March 31, 2010

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NO. 09-42

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: Removal of System Access for Former Employees

1. Purpose. To inform the human resources departments and the center Points of Contact (POCs) of the policy regarding the periodic review of information system accounts (to include the matching of personnel files) in order to ensure that terminated or transferred individuals do not retain system access, and to request that the necessary actions be taken to ensure this policy is met.

2. Background. It has been Job Corps policy that the center Point of Contact (POC) must immediately disable a user's account upon receiving official notice of that employee's separation (termination or transfer). Additionally, it is Job Corps policy (as mandated by the Department of Labor) to review all information system accounts at least every 6 months to include the matching of user records (e.g., personnel files).

An independent audit of the Department of Labor (DOL) found weaknesses in the controls in place to ensure that separated employees do not retain system access. "Certain terminated personnel had active system accounts, and in some cases, terminated employees accessed systems after their termination date," the report states (http://www.dol.gov/_sec/media/reports/annual2008/IAR.htm).

Although Job Corps' information system automatically disables accounts that are inactive, if terminated users continue to log in to their account (keeping it active), then they could continue to access the Job Corps system. This unauthorized access would compromise the confidentiality and integrity of data, including Personally Identifiable Information (PII), stored in the Job Corps system. In order to adequately prevent this occurrence, Job Corps is strengthening the account management process to ensure the information system account of a terminated user is immediately disabled.

3. Action. To successfully ensure that terminated or transferred users do not retain system access, Job Corps requires the assistance of the human resources departments, the center Points of Contact (POCs), and the Job Corps Security Team.

a. Human Resources Responsibilities

i. When an individual is terminated or transferred, immediately contact the POC in order to ensure that the user's information system account is disabled.

ii. On a monthly basis, send the POC a list of all active employees.

b. POC's Responsibilities

i. Immediately upon receiving official notification of an employee's separation, disable that user's account.

ii. Before approving or rejecting a user's account recertification, check to ensure the user's name is on the most current list of active employees.

c. Job Corps Security Team's Responsibilities

i. To further ensure that terminated or transferred employees are not retaining access to the system, the Job Corps Security Team will begin conducting audits of the account management process. Additional information regarding the account management audits will be sent to the appropriate individuals when details are finalized.

4. Expiration. Until superseded.

5. Inquiries. Inquiries should be directed to Christopher Cale at (888) 886-1303 x7223, or e-mail cale.chris@jobcorps.org, or Linda Estep at (888) 886-1303 x7212, or e-mail estep.linda@dol.gov.