

COLORADO DEPARTMENT OF LABOR AND EMPLOYMENT
STANDARD POLICY AND PROCEDURE

<u>STANDARD POLICY</u> <u>AND PROCEDURE</u>	COLORADO DEPARTMENT OF LABOR AND EMPLOYMENT 1515 Arapahoe Street Denver Colorado 80202 Remote Access and Security	NUMBER: SPP-0008 DATE: August 16, 2004 SUPERSEDES: N/A DATE: EXECUTIVE DIRECTOR'S APPROVAL:
--	--	--

I. PURPOSE2

II. BACKGROUND 2

III. POLICY.....3

IV. APPLICABLE GUIDELINES4

V. PROCEDURES6

I. Purpose

The purpose of this Standard Policy and Procedure (SPP) is to (1) provide direction for and (2) mandate virus protection of remote access connections to the Department of Labor and Employment's (CDLE) networks.

II. Background

This SPP applies to (1) all CDLE employees, contractors, consultants, temporary, and other workers including all personnel affiliated with third parties accessing the CDLE network (VPN); and (2) implementation of secure networks that are directed through a security channel, or an IPSec Concentrator.

What is the VPN?

1. VPN stands for Virtual Private Network. It is the software that allows you to safely log into the CDLE private network from a remote location.
2. Because a PC can only be connected to one network at a time, you will have to log out of any programs you may have been using before using VPN to log into the CDLE private network.
3. When you are finished using the CDLE private network resources, you must remember to disconnect from the VPN connection to the CDLE private network before using your normal programs like Joblink or email.

Why use the VPN?

1. Security of the network and the data contained therein.
2. Certain things are only available throughout the department's private computer network, like the Intranet home page and EDSys.
3. Logging into the department's private network via the VPN can be used via Windows Remote Desktop or PC Anywhere to an individual PC that is physically located on the private network at the two main Denver office locations.
4. VPN is for people whose main PC is at one of those buildings, who sometimes work at other locations, and need to access their files via laptop or another remote PC.
5. You must have special permission and software for this kind of access, so if this is something you need to do, please contact your manager.

III. Policy

1. Only approved CDLE employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPN's, which are a "user managed" service.
 - a. Some special cases are temporarily granted for users not otherwise authorized.
 - b. "User managed" service means that the user may be responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and possibly paying associated fees.
2. The Request For Services (RFS) system will be used to request VPN access.
3. IMO's InfoSec will be responsible for ensuring the correct authorized usage of VPN for CDLE employees.
4. If, for any reason, the VPN connection generates malicious traffic or InfoSec believes that unauthorized access has being granted, the user's VPN connection can be cancelled.
 - a. If cancelled, the HELP Desk should be contacted for details on the cancellation.
 - b. The user assumes responsibility for ensuring that there is no malicious traffic on their machine.
5. All non-CDLE users will be responsible for setting up any anti-virus and anti-spyware and Microsoft patch programs on their PC's to ensure that the VPN Client computer is properly protected. Malicious traffic could still be generated if the VPN Client PC is connected to another network at the same time.
6. All non-CDLE users will be responsible for ensuring that they are not echoing other traffic into CDLE's networks. Contact the CDLE HELP Desk for questions on echoing.
7. The process of allowing other machines to be connected to the VPN Client PC while connecting into VPN is called Dual or Split tunneling.
 - a. Dual (split) tunneling is ONLY permitted with IMO approval and coordination.
 - b. Contact the CDLE HELP Desk for questions on Dual or Split tunneling.
8. When any user creates a password for their VPN account, they need to ensure that it is not a word found in the dictionary and also a word that they do not store locally on their machine or on a piece of paper that others can read.
 - a. They should use a strong password.
 - b. A strong password is usually one that has both alpha and numeric characters, is at least six (6) characters long and cannot be easily guessed.

9. VPN users will be automatically disconnected from CDLE's network after 45 minutes of inactivity.
 - a. The user must then log-on again to reconnect to the CDLE private network.
 - b. 45 minutes may seem like a long time but UI Tax and Boiler/Oil Inspection users may have longer periods of inactivity on their laptops while at field locations and need the extra time.

10. Pings or other artificial network processes are not to be used to keep the connection open.
 - a. The VPN connector will be limited to an absolute connection time of ten (10) consecutive hours.
 - b. There are typically 8 hours in a normal business day, but there are CDLE employees that work more than a normal 8 hour workday.
 - c. For this reason, it was felt reasonable to accommodate users that work more than 8 hours.

11. Only IMO approved or supplied VPN clients may be used. While using VPN technology with personal equipment to connect to the CDLE networks, non-CDLE users must understand that their machines are a de facto extension of CDLE's private network, and as such, are subject to the same rules and regulations that apply to CDLE-owned equipment.

12. Any employee found to have violated this policy might be subject to corrective and/or disciplinary action, up to and including termination of employment.

IV. Applicable Guidelines

Published State of Colorado, Federal government and private sector documentation regarding remote computer security.

V. Procedures

1. If the remote computer is a CDLE computer, please follow any information distributed from the Help Desk on ensuring that the patches and Trend Micro definitions are current.
2. If the remote computer is a non-CDLE computer, the user needs to make sure that their anti-virus software is current and that they have the current Microsoft patches installed.
3. Microsoft patches can be installed by going to the Internet Explorer and using the Tools->Windows Update menu options. The user needs to consult their anti-virus software company for procedures on ensuring that their anti-virus signatures are current.
4. A user that needs VPN access must complete a RFS (Request For Service) and obtain supervisory approval for access into VPN.
5. The InfoSec group from IES will provide the CDLE user the required software and installation instructions as well as userid and initial password when they complete the RFS.
6. If an issue is encountered with the VPN instructions, the Help Desk can be contacted during their business hours of 7:00 a.m. – 5:00 p.m. at (303) 318-8300.
7. How to Access the VPN.
 - a. Close out of any programs you are currently using. Your screen should show the Windows desktop.
 - b. In the lower left hand corner of the screen, click the START button. The START menu should open.
 - c. Click on the ALL PROGRAMS menu option. A list of programs should pop up to the side.
 - d. In the list of programs, click on CISCO SYSTEMS VPN CLIENT. A list of programs associated with the VPN should appear.
 - e. Choose VPN DIALER from the list.
 - f. The VPN dialog box should open.
 - g. In the CONNECTION ENTRY list box, enter or select the text CDLE VPN.
 - h. In the HOST NAME OR IP ADDRESS OF REMOTE SERVER list box, the text “165.127.89.4” should already be entered.

- i. Click the CONNECT button. There should be a pause while the connection is established. The USER AUTHENTICATION dialog box should then appear.
- j. In the USERNAME dialog box, enter your CDLE network USER ID (your “Qxxxxx” number). The ID should then appear in the list box.
- k. In the PASSWORD list box, enter the VPN password supplied to you by the CDLE Help Desk. Asterisks should then appear in the list box.
- l. Note: You should have been supplied your username and password by the CDLE Help Desk. ID’s and Passwords are case sensitive, so if you have your CAPS LOCK key on, the system may not recognize them.
- m. Click OK. There should be a pause while you are logged into the CDLE network. You should then receive a dialog box telling you that login is complete.
- n. Click CONTINUE. The dialog box should close and you now have access to the CDLE network and features like the CDLE Intranet Home Page and EDSys.
- o. Note: Network security for those logging into the CDLE network outside of the two main buildings is very sensitive. This is to prevent any unauthorized access. If you enter the incorrect log in information five times, you will be locked out of the VPN and will have to be reset by the CDLE Help Desk, (303) 318-8300, before you may attempt to access it again.
- p. Once you have gained access to the CDLE network, open INTERNET EXPLORER. The internet should open and display your default home page.
- q. In the ADDRESS list box toward the top of the screen, type ‘<http://s-dole-web>’ and hit the ENTER key. The CDLE Intranet home page should then display on your screen.
- r. Note: Some features on the CDLE Intranet, like the IMO RFS (“Request for Service”) and Facilities’ RFBS (“Request for Building Service”) require an internal ID and password. You should know when trying to access these features because you should get an additional login box. If these features are needed, contact the CDLE Help Desk to request an ID and password.

8. How to Access the CDLE Intranet.

- a. You must contact your manager to have an internal account created for you by IMO. Once you have been assigned this ID you can access the Intranet features that require this.

- b. Click on the feature you want to access. A LOGIN dialog box should appear.
- c. In the user name list box, enter CDLEINT\xxxxxx where the Qxxxxx represents your “Q” number. The text should appear in the box.
- d. In the password list box, enter the password IMO issued to you for your internal account. Asterisks should appear in the list box.
- e. Press the ENTER key. You are logged into the feature application.
- f. Note: You must log in using this same internal user ID and password when using PC Anywhere or Windows Remote Desktop to access your PC in your Denver office.
- g. When you have completed your business, you may log out of the CDLE Intranet.

9. How to Access EDSys.

- a. Once you are in the CDLE Intranet, click on the EMPLOYEE DATA SYSTEM link toward the right side of the screen. The login dialog box for EDSys should appear.
- b. In the USER ID list box, type your “Q” number. The text should be entered in the box.
- c. In the PASSWORD list box, type your EDSys password. Asterisks should appear in the list box.
- d. Note: If you do not have an EDSys password, please contact the HELP Desk who will initiate the password for you. You can then change it to one of your choosing. Instructional material for using EDSys is available on the CDLE Intranet home page. Click on one of the links under EDSys to access the material.
- e. When you have completed your business, you may log out of EDSys.

10. How to Log off the VPN.

- a. Double-click on the VPN PADLOCK ICON in the lower right corner of the screen. The VPN Status Box should open.
- b. Click on the DISCONNECT button. The dialog box should close and the connection should be terminated.