US DEPARTMENT OF LABOR

Office of Job Corps

# Job Corps Rules of Behavior

Version 3.0

Last Update – July 6, 2006

## *Table of Contents*

## Introduction

In accordance with Office of Management and Budget (OMB) Circular A-130, the Job Corps network must have a set of rules established to govern the use of and behavior within the system. These rules must clearly delineate responsibilities and expected behavior of all individuals with access to this system. The Rules of Behavior (ROB) contained in this document are to be followed by all users of Job Corps systems.

## Non-Compliance

Employees who violate the Job Corps policy regarding Job Corps Rules of Behavior may be subject to disciplinary action at the discretion of Job Corps' management. Actions may include a verbal or written warning, removal of system access either permanently or for a specific period of time, reassignment to other duties, or termination depending on the severity of the violation. In addition, audit logs are reviewed on a weekly basis to determine unauthorized access to Job Corps network. The Job Corps Data Center (JCDC) Security Team will investigate any suspected violations of these policies. As a system user, you are responsible for ensuring your compliance to the policies stated in the Job Corps Rules of Behavior.

***Note***: *Job Corps Points of Contact (POCs) should keep the user's signed acknowledgement agreement, found at the end of this document, on-file for a period of one (1) year after the user's separation from Job Corps.*

## Other Policies

The rules are consistent with the policies and procedures described in the following directives:

1. DLMS-9, Department of Labor Management Series 9, Chapter 1200, Draft, contains department-wide appropriate use policy.
2. DOL Computer Security Handbook, Draft, contains computer security procedures, guidance, and standards on a wide range of topics.
3. NIST 800-18 *Computer Security Guidelines.*
4. Job Corps Internet and Email Usage Policy.
5. NIST 800-53 *Recommended Security Controls for Federal Information Systems.*

## Acceptable Use

DLMS-9, Chapter 1200 states employees are authorized limited personal use of Department of Labor (DOL) office equipment. This personal use must not result in loss of employee productivity or interfere with official duties. Job Corps and DOL employees are permitted this limited personal use as long as it does not interfere with the DOL or Job Corps mission, involves virtually no additional expense to the Department, and does not violate the Standards for Ethical Conduct for Federal Employees. All internet and email usage must comply with the Job Corps Internet and Email Usage Policy located at http://training.jobcorps.org/security/policies.htm.

## Job Corps Rules of Behavior

The following are the rules of behavior and responsibilities that users are expected to follow when using the Job Corps network:

### Rules and Responsibilities

1. Only authorized users are allowed access to the Job Corps network and the data contained within.
2. Unauthorized Job Corps network or system access is punishable by a fine, imprisonment, or both. Use of the Job Corps network is not considered private and may be monitored at any time.
3. 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 into 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.
4. Using tools to compromise the system security or any attempt to disrupt or deny operation of the Job Corps network is strictly prohibited.
5. Knowingly transmitting viruses via email, or otherwise, when using this network is not allowed.
6. Each user must have a unique user name and password for accountability purposes. Sharing user login information (ex: your username and password) is strictly prohibited. Users are responsible for all actions performed under their user account name. Therefore, each individual user must take the necessary steps to ensure that others do not use their account to gain unauthorized access to the Job Corps network where they have a registered account. This issue is stressed in computer security awareness training provided by Job Corps and DOL.

7. Users will be assigned only the access rights or privileges needed to perform their tasks based on their job requirement. Users are to work within the confines of the access allowed, and are not to attempt to access unauthorized systems or applications.
8. Users are not authorized to assign their own access rights. Only the System Administrator (SA) and designated network support specialists will implement assignment of user access rights and permissions.
9. Posting material or information that is unlawful, such as obscene materials, inappropriate content, or language on any Job Corps sponsored Web site is prohibited. Users will be held solely responsible for any information posted and published to a Job Corps web site that is in violation of this policy.
10. Posting material or information that violates the Privacy Act of 1974 without prior written permission or authorization on any Job Corps sponsored Web site is prohibited.
11. Unauthorized attempts to upload information, delete, tamper or change information on any Job Corps Web sites where access is not explicitly granted is strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996.
12. Select secure passwords that are at least eight (8) characters in length and are a combination of both numbers and characters, which cannot be easily associated with the user. Passwords must be changed at least every three (3) months. Users should not use common dictionary words nor reuse their last twenty-four (24) passwords.
13. 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 nor display their passwords. Users should not record a password in writing.
14. Notify supervisory or security personnel when authorized access rights and privileges are no longer required.
15. Users will control access to their personal computers by locking their workstations, manually logging off, activating their locked screen savers, or shutting down computers when leaving workstations unattended.
16. Ensure that critical workstation data is backed up to diskette, CD-ROM, or a network drive at least weekly and that the media that contains backup data is stored in an area physically removed from the workstation.
17. Anti-virus protection is required on all Job Corps systems. Ensure that the auto-update feature is enabled on your anti-virus software. The use of real-time virus scanning is required. This is to ensure that every file being processed is checked for virus activity. Anti-virus email scanning is performed at the email server level by the JCDC.
18. If a user receives a “virus hoax” the user should verbally report the suspected virus hoax to the center POC or JCDC Technical Assistance Center (TAC). Do not forward these hoax messages as they may actually contain a virus. Users must not carry on the virus hoax nor send it to anyone else.
19. Ensure that individual workstations and peripheral devices are connected to a surge suppressor or other power protection device.

20. Protect system hardware from hazards, such as water or excessive heat. Safeguard system hardware by avoiding smoking, drinking, and eating near workstations. No food or drinks are allowed near any of Job Corps' network servers.
21. Do not install or use any personal software or hardware on the Job Corps network. Doing so may spread viruses, cause system configuration corruption and/or compromise the security of the Job Corps network.
22. Users must read and comply with the Job Corps Internet and Email Usage Policy located at http://training.jobcorps.org/security/policies.htm.

## Protecting Sensitive Data

The loss of personally identifiable information can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because Job Corps employees and contractors may have access to personal identifiable information concerning individuals and other sensitive data, we have a special responsibility to protect that information from loss and misuse.

**With these responsibilities in mind, users must:**

- **Safeguard the information to which they have access at all times.**
- **Obtain supervisor's written approval prior to taking any Job Corps sensitive information home or otherwise away from the office. The supervisor's approval must identify the business necessity for removing such information from the Job Corps facility.**

**When approval is granted to take sensitive information home or away from the office, the user must adhere to the security policies described above.**

### *Other Protective Measures*

- Employee personnel information is kept confidential at all times (ex: names of current or past employees, dates of their employment, reference information or medical information for current or past employees).
- The Job Corps network may not be used to collect personal information for non-business purposes.
- All individuals who access the Job Corps network must be aware of the sensitivity of data residing on the system. They must be aware that any intentional disclosure, modification, corruption, or falsification of data will result in disciplinary action or termination.
- Users should not provide project related information concerning specific technical methods and sensitive materials used to protect confidential information to unauthorized individuals.
- It is prohibited to sell or share any of the data or information obtained from the Job Corps network.

- Never discuss or otherwise reveal sensitive information that should not be disclosed to unauthorized personnel, either over the phone, in face-to-face discussions, or in an area where unauthorized personnel might overhear conversations involving sensitive information.
- Safeguard sensitive hard copy data and reports (particularly reports containing Privacy Act data), when not attended, by securing it in a locked office or secured desk or cabinet. If not already labeled, mark all screen printouts and hard-copy output containing Privacy Act information with an indication that they contain data subject to the Privacy Act of 1974. Destroy sensitive documents and reports by shredding. Never remove sensitive data from any Job Corps facility without the prior approval of supervisory personnel.
- Be sure that only authorized personnel are allowed to view sensitive information; whether the information is on a computer monitor or on paper. When printing hard-copy output containing sensitive data at a printer accessible to unauthorized personnel, pick up the printed material immediately to ensure that unauthorized personnel cannot view or obtain the output. When viewing or processing sensitive information on a personal computer, make sure the monitor is positioned away from doors, windows, and heavily traveled areas.
- Upon observation of unknown personnel in areas where sensitive data is being used or stored, report them immediately to management or security.
- When copying sensitive information to electronic media, label the media with an indication that the output contains sensitive information and that it should be withheld from disclosure to unauthorized personnel.
- Only access sensitive data on the Job Corps network when it is necessary to perform assigned duties, and report failures in the systems access control mechanism to supervisory personnel.

## *Reporting an Incident*

If an incident is suspected, report it immediately to a Center POC, management, or the JCDC TAC. This includes security infractions by co-workers, attempted access by unauthorized personnel, violations of procedures, disclosure of sensitive information, loss of availability of the Job Corps network resources, destruction of data, or detection of erroneous information or unexplained system activity.

When reporting an incident, the following information is required:

1. Date and time of the incident
2. Log files (if appropriate)
3. Contact information for person reporting the incident
4. Examples of the incident or any other information that may be useful to the investigation and verification of the incident.

## Training

- All users must take New Employee Security Awareness Training within sixty (60) days of the start of their employment.
- All users must take an annual refresher Security Awareness Training course.
- All users must participate in Job Corps directed security training as required by the Job Corps Data Center.

## Working Away from the Office

- All Job Corps equipment used offsite must be approved by the JCDC Property Officer or center management.
- All remote connections into the Job Corps network must adhere to Job Corps security polices and procedures.
- If logging in from non-Job Corps issued equipment, it is your responsibility to ensure that all Job Corps-required security measures are in place.
- If using wireless access, ensure that wireless security features are enabled.
- All remote users must follow the same rules of behavior established for all users on the Job Corps network.

## Dial-up Access

The JCDC Information Technology (IT) Director may authorize dial-up access to the Job Corps network for individual users. Dial-up access poses additional security risks, but it may be necessary for certain job functions. If dial-up access is allowed, the JCDC will review the telecommunications logs regularly, and conduct spot-checks to determine if Job Corps dial-up users are complying with controls placed on the use of dial-up lines. All dial-up users must follow the same rules of behavior established for all Job Corps network users.

## Protection of Software Copyright Licenses

All copyright licenses associated with the use of commercial off-the-shelf software will be adhered to by Job Corps personnel, as well as by contractors responsible for developing and maintaining the Job Corps network

Software includes any software for communications packages, database management, word processors, spreadsheets, graphics, or specialized applications. Job Corps requires that all software copyright licenses and license agreements for PC-based and LAN-based software used by employees and contractors are fully understood, and that personnel comply with the license

requirements. Software diskettes, license agreements, and software manuals are to remain in the possession of Job Corps.

## *Rules of Behavior Acknowledgement*

I acknowledge receipt of this policy (version 3.0, July 6, 2006) governing the Rules of Behavior concerning the Job Corps network, understand my responsibilities, and will comply with these rules of behavior for the Job Corps network as written.

I understand the National Job Corps Data Center reserves the right to disable my account access or enforce other sanctions as described in these rules without notice for violation of these polices.

Printed Name of User

Signature of User

Date