

November 10, 2010

|   |
|---|
| <b>DIRECTIVE:</b> JOB CORPS PROGRAM INSTRUCTION NO. 10-21 |
|---|

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

**FROM:**                EDNA PRIMROSE  
                          National Director  
                          Office of Job Corps

**SUBJECT:**            Job Corps Prohibition on Sharing User Accounts

1.     Purpose. To prohibit the sharing of Job Corps user accounts in order to (1) ensure that Job Corps students' private information remains secure and confidential, and (2) ensure that Job Corps staff are not wrongfully accused of improper system use.

2.     Background. The *Job Corps Rules of Behavior* (which all users are required to read and acknowledge before receiving access to the system) prohibits the unauthorized access of data through circumvented system authentication. Any individual who accesses the Job Corps network without using his or her own user ID and password is in violation of this policy:

The Job Corps network may not be used in an attempt to circumvent the system authentication or security of any account, network, or host. This would include, but is not limited to the following: Accessing data that is not intended for your information, logging on to a server or account to which you are not authorized to gain access, or probing the security of other networks. Do not attempt to bypass security safeguards and countermeasures implemented for the protection of Job Corps data or processing systems. (*Job Corps Rules of Behavior*, page C-4, bullet 3)

Also in the *Rules of Behavior*, Job Corps prohibits the sharing of passwords:

Safeguard passwords and user account numbers from other personnel by not disclosing them either verbally or in written form. Users must not at any time share or display their passwords. Users should not record a password in writing. (*Job Corps Rules of Behavior*, page C-5, bullet 13)

Additionally, please note that students are strictly prohibited, at all times and in all circumstances, from accessing the Job Corps Administrative Network:

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.

*(Job Corps Access Control Policy and Procedures, Appendix B, "Account Management Policy and Procedures," page 45)*

3. Risk to Staff of Sharing Accounts. These policies are in place not only to protect students' private information, but also to protect the staff members who use the Job Corps system:

Each individual is responsible for all activities performed using his/her account.

*(Job Corps Access Control Policy and Procedures, Appendix B, "Account Management Policy and Procedures," page 45)*

If students or staff members are allowed to access the Job Corps system under a different user's ID, then the staff member who is logged in will be held accountable for any actions performed under that user ID. Unauthorized access and use of a federal information system is a serious matter, with actions punishable by fines and even imprisonment.

4. Action. To avoid being wrongfully accused, information system users must protect themselves, as well as students' private information, by following these policy requirements:

- a. Keep your password secret at all times (never share it with anyone).
- b. Lock your workstation before leaving it (even if only stepping away for a minute).
- c. Never log in and then allow a student or another staff member to access your workstation.

Thank you for your help and cooperation in keeping the Job Corps systems secure. Addressees are to ensure this Program Instruction is distributed to all appropriate staff.

5. Expiration Date. Until superseded.

6. Inquiries. Inquiries should be directed to Christopher Cale at (888) 886-1303, ext 7223 or [cale.chris@jobcorps.org](mailto:cale.chris@jobcorps.org), or Linda Estep at (888) 886-1303, ext 7212 or [estep.linda@dol.gov](mailto:estep.linda@dol.gov).