US DEPARTMENT OF LABOR

Employment and Training Administration
Office of Job Corps

Job Corps Network IT and Security Policies and Procedures

ATTACHMENT

Job Corps Network IT and Security

Policies and Procedures

1.0 Purpose

This policy and procedures document defines how network access controls to protect the Job Corps network against unauthorized access are to be implemented across the Job Corps network.

2.0 Scope

This policy and the associated procedures should be implemented throughout the Job Corps community and apply to all systems and applications that are operated on the Job Corps network.

3.0 Policy

Job Corps Center/Agency Management and Points of Contact are responsible for ensuring that (1) devices that can be connected to the Job Corps network have sophisticated enough Operating Systems with integrated security features to ensure user authentication and management; (2) hubs and unauthorized wireless devices are not installed on the network and if found are removed immediately; (3) unauthorized third party circuits are not installed on the network and if found are disconnected immediately; and (4) all systems that connect to the Job Corps network have the appropriate virus signature files, the latest security patches and that the user takes precautions to prevent unauthorized access to Job Corps computers.

3.1 Operating Systems

To ensure that devices that can be connected to the Job Corps network have sophisticated enough Operating Systems with integrated security features to ensure user authentication and management, PCs must be running Windows XP Professional (JCDC Notice 04-103) with Service Pack 2 installed.

- Thin clients that are managed and maintained from a central console, controlled by the Job Corps Data Center may replace the older, non-compliant PCs.

3.2 Hubs and Unauthorized Wireless Devices

Hubs and unauthorized wireless devices may not be attached to the Job Corps network. If one is found it must be removed immediately. Failure to remove the devices could result in discontinuation of network services until the unauthorized devices have been removed from the network.

3.3 Third-Party Circuits

Unauthorized third-party circuits must be disconnected immediately. Third-party circuits are only allowed if a signed Memorandum of Understanding is on file between the center and the National Office of Job Corps. Failure to disconnect any unauthorized third-party circuits may result in disconnection from the Job Corps network.

3.4 Viruses and Security Patches

All systems that connect to the Job Corps network must have the appropriate virus signature files, the latest security patches and that the user takes precautions to prevent unauthorized access to Job Corps computers/

- All systems that connect to the Job Corps network must have the appropriate virus signature files and the latest security patches.
- The user must take precautions to prevent unauthorized access to Job Corps computers.
- To combat viruses and security threats, the Business Oriented Software Solutions (BOSS) Automated Security Patching software must be installed on all PCs on the Job Corps network.
- All systems connected to the Job Corps network must have anti-virus software loaded and up-to-date with the latest signature files.
- All PCs must be updated with the latest security patches on a regular basis.
- The Cisco Security Agent (CSA), a host-based intrusion detection software package, must be installed on every PC in the Job Corps network. The CSA detects unusual activity at the local-PC level and stops the activity based on a user profile and a set of configured rules that reside on a central server. CSA will prevent a virus-infected PC from infecting other PCs on the network.