



Job Corps Account Management Policies and Procedures

Version 5.0

January 2020

Document Change History

Date	Filename / Version #	Author	Revision Description
12/15/2006	Job Corps Account Management Policy and Procedures V 1.0	Lori McElroy	Reviewed and updated for Job Corps applicability.
4/2/2009	Job Corps Account Management Policy and Procedures V 2.0	Christopher Cale	Policy updates.
04/04/2017	Job Corps Account Management Policy and Procedures V 3.0	JCDC Security/Nancy Summerville	Updates to Sect. 7.0 – Account Recertification Process
08/22/2019	Job Corps Account Management Policy and Procedures V 4.0	JCDC Security/Nancy Summerville	Updates to Sections 3.2 and 4.0
08/07/2020	Job Corps Account Management Policy and Procedures v 5.0- Annual Review	Nancy Summerville	Adjusted TOC, minor formatting

Document Review History

Date	Version #	Reviewers
4/2/2009	Job Corps Account Management Policy and Procedures V 2.0	Christopher Cale, Nancy Summerville, Jim Fyffe
05/26/2010	Job Corps Account Management Policy and Procedures V 2.0	JCDC Security
05/20/2011	Job Corps Account Management Policy and Procedures V 2.0	JCDC Security
04/20/2012	Job Corps Account Management Policy and Procedures V 2.0	JCDC Security
05/21/2013	Job Corps Account Management Policy and Procedures V 2.0	JCDC Security
02/26/2014	Job Corps Account Management Policy and Procedures V 2.0	JCDC Security
02/02/2015	Job Corps Account Management Policy and Procedures V 2.0	JCDC Security
04/04/2016	Job Corps Account Management Policy and Procedures V2.0	JCDC Security
04/04/2017	Job Corps Account Management Policy and Procedures V 3.0- Annual Review	JCDC Security
01/25/2018	Job Corps Account Management Policy and Procedures V 3.0- Annual Review	JCDC Security/Nancy Summerville
04/01/2019	Job Corps Account Management Policy and Procedures V 3.0- Annual Review	Nancy Summerville/JCDC Security

Table of Contents

1.0 Purpose.....	4
2.0 Scope	4
3.0 Policy.....	4
3.1 Job Corps Standard Naming Convention for User Accounts	4
3.2 Approving and Creating Accounts.....	4
3.3 Permanent Accounts.....	5
3.4 Temporary Accounts.....	5
3.5 Administrator Accounts	6
3.6 Student Accounts and Use.....	6
3.7 Protecting Accounts	6
3.8 Deactivating Accounts	7
4.0 Reactivating Accounts.....	8
5.0 Deleting Accounts.....	8
6.0 Security Training.....	8
7.0 Account Recertification.....	8
8.0 Reviews.....	8
9.0 Enforcement	9
10.0 Account Request Flow Process.....	9

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.

The standard naming convention is *lastname.firstname*. 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 separation of duties. Job Corps User ID Request Forms are available on the Job Corps Community Website under Forms.
- Ensure that the user identified on the form has read and signed Section IV (“User Responsibilities”) of the User ID Request Form.
- Sign and date the form.
- Forward the request to the local Point of Contact (POC) for processing.

The Point of Contact (POC) must:

- Verify that the access requested is in compliance with the separation of duties guidelines.
- Only process requests that have management’s approval.
- Sign and date the form.
- Send a copy of the form to the JCDC Account Control Team by email AccountControl@jobcorps.org or by fax (888) 278-8389.

- When the request resolution is received from the TAC, ensure that the new/modified account's credentials are delivered in-person to the user (or over the phone when in-person issuance places an unreasonable burden on the POC or the user).
- If the account credentials are printed or written down, then ensure they are protected during delivery to the user, and make sure the user understands they must also protect it, and destroy it by shredding immediately after using the credentials to login.

The user must:

- If the account credentials were printed or written down when being delivered, then protect them from exposure, and destroy them by shredding immediately after initial login.
- Immediately set a password upon initial login.
- Immediately after login, take the Security Awareness Training (SAT) before receiving access to other resources on the Job Corps network.
- Acknowledge and understand the Job Corps Rules of Behavior contained within the SAT prior to accessing other resources on the Job Corps network.

The Job Corps Data Center (JCDC) Account Control Team must:

- Check the User ID Request Form for proper completion, including all required signatures.
- Use the Job Corps Standard Naming Convention for all Job Corps accounts.
- Use the Account Approval Process Flow (at the end of this document) as a guide for requesting account creations, modifications, and deletions.
- Keep the User ID Request Form on file for a period of one year beyond the separation date of the user.

The information system:

- Automatically ensures that all new users take the Security Awareness Training (SAT) prior to being allowed access to the system.
- Automatically ensures that all new users acknowledge that they have read and understood Job Corps' Appropriate Use policies (Rules of Behavior) contained within the SAT prior to being allowed access to the system.

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, emergency, anonymous, and guest accounts are not permitted.

3.5 Administrator Accounts

Administrator accounts are set up to provide system administrators and/or POC's with the capability of creating end-user accounts. The following guidelines should be used when setting up Administrator accounts:

- 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.
- There should be no more than three super user accounts for each system per agency.
- Use the Job Corps Standard Naming Convention identified in 3.1 for all Job Corps accounts.

3.6 Student Accounts and Use

Student accounts may only be created on the Job Corps Student Network. All student accounts must follow the Job Corps Standard Naming Convention.

Individual student accounts must not be established for student's use on the Job Corps Administrative 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.

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:
 - Minimum length – 8 characters
 - Maximum length – none
 - 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 he/she 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:
 - Minimum length – 8 characters
 - Maximum length – none
 - 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 characters.
- Automatic log off or locking of idle terminals should be set to 15 minutes.

3.8 Deactivating Accounts

The information system automatically disables inactive accounts after 60 days. The following procedures should be followed:

Account Inactivity

- A scheduled task is set to run nightly (7:30 central time) to determine if a user has authenticated within the last 60 days.
- If the user has not authenticated within the last 60 days, the account is put into a disabled state.
- If the account remains in a disabled state for an additional 60 days, it will then be deleted.

Employee Separation

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

Completion of Project

- Manager or POC will deactivate the account.

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 Job Corps Data Center (JCDC) Technical Assistance Center (TAC) at (800) 598-5008.
- Account management resolutions are sent to the POC responsible for authorizing the request. The POC is responsible for relaying the resolution to the end-user.
- When the request resolution is received from the TAC, then ensure that the new/modified account's credentials are delivered in-person to the user (or over the phone when in-person issuance places an unreasonable burden on the POC or the user).
- If the account credentials are printed or written down, then ensure they are protected during delivery to the user, and make sure the user understands they must also protect it, and destroy it by shredding immediately after using the credentials to login.

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 in a disabled state for a period of 60 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:

- New Employee Security Awareness Training immediately upon hire and prior to accessing the Job Corps network.
- Annual refresher security training thereafter.

7.0 Account Recertification

- The Job Corps information system is configured to ensure that all user accounts on the Job Corps network and CDSS Suite be recertified on a bi-annual (or "as needed") basis.
- Every 6 months, the system sends a user an email saying that they are due to recertify their account.
- The user clicks the Account Recertification link to view their assigned access (such as Citrix and CDSS applications) and either accepts or denies the responsibility for that access.
- After the user completes the certification process, the POC has 2 weeks to login to the POCAAdmin tool and review the user's access by comparing against personnel records. The POC can then either approve or reject the access. If the access needs to be modified, the POC must submit a User ID Request Form for that modification.
- The system automatically disables any accounts that are:
 - Not recertified by the user after the 6-month period, or
 - Not approved by the POC during the 2-week period.

8.0 Reviews

JCDC Security Team will conduct audit reviews of the account management and annual recertification process on a random annual 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 Flow Process

