January 31, 2011

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NO. 10-31

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: Important Reminders Regarding the Securing of Job Corps Information

1. Purpose. To remind the Job Corps community of the importance of securing Job Corps information, and to bring special attention to the following policies, which have recently been an issue: (1) sharing user accounts is prohibited; (2) only authorized government-furnished equipment (GFE) may access Department of Labor (DOL) networks; (3) incidents of possible security breach (e.g., lost or missing personally identifiable information [PII]) must be reported in a timely manner; and (4) there must be no expectation of privacy on the Job Corps network.

2. Background. Job Corps has a responsibility to keep its systems secure and to protect the confidentiality, integrity, and availability of the data contained therein. To safeguard Job Corps systems, strict security guidelines must be upheld, and it is the responsibility of every Job Corps system user to abide by them in the course of their duties.

3. Policy. Please pay close attention to the following policy requirements. Job Corps system users who are found to be in violation of any of the following policies are subject to disciplinary action at the discretion of Job Corps' management, including a verbal or written warning; removal of system access, either permanently or for a specific period of time; re-assignment to other duties; or termination, depending on the severity of the violation.

a. Sharing User Accounts Is Prohibited.

Under no circumstances may a Job Corps system user share his or her user account with another individual. This policy is to protect Job Corps personnel as much as it is to protect the Job Corps system. Please refer to Program Instruction

10-21, "Job Corps Prohibition on Sharing User Accounts," dated November 10, 2010, for details.

b. Only Authorized Government-Furnished Equipment (GFE) May Access DOL Networks.

Because DOL has no guarantee that unauthorized equipment has the proper security controls in place, the use of unauthorized devices to connect to DOL networks is explicitly prohibited (DOL Computer Security Handbook, Volume 16, Section II, p. 17, dated December 29, 2006):

> *All connected hosts (hard-wired, wireless, or mobile) must be authorized to operate in the DOL infrastructure … no unauthorized connections are allowed.*

Equipment that was not furnished by the government (i.e., personally-owned or contractor-issued equipment) is not authorized to connect to DOL networks without going through an official approval process. Using unauthorized equipment to plug into any DOL network (such as the Employment and Training Administration or Job Corps networks) is a violation of Job Corps and DOL security policies and puts the network at risk.

c. Report Incidents of Possible Security Breach (e.g., Lost or Missing PII) in a Timely Manner.

Security incidents can pose a risk to Job Corps systems and the information contained therein. When a security incident occurs, timely reporting is of utmost importance. Suspected security incidents must be reported immediately to the Job Corps Technical Assistance Center (TAC) at 1-800-598-5008.

Any suspected unauthorized access of Job Corps information is considered a security incident. It is especially critical to be aware of any loss or theft of students' sensitive PII, whether paper-based or electronic. If equipment (e.g., laptop, Personal Digital Assistant [PDA], thumb drive) or papers (e.g., files, printouts, W2 forms) that may contain PII are suspected lost or stolen, immediately call the TAC (1-800-598-5008) to report the incident. For more information, please refer to Program Instruction 09-34 "Handling Personally Identifiable Information and Properly Reporting a Loss," dated February 17, 2010.

d. There Must Be No Expectation of Privacy on the Job Corps Network

The Job Corps network (including the e-mail system and file repository) is for official government use only. Job Corps network users do not have a right, nor should they have an expectation, of privacy while using any government office equipment at any time, including accessing the Internet and using e-mail. To the extent that network users wish their private activities to remain private, they

should avoid using Job Corps equipment, such as their work-issued or center-provided computer, for accessing the Internet or e-mail. By using government office equipment, Job Corps network users imply their consent to disclosing the contents of any files or information maintained in or passed through Job Corps office equipment.

It has been recommended that contractors consider storing their proprietary e-mails and documents in their own corporate systems.

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

5. Expiration. Until superseded.

6. Inquiries. Inquiries should be directed to Christopher Cale (cale.chris@jobcorps.org) or Linda Estep (estep.linda@dol.gov).