February 17, 2010

DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 09-34

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: LYNN A. INTREPIDI
Interim National Director
Office of Job Corps

SUBJECT: Handling Personally Identifiable Information and Properly Reporting a Loss

1. Purpose. To highlight the importance of protecting Job Corps students' Personally Identifiable Information (PII), to remind the Job Corps community of best practices in handling PII, and to review the notification procedure for suspicion of lost or compromised PII.

2. Background. Job Corps has a critical responsibility to protect the personal information that it collects from Job Corps students. Loss or unnecessary sharing of a student's personal information could result in harm (e.g., identity theft) to the student, and it is a liability to both Job Corps and the Department of Labor.

Every staff member in the Job Corps community, regardless of job position, has an obligation to protect the PII data of the Job Corps students we serve. PII that resides on the Job Corps system includes:

a. First and last name

b. Social Security Number

c. Date of birth

d. Home address

e. Home phone number

3. Action. PII must be treated as sensitive information and, as such, requires special handling and consideration at all times:

a. Sharing – Only share PII on a need-to-know basis. Before sharing it, always take a moment to consider whether it is absolutely necessary to use PII, and whether the person(s) that are receiving it need to know and are authorized to view the sensitive information.

b. Transporting – When sending PII electronically, it must be encrypted during transmission (e.g., e-mail on your Citrix desktop, not through your personal e-mail); when sending a hard copy in the mail, it must be double-sealed.

c. Storing – All PII stored on a hard drive, flash drive, or disk must be encrypted. All PII in physical form must be protected as well (e.g., in a locked drawer or filing cabinet, not left lying unattended on a desk).

d. Disposing – PII must be disposed of in such a manner that the information cannot be recovered (e.g., shredded).

If there is any reason to suspect that PII has been lost or compromised, it must be reported **within 1 hour** of discovery. Here are some of the ways that PII may be lost or compromised:

a. Lost or stolen flash drives, laptops, desktop computers

b. Missing printed reports or W2 forms that contain PII

c. E-mail that contains PII (in the body of the message, attached spreadsheets, Word documents, scanned documents, PDF, etc.) sent outside of the Job Corps domain

d. PII displayed on a screen that may be viewed or copied by an unauthorized individual

e. Loss or theft of backup tapes, CDs, etc.

A suspected loss or compromise of PII must be reported **within 1 hour** to the Job Corps Technical Assistance Center (TAC) at (800) 598-5008, Option 4. If the incident occurs after working hours (7 p.m. – 7 a.m. CST), contact TAC and select Option 7 to report a PII incident.

It is the responsibility of every Job Corps employee to ensure that PII is protected at all times and to immediately report any circumstance or incident that may indicate the loss or compromise of such information.

4. Expiration Date. Until superseded.

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