeric and special characters including: {, }, [, ], (, ), <, >, :, ', ", ?, /, |, `, ~, !, @, #, $, %, ^, &, *, _, -, +, =

- User accounts should be disabled after successive failed attempts. Accounts should be locked after 3 invalid password attempts. Password history should be set to disallow reuse of passwords. Password history should be set to a minimum of 12.

- Users should be required to change their initial password.

- Passwords should be encrypted.

- Passwords should be at least 8 and no more than 13 characters.

- Automatic log off or locking of idle terminals should be set to 15 minutes.

### 3.8 Deactivating Accounts

System Administrators/POCs are responsible for auditing and disabling accounts. The following procedures should be followed:

**Account Inactivity**

- System Administrator/POC will periodically audit systems and deactivate accounts that have not been used within the past 60 days.

- JCDC will periodically run scripts to deactivate accounts that have not been used within 60 days.

**Friendly Separation**

- Manager or POC will deactivate the account within the first 5 days of separation.

**Unfriendly Separation**

- Manager or POC will deactivate the account immediately upon receiving official notification that an employee has separated from employment.

**Completion of Project**

- Manager or POC will deactivate the account.

- Temporary accounts should be deactivated at the end of the assigned work project.

### 4.0 Reactivating Accounts

POCs are responsible for authorizing the reactivation of accounts created under their authority.

To request reactivation for accounts that have been deactivated, please contact the JCDC TAC at (800) 598-5008.

### 5.0 Deleting Accounts

The JCDC is solely responsible for deleting accounts. Accounts will be deleted under the following conditions:

- All network accounts that have been disabled for a period of 30 days will be deleted.

- A log of the deleted accounts will be maintained for auditing purposes.

**6.0 Security Training**

All account holders are required to attend:

- Initial security training within 60 days of the hire date.

- Annual refresher training.

**7.0 Re-Certification**

The Job Corps Security Team is responsible for initiating the re-certification process. Re-certifications must be conducted on an annual or "as needed" basis. The Job Corps Security Management Team will:

- Issue a Program Instruction from the National Director to inform the Job Corps POCs and users of the need to begin the re-certification process.

- Provide POCs with a user list (if required) or instructions for printing a list of user accounts to be re-certified. Re-certifications should be conducted at the management level based on segregation of duties. Use section 3.2 of the "Segregation of Duties Policies, Procedures and Guidelines" as a guide.

- Provide a standard format for reporting results.

- Account re-certifications are required for the following systems:

  Outreach and Admissions Information System (OASIS)

  Career Transition System (CTS)

  Center Information System (CIS)

  Network Accounts/Citrix

  Note: Upon the completion of the re-certification process, POCs will sign and fax the reporting results to the Job Corps Security Team.

**8.0 Reviews**

JCDC Security Team will conduct audit reviews of the account management and re-certification process annually on a random basis. The results of the audit review will be reported to the National and Regional Offices.

**9.0 Enforcement**

Any Job Corps center found to have violated this policy may be subject to disconnection from the network and a letter stating the violation to the center's Regional staff and National Office.

## 10.0 Account Request Process Flow and Contact Listing

**Account Approval Process Flow**

Manager fills out request form based on Segregation of Duties

User signs request form

Manager delivers form to POC

POC reviews form and creates account

JCDC creates accounts for Super Users / Regional OA and CTS

POC files form for future audits

Job Corps files forms for future audits