July 14, 2008

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NO. 08-04

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: ESTHER R. JOHNSON, Ed. D.
National Director
Office of Job Corps

SUBJECT: Mandatory Annual Account Recertification for Citrix and Career Development Services System Suite of Applications Using the Job Corps Segregation of Duties and Account Management Policies and Procedures

1. Purpose. To notify the Job Corps community of the federal requirements, policies, and guidelines associated with the Citrix and Career Development Services System (CDSS) Suite of Applications Account Recertification process; provide updated copies of these policies; and outline the 2008 Account Recertification process. The Segregation of Duties and Account Management Policies should be used to ensure procedures are in place to limit staff access to only those functions necessary for their job and enforce general account maintenance procedures. These policies, procedures, and guidelines are necessary to maintain data integrity and must be followed by the Job Corps community at all times.

Important Note: Job Corps is currently conducting the Tri-Annual *Certification and Accreditation audit* that is required to renew Job Corps' "Authority to Operate" status. A successful account recertification is required in order for Job Corps to pass the audit. Therefore, it is imperative that ALL users complete the recertification by the due date.

2. Background. Job Corps continues to ensure compliance with federal security requirements, Job Corps Segregation of Duties Policies and Procedures, and Job Corps Account Management Policies and Procedures by conducting an annual Account Recertification audit for Citrix and the CDSS Suite of Applications. This year, Job Corps will require a completed Account Access Authorization Form certification from **each individual user** (for both Citrix and CDSS applications).

3. Action.

a. Instructions and Deadline for Completing the Form.

Staff will recertify by completing the electronic form available at https://cdssrecert.jobcorps.gov by July 25, 2008. Log in using your Citrix ID and password. The electronic form must be filled out in its entirety. All Citrix and CDSS users must complete the form. Further instructions for completing the electronic form are included in an attachment to this Program Instruction.

b. Submitting the Form.

Completed forms must be printed out and signed by your supervisor. Signed forms may be scanned and the electronic version returned to the Job Corps Data Center (JCDC) Security group (jcdcsecurity@jobcorps.org). If no scanner is available, the form may be returned by fax to: (877) 389-9451. Center/agency Points of Contact (POCs) should keep originals for their records, in the event of an audit.

c. Required Policy Review.

Regional Offices and Job Corps center operators must ensure compliance with the following. Effective immediately, Job Corps Center Directors and OA/CTS contract managers must conduct a policy review, as follows:

(1) Read the Segregation of Duties and Account Management documents (Attachments A and B).

(2) Ensure these policies and procedures are incorporated into their agency's Standard Operating Procedures (SOP). If any exceptions exist as defined in Section 4 below (Exceptions to the Segregation of Duties), it will be necessary to request approval from the National or Regional Office to use compensating controls and provide supporting documentation to JCDC Security by July 25, 2008.

(3) If any of these exceptions exist, please contact jcdcsecurity@jobcorps.org for further instructions.

Addressees are to ensure that this Program Instruction is distributed to all appropriate staff.

4. Exceptions to the Segregation of Duties. In those instances where duties and system access to critical system functions cannot be fully segregated (normally due to staffing constraints), compensating controls must be established (at each location) as appropriate. Compensating controls are additional procedures designed to reduce the risk of errors, irregularities, or fraudulent activities. Procedures could include such controls as maintaining

logs, monitoring staff activities, dual authorization requirements, and documented reviews of input/output. Special permission must be obtained from the National or Regional Office Director or designee to qualify for use of a compensating control. These requests should be rare and must be accompanied by complete documentation, including a justification for each compensating control to be used. All records must be strictly maintained, and periodic audits will be performed for those centers with compensating controls in place. If a condition exists that warrants an exception, obtain supervisor and National or Regional Office Director or designee approval and forward this approval to jcdcsecurity@jobcorps.org.

5. Multiple System Access. According to the Segregation of Duties Policies and Procedures, "No individual user should have access to all three student-tracking applications – Outreach & Admissions Student Input System (OASIS), Career Transition System (CTS), and the Center Information System (CIS) – unless special authorization is obtained from the National or Regional Office. For example, the National Office may authorize an employee to have access to all three systems to conduct internal audits at Job Corps centers." If this condition exists for any user, it is necessary to obtain the required approvals. A supervisor and National or Regional Office Director or designee must sign off on the Authorization Form.

NOTE: JCDC Security continues to conduct quarterly center audits, which require each center to provide evidence of the New User Account request forms with appropriate signatures for all major applications (CIS, CTS, and OASIS). According to the Account Management Policies and Procedures, all POCs must verify the approvals and requested accesses indicated on the New User ID Request Form and keep a copy of this form on file for 1 year beyond the separation date of the user. User ID request forms are available at the Job Corps Community Web Site in Citrix.

6. Expiration Date. Until superseded.

7. Inquiries. Questions or comments may be addressed to James Fyffe at fyffe.james@jobcorps.org; Christopher Cale at cale.chris@jobcorps.org or (888) 886-1303, ext 7223; Linda Estep at estep.linda@jobcorps.org or (888) 886-1303, ext 7212; or the JCDC Technical Assistance Center at (800) 598-5008.

Attachments

A – Job Corps Segregation of Duties Policies and Procedures

B – Job Corps Account Management Policies and Procedures

C – Authorization for Access to Multiple Applications

D – Instructions for Completing the Online Recertification Form