

**COLORADO DEPARTMENT OF LABOR AND EMPLOYMENT
STANDARD POLICY AND PROCEDURE**



Rick Grice
Executive Director

SUPERSEDES: DL(OIS) 90-174, DL(OIS) 91-9, SPP NUMBER: SPP-0026
DL(ADM) 99-5, SP-71, SP-89, DATE: 3/27/06
SP-159, SP-223, SP-229, SP-230
SUPPLEMENTS: DL(ADM) 02-03, SPP-0001, SPP-0002, SPP-0008

EXECUTIVE DIRECTOR'S APPROVAL:

SUBJECT TITLE: Information Technology Security & Usage Policies and Procedures

CATEGORY/UNIT: Information Management Office	AUTHOR: Rich Helton
SUB-CATEGORY: Information Technology Security	DISTRIBUTION: All CDLE Employees

PURPOSE: To understand that certain security and confidentiality procedures need to be adhered to so that CDLE information systems can continue to operate in a safe and efficient manner.

ACTION: All CDLE employees must read and understand the importance of this SPP. The overview is provided on pages 3 and 4 for quick reference. Details are described on pages 6 through 11.

Table of Contents

Section Name: Page

Overview of SPP. This overview is presented to provide the reader with the basics of each section. If more detail is desired or required, use the table of contents below to obtain the additional information. This page will generally assist the reader in understanding the complexity of and need for IT security. 3

I. Purpose 4
 1. Purpose
 2. Guiding Principles
 3. Definitions

II. References 5

III. Responsibilities 6 - 7
 1. CDLE Employees
 2. Appointing Authorities
 3. Chief Information Officer
 4. Chief Information Security Officer
 5. Information Security Unit
 6. IMO HELP Desk
 7. RFS System
 8. Contractors
 9. Investigations and Criminal Enforcement Unit
 10. Office of Human Resources

IV. Policy Statements 8 – 11
 1. Compliance
 2. Passwords/Pass Phrases
 3. Unsuccessful Logins
 4. Electronic Signatures
 5. Identification Fraud
 6. Anti-Virus Protections
 7. Hacking/Monitoring Tools
 8. Connectivity to CDLE Network
 9. Remote Connectivity to CDLE Network
 10. Peer to Peer (P2P) Connectivity to CDLE Network
 11. Email
 12. Site Security
 13. Protecting CDLE from Home Personal Computers

V. Recommended Best Practices 12

VI. Prohibited Practices Reminders 12

Overview of SPP.

- I. Purpose. To understand that certain security and confidentiality procedures need to be adhered to so that CDLE information systems can continue to operate in a safe and efficient manner. Page 4.
- II. References. List of governing documents related to IT security. Page 5.
- III. Responsibilities. Pages 6 – 7.
 1. This SPP applies to all divisions, offices, and units in CDLE. At each level, authority, responsibility and accountability must be consistently executed.
 2. CDLE employees must protect their password(s)/data from anyone but themselves.
 3. CDLE employees must use CDLE data for business purposes only.
 4. CDLE employees must secure and maintain equipment assigned to them.
 5. CDLE employees must simply LOG OFF their computers at the end of a business day or week. DO NOT TURN OFF THE COMPUTER unless directed to by the IMO HELP Desk.
 6. Appointing Authorities are responsible for ensuring security of CDLE's information systems, data and equipment.
 7. Appointing Authorities have the authority to allow other parties to access their data.
 8. Chief Information Officer (CIO) has overall responsibility for the operation, design, and development of CDLE information systems.
 9. CIO has overall responsibility for ensuring the security, availability, confidentiality, and integrity of CDLE information systems and communication networks.
 10. IMO HELP Desk is the Single Point of Contact for employees that have IT security questions or encounter IT security issues using the CDLE information systems. The IMO HELP DESK will attempt to resolve the questions/issues and/or relay those questions/issues to the CISO.
 11. Request For Service (RFS) is the primary document used to request IT support. It is available online via the CDLE Intranet page.
 12. Contractors are given access only to CDLE information systems that relate to their contract.
 13. Investigations and Criminal Enforcement (ICE) is empowered to conduct criminal investigations involving crimes affecting CDLE including IT related cases.
 14. The Appointing Authority, or designee, has the responsibility for employee in-processing and out-processing including retrieval and/or accounting of IT assets.
 15. Responsibility for the physical security of the CDLE building at 251 E.12th Avenue is vested in the Director, Unemployment Insurance. Responsibility for the physical security of the building that CDLE occupies at 633 17th street is vested with the building's landlord.
- IV. Policy Statements. Compliance, Passwords/Pass Phrases, Unsuccessful Logins, Electronic Signatures, Identification Fraud, Anti-Virus Protections, Hacking/Monitoring tools, Connectivity to CDLE Network, Remote Connectivity to CDLE Network, Peer to Peer (P2P) Connectivity to the CDLE Network, Email, Site Security, and Protecting CDLE from Home Personal Computers. Pages 8 - 11.
- V. Recommended Best Practices. Page 12.
- VI. Prohibited Practices. Page 12.

I. Purpose

1. The purpose of this SPP is to ensure the security, availability, confidentiality and integrity of the information systems and communication network(s) for all organizations within CDLE.
2. The guiding principles of this SPP are:
 - a. To guarantee the security of the information systems, the Information Management Office (IMO) must publish security policies, procedures and tools and maintain on-going processes to protect CDLE's information systems.
 - b. To guarantee the availability of the information systems, users must respect their use to minimize their negative impact to CDLE operations.
 - c. To guarantee the confidentiality of the information systems, users must ensure that proper policies and procedures are employed to protect CDLE's confidential information, to prevent identity theft of Colorado citizens, and to prevent fraudulent use of the State's resources.
 - d. Unauthorized use of CDLE information systems will be subject to investigation by the Investigations and Criminal Enforcement (ICE) unit and subject to disciplinary action based on Appointing Authority decision. IMO will assist in such investigations.
 - e. IMO personnel will monitor the CDLE Information systems to ensure that the systems meet the conditions of availability, confidentiality and integrity.
 - f. Only designated IMO security personnel will perform security audits on the information systems. The CDLE Chief Information Security Officer (CISO) will be responsible for the security of CDLE's information systems. If necessary, the CISO will contact CDLE's ICE unit for assistance.
 - g. The HELP Desk can be contacted by the user if there are any issues or concerns.
3. Definitions:
 - a. Authentication – is the process of validating that the users are who they say they are. This is usually represented in the form of a User ID and password. See paragraph III.2.c.
 - b. Authorization – is the process of validating that the users are accessing the proper information. Access is granted through the RFS system. The Appointing Authority of the system must approve the RFS. The RFS system is administered by IMO. See paragraph III.2.c.
 - c. Information systems -- any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. Information systems, in this case and not limited to, refers to such equipment as desktop and laptop computers, printers, scanners, servers, routers, switches, etc.; but not such equipment as copiers and fax machines.

II. References. Short list to address security for the entire Department.

1. State of Colorado, Colorado Judicial Department, "Electronic Communications Usage Policy: Technical, Security, Content and System Management Concerns", Final Draft, May, 2004, or its latest version on the state's website.
2. State of Colorado, Commission on Information Management and Governor's Office of Innovation and Technology, "Information and Technology Management Code", draft v.08, October 2, 2005, or its latest version on the state's website.
3. State of Colorado, Office of Information Technology, "Colorado Data Destruction Policy and Computer/Other Electronic Media End-of-Life Policy", July 1, 2004.
4. State of Colorado, Architecture Advisory Board, "Information Technology Standards", v1.2, June 18, 2004.
5. State of Colorado, Information Security Task Force, "Information Security Strategy", v1.0, June 30, 2003.
6. U.S. Department of Labor, Information Technology Support Center, "Guidebook for Maintaining a Secure Operating Environment", October, 2003.
7. U.S. Department of Labor, Information Technology Support Center, "Security guidebook for Implementing UI Internet Applications", June, 2003.
8. U.S. Department of Labor, Information Technology Support Center, "Secure Internet Communications", September, 2002.
9. U.S. Department of Labor, Information Technology Support Center, "UI Security Risk Assessment Guidebook", September, 2001.
10. U.S. Department of Justice, Civil Rights Division, "IT Equipment Accessibility Checklist, undated.
11. U.S. Department of Justice, Civil Rights Division, "Software Accessibility Checklist", undated.
12. U.S. Department of Justice, Civil Rights Division, "Web Page Accessibility Checklist, undated.
13. Department of Labor and Employment SPP-0001, June 18, 2004, and SPP-0002, March 29, 2004.

III. Responsibilities

1. CDLE Employee responsibilities:
 - a. The employee is responsible for the safeguarding their password(s). See paragraph IV.2.
 - b. The employee is accountable for all IT equipment, especially laptops, that is assigned to them by CDLE.
 - c. The employee is responsible for the security of all IT equipment that is assigned to them by CDLE.
 - d. The employee shall only use CDLE's information systems for CDLE related business needs.
 - e. The employee is responsible for complying with this SPP.
 - f. If an employee has a question about this SPP, they should contact the IMO HELP Desk for possible resolution. If the IMO HELP DESK is unable to resolve the question, that information will be forwarded to the CISO.
2. Appointing Authority responsibilities:
 - a. The Appointing Authorities are the overall responsible parties for the security of their data.
 - b. The Appointing Authorities are the overall responsible parties for the conduct and compliance of this SPP by their employees. The EDSYS system identifies the Appointing Authorities and their employees. Appointing authorities may further delegate this responsibility to the supervisory level.
 - c. The Appointing Authorities assign, authenticate and/or authorize who has rights to use their data by using the Request for Service (RFS) system.
 - d. The Appointing Authorities may request an audit on their systems, data or employees from the CISO.
 - e. Upon termination of a CDLE employee, or the end of contract, the Appointing Authorities must issue an RFS to delete the employee /contractor's access to the CDLE information systems.
3. Chief Information Office (CIO) responsibilities:
 - a. The CIO is the overall responsible party for the operation, design and development of the information systems for CDLE. The CIO is responsible for ensuring that systems designed and/or developed by third parties are in compliance with this SPP and all other IT SPP's published by the state.
 - b. The CIO is the overall responsible party for ensuring the security, availability, confidentiality and integrity of the information systems and communication network(s) for all organizations within CDLE.
 - c. The CIO continually communicates the status of CDLE's information systems with the Executive Director and his management staff.
4. Chief Information Security Officer (CISO) responsibilities:
 - a. The CISO is responsible for ensuring that there is a designated Single Point of Contact (SPOC) for security issues that may affect the information systems.
 - b. The CISO is responsible for continual evaluation and enhancement of CDLE's security infrastructure.

- c. The CISO can disable a person's program, network packets, computer or other electronic medium if it is viewed as maliciously or improperly affecting other electronic systems with concurrence of that person's Appointing Authority.
5. Information Security unit (InfoSec) responsibilities:
 - a. The InfoSec is a unit that reports to the CISO who controls access administration to CDLE's information systems. The unit keeps an audit trail on who has access to the CDLE information systems.
 - b. The InfoSec unit issues User identification to all CDLE employees.
 - c. The InfoSec unit routinely audits the information systems to insure that they meet current security standards.
 - d. The InfoSec unit has the ability to monitor CDLE's data processing to ensure compliance to security standards.
6. IMO HELP Desk responsibilities:
 - a. The IMO HELP Desk is the SPOC for CDLE employees who have questions or encounter issues using the information systems.
 - b. The IMO HELP Desk is responsible for notifying the users of any concerns or outages.
 - c. The IMO HELP Desk will administer any connections of equipment to CDLE's information systems. This equipment includes telephones, laptops, printers, desktops, VPN, etc.
7. The Request for Services (RFS) system:
 - a. The RFS is used to receive a request from an employee for services from IMO.
 - b. Services include any scheduled work to/on the information systems. This includes changes in access, the addition or removal of hardware and software.
 - c. The requesting Appointing Authority, or their designee, may approve an RFS. When an Appointing authority approves an RFS, they are agreeing to changes and costs associated with the RFS.
8. Contractors: Access is given to contractors to the systems that they are working on during the timeframe needed to complete their contract and only during the duration of that contractual time.
9. Investigations and Criminal Enforcement (ICE) Unit:
 - a. Established in 1981, Investigations & Criminal Enforcement (ICE) is empowered to conduct criminal investigations involving crimes affecting the Department. Crimes investigated fall into categories of Workers' Compensation fraud, threats involving Department resources and personnel, internal breaches of program integrity, Unemployment Insurance claimant and employer fraud, and fraud against other programs including the explosives and petroleum storage tanks section.
 - b. Appointing Authorities, ICE, and the CISO may investigate employees for the misuse of CDLE's Information Systems. Misuse of CDLE's Information Systems may be considered fraud.
10. Office of Human Resources (OHRP) Unit: As the office responsible for all personnel actions, the OHRP conducts New Employee Orientation for new hires and exit processing for departing employees.

IV. Policy Statements

1. Users who fail to comply with the policies and procedures of this SPP may be subject to disciplinary action, including termination.
2. Passwords/Passphrases responsibilities of CDLE employees:
 - a. CDLE User ID's will be issued by the IMO.
 - b. User ID's must never be reassigned to another person.
 - c. Users are encouraged to use "passphrases" rather than "passwords". Passphrases are more difficult to "hack" and thus more secure than the traditional passwords. Passphrases should include at least one numeric character; e.g., "toothachegone1", or "Gone2lunch", or "4teeandstillgoing".
 - d. Passwords/passphrases are used to access the CDLE network and applications systems. Each application (e.g., EDSys) shall have its own security layers. Passwords/passphrases are changed as established in each application.
 - e. Passwords/passphrases shall be changed, as instructed by each application or when otherwise necessary.
 - f. Best practices for Passwords/passphrases stipulate they should be at least eight (8) characters long. It should include at least 3 out of the following 4 types of characters: at least one (1) lower case letter, one (1) upper case letter, one (1) numeric character, and one (1) special character, such as the # or % character.
 - g. All personnel must be diligent in protecting their User ID's and passwords/passphrases. Personnel shall not let any other person use their User ID or password/passphrase, nor shall they use another person's User ID or password/passphrase.
 - h. If users need to share data residing on a desktop computer, they should utilize message forwarding facilities; e.g., e-mail attachments; public directories on local area network servers; e.g., the 'Y' drive; and other authorized information-sharing mechanisms.
3. Access to CDLE's network or applications systems are shutdown after several failed attempts. The failed attempts will range from three (3) at DoIT to seven (7) CDLE failed attempts. This access shutdown procedure is in effect.
 - a. All requests for resetting passwords/passphrases must originate with the user, and not a surrogate, or someone who claims to know the user.
 - b. The IMO HELP Desk is the Single Point of Contact for these requests.
 - c. An Appointing Authority, or designee, must approve, or disapprove, any access granted to their system. These requests are submitted through the RFS process.
 - d. The IMO Access Control Group maintains a list of all infrastructure User ID's.
 - e. User ID's and "passwords/passphrases" will be inactivated from the application system or network for individuals who have no activity registered to those ID's for more than thirty (30) consecutive days. If an employee's absence for 30 or more consecutive days is known in advance, the supervisor must submit and RFS to have that employee's userid and "passwords/passphrases" temporarily inactivated. Upon return to work, that employee should submit and RFS to have the IMO HELP DESK provide a temporary "passwords/passphrases" allowing the employee to regain access.
 - f. Users shall not use family member names or other terms that could be attributed to the user as "passwords/passphrases".

- g. "Passwords/passphrases" will not be publicly posted in writing and/or easily accessible by others. Owners may write "Passwords"/"passphrases" down so long as it is not easily accessible by anyone else.
- h. User ID's and passwords/passphrases shall not be recorded in a macro.
- i. Passwords/passphrases shall not be stored such that someone can gain access to the network or application system with only a User ID. There are a few exceptions to this rule, such as the public kiosk, and any exception must be approved through the RFS system.
- j. The IMO's system and network administrators shall conduct User ID audits on a periodic basis. These are no-notice audits that are randomly performed to enhance security.
- k. Whenever an employee leaves CDLE, Appointing Authorities must notify the IMO's Access Control Group (via an RFS) to ensure that the access of the employee is terminated promptly after they have left CDLE.
 - 1) An employee's User ID is disabled on their last day of employment.
 - 2) It is the supervisor's responsibility to submit an RFS to disable the access of the employee.
 - 3) This disabling includes archiving instructions from the supervisor for the e-mail box on the employee's "J" drive.
 - 4) These archived items can be copied to CD (and supplied to the supervisor), transferred to another employee, or deleted.
 - 5) Failure to notify the IMO's Access Control Group at least one week in advance of the separation is a violation of this policy and will allow an unauthorized access to be active. The exception to this notification policy is when an employee leaves unexpectedly. In those cases, notification must be provided no later than the day the person leaves.
 - 6) If IMO discovers that access is still active after the termination of an employee, the access will be removed as quickly as possible. However, that unit's Appointing Authority will still be the responsible party regarding this noncompliance.
- l. The IMO's Access Control Group will disable the User ID's of users leaving the employment of the Department within eight (8) work hours of the user's last work day.

4. Electronic Signatures

- a. Refer to SP-247, July 16, 2003 for details.
- b. Do not scan and paste your signature into a Word Document.
- c. A scanned signature is not an electronic signature and is a dangerous procedure that may be copied by anyone receiving a Word document as an attachment and used.

5. Identification Fraud

- a. Identification fraud includes misrepresenting, obscuring, suppressing, or replacing a user's identity in an information system. Identification fraud is prohibited.
- b. The user name, e-mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings to avoid identification fraud. For assistance, contact the CDLE Staff Development Office or IMO HELP Desk.

6. Anti-Virus Protections

- a. When a user signs on, the system will automatically scan all hard drives with the anti-virus software to ensure that files do not contain a virus.
- b. Users, without opening, shall report any suspected virus to the IMO HELP Desk immediately.
- c. Only IMO shall install and administer CDLE's anti-virus software.

7. Hacking/Monitoring tools: CDLE employees are prohibited from downloading and using any hacking type tools, network scanning software or password/passphrase crackers, unless specifically approved and authorized by the CDLE CISO in writing.

8. Connectivity to the network

- a. Users shall log off the network when they leave their PC for more than thirty minutes. At the end of the work day, users also must log off, but WILL NOT shut down their machines unless specifically instructed to do so by the IMO. The user is responsible for the security of their area, password and ID.
- b. Log on/log off and turn on/off procedures are described in SPP-0002, March 29, 2004.

9. Remote connectivity to the CDLE network

- a. Remote access to the CDLE network must be arranged and registered through the IMO HELP Desk via RFS, for a virtual private network (VPN) connection or other IMO-approved communication access method.
- b. Users must be sure to close the VPN sessions on their remote computer when they are not using the CDLE network connection. However, users may maintain connection to the Internet Service Provider (e.g., MSN, AOL, etc) after they have closed their VPN session.
- c. The IMO's network administrator is responsible for maintaining a current and accurate list of all approved VPN connections.
- d. VPN connections will be deployed on CDLE owned and authorized equipment as part of standard suite of software.
 - (1) Personally-owned computers may be authorized by submitting and obtaining approval via the RFS process.
 - (2) Users must comply with all published VPN procedures and may be disconnected from their VPN connection and have their VPN connection privileges revoked for violation of these procedures.
- e. Remote connectivity (VPN) procedures are described in SPP-0008, July 16, 2004.

10. Peer to Peer (P2P) Connectivity

- a. P2P communications are not allowed. Examples are "Napster" and "Gnutella". Peer to Peer (P2P) connections to servers and personal computers outside the CDLE network are one of the most serious security threats that currently exist and are strictly prohibited.
- b. On the Internet, peer-to-peer is a type of Internet network that allows computer users from outside the CDLE network who share the same networking program as someone within the CDLE network to connect with each other. Thus, P2P connectivity allows someone outside the CDLE network direct access to that CDLE user's files from within the CDLE network.

11. E-Mail

- a. Care should be taken in opening any electronically received message. If the user is not familiar with the message sender, or with the site from which information is extracted, the message or file should not be opened. If there is a suspicion of an email message, the user should call the IMO HELP Desk to report a possible virus.
- b. Storage of email messages, procedures are described in SPP-0001, February 18, 2004.
- c. Use of E-Mail Messages is addressed in DL (ADM) 02-03, June 4, 2002.
- d. Intercepting, Monitoring Data and Users. Users shall not intercept data or user activity.

12. Site Security

- a. The IMO, located at 633 17th Street and 251 East 12th Avenue, Denver, is responsible for security of data centers including their assets and access to the assets therein.
- b. Overall physical security, on the other hand, is the responsibility of the building owner at 633 17th Street or CDLE's Unemployment Insurance unit at 251 East 12th Avenue.
- c. The CIO is the primary manager responsible for implementing, monitoring, and enforcing information technology compliance with site security policies at both locations.
- d. Access to Data Center Facilities is addressed in SPP-0016, March 2, 2005.
- e. Site Security at remote locations such as workforce centers, county offices, etc., is the responsibility of the building owner or CDLE's primary occupant of that location.

13. Protecting CDLE from Home Personal Computers

- a. When working at home and sending email to CDLE users from that user's home computer, it is the user's responsibility to have current antivirus software installed on their own personal computer.
- b. If discovered that such software is not installed on the home personal computer, the user may be solely responsible for any damage done to CDLE's information systems and/or its related assets.

V. Recommended Best Practices

1. Close VPN sessions when you are not using your CDLE network connection.
2. Promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the IMO HELP Desk at (303) 318-8300.
3. Keep your home PC current with anti-virus software and Microsoft updates especially when it is also used for work purposes.
4. Encryption is the encoding of data in such a way that it cannot be read without keys from the user to read the sensitive material. Keys are used to decrypt and encrypt data. Any confidential or sensitive data that is transmitted to or through unsecured areas of a network must be encrypted to protect the data. The confidential or sensitive data is defined by the business owners. All encryption used by CDLE information systems must also meet the standards specified in the State of Colorado's IMC Management Code.

VI. Prohibited Practices Reminder

1. **DO NOT** share individual User ID's or password/passphrases with anyone. To do so exposes the authorized user to responsibility for actions other parties take with the User ID and password/passphrase. Call the IMO HELP Desk if you have forgotten your password/passphrase.
2. **DO NOT** connect non-CDLE users to the CDLE Network without going through the IMO HELP Desk.
3. **DO NOT** use CDLE information systems for private business activities or amusement/entertainment purposes.
4. **DO NOT** open e-mail messages or attached files to e-mail messages if you are not familiar with the message sender, or with the site from which information is extracted. If the email appears to be malicious, please report it to the IMO HELP Desk.
5. **DO NOT** shut down your PC unless instructed to do so by IMO. IMO installs security updates to your PC remotely, and your PC needs to be on for this process to work. Simply log off the network and turn off the monitor when you will not be using the PC for a long time (e.g., lunch, overnight, on annual/sick leave, and over the weekend).