

Modern DCPDS and Security

A Few Important Points

The following has been taken from Appendix L 1, Security Features User's Guide, Defense Civilian Personnel Data System (DCPDS) System Security Authorization Agreement, February 9, 2000.

ALL USERS OF MODERN DCPDS ARE REQUIRED TO READ THROUGH THIS DOCUMENT.

L1.2.2 Your Security Responsibilities.

Your responsibilities with respect to properly using the modern DCPDS security features are:

- (1) Attend the initial security training as coordinated by your ISSO, prior to accessing the modern DCPDS. Participate in the security awareness program and in the annual refresher security training provided by your ISSO.
- (2) Learn and follow the security guidance provided by the modern DCPDS Security Policy, other applicable security directives and local operating instructions. Only use your access privileges for the intended purpose. Abuse of access privileges will result in access removal. All employees must have a copy of these operating instructions.
- (3) Protect modern DCPDS data and resources from unauthorized disclosure, modification, or deletion. Do not give unauthorized persons the telephone numbers of the modern DCPDS dial access modems. Dial-in modems should not be connected to the system unless absolutely necessary and validated as part of the system. Protect storage media as sensitive information - For Official Use Only or Privacy Act. When not in use, store removable media in lockable containers. Secure your office after duty hours and during periods when the office is unmanned. Make backup copies of your work and protect the media appropriately. Mark and protect sensitive-unclassified output appropriately.
- (4) Protect your password as For Official Use Only (FOUO). Your password is considered to be sensitive-unclassified information and is not to be shared with anyone. Change your password when instructed by the system; you have no choice not to change the password. Failure to change the password when directed will result in lockout from the system. If you feel that your password has been compromised, change it immediately and notify your ISSO.
- (5) DoD requires anti-viral software be used on all government owned equipment. Use the anti-viral software installed on your system to scan all files from external sources and disks prior to initial use. Scan all software for viruses prior to initial use. Do not install or use privately owned, personally developed, public domain, or shareware software on your system without prior authorization. Notify your ISSO of all suspected or confirmed virus attacks.

- (6) Log out of Oracle HR when you leave your workstation unattended for an extended period of time. Alternatively, turn on the automatic password protected screen-saver or lock screen capability so that the screen saver activates when the system is left unattended.
- (7) Protect from unauthorized view the entry of your password or the display of sensitive-unclassified data on your workstation. Do not write your password down. You may be held responsible for the actions attributed to the misuse of your password.
- (8) Comply with your site's security policies on use of the Internet (WWW), downloading of files, and e-mail.
- (9) Do not modify or change the hardware or software configuration of your workstation by adding unapproved hardware or software. Do not bypass any surge protection or power line conditioning devices installed on your system.
- (10) Do not download unapproved or personally owned software to your PC except where authorized and pre-approved by the ISSO.
- (11) Notify your ISSO of any security vulnerabilities associated with the operation and use of the modern DCPDS (e.g., the system grants you access to information which you are not authorized).
- (12) Comply with local policies concerning smoking, eating, and drinking around government computers.
- (13) Notify your ISSO and/or supervisors when you will be away from your office for more than 30 days. Supervisors must notify the ISSO when an employee no longer requires access to the modern DCPDS so system and database access can be removed.
- (14) Address all security related questions to your Supervisor or ISSO for resolution. To properly purge or clear storage media, consult with your ISSO.
- (15) Notify your ISSO of all suspected or confirmed intrusion attempts (i.e., hacker attacks). When the system displays the last date, time, and location at which your UserID was used; make sure it is correct! When the system advises of unsuccessful logins since your last session, ensure that it was you and not someone attempting to use your *User Name/Password* combination.

L1.4.4.1 Password Length and Structure.

a. Your password is the most vulnerable point for any hacker to break into your computer system. Taking care in choosing and protecting your password is the single most important contribution you can make to the security of the modern DCPDS. You should use a password that begins with an alpha character and contains at least one special character. The special characters for Oracle HR are the dollar sign (\$), the number sign (#), the numbers 0 through 9, and the underscore (_). The password should consist of a combination of letters and numbers (or special characters) and be eight (8) to ten (10) characters in length. Avoid passwords that are either all numbers or all letters to the greatest extent possible. Never select a

password that is related to your personal identity, history, or environment. Never select a word that can be found in a dictionary.

b. A simple method for developing a password is to create a phrase that you can remember and then use the first character of each word for your password. Some examples include:

Sample Pass Phrases	Resulting Password
I have been happily married for 22 years	Ihbhm f22y
I was awarded the CISSP designation in 96	IwatCdi96
We have 2 bathrooms in our new house	Wh2bionh
She graduated from College with a 3.7 GPA	Sgfcwa3GPA
I enlisted in the Army in 1997	IeitAi97

WARNING: Do not use any of the above examples as your password.

L1.5.10 Clearances.

a. A security clearance is not required for access to sensitive-unclassified information. However, all persons accessing the modern DCPDS, at minimum, will have a completed National Agency Check (NAC, ENTNAC, or equivalent). (Appendix D security requirement reference - Para D5.1)

b. Supervisors will consider limiting or removing access, if unfavorable information should come to light about an individual, especially if the individual concerned is considered to be a disgruntled employee. Supervisors will make sure such information is properly documented in the employee file. (Appendix D security requirement reference - Para D5.1)

L1.5.15 Entry Controls to Workstations.

a. All workstations and terminals capable of accessing the modern DCPDS will be provided the level of physical security as specified by local security policy for AIS hardware. ISSOs share responsibility for the physical protection and use of these assets with the actual users. (Appendix D security requirement reference - Para D6.3)

b. All workstations used to access the modern DCPDS will use password protected screen saver programs or similar features, where available, to protect against users leaving their workstations unattended for short periods of time. Where features are not available, users will log out of the system before leaving their workstation unattended. (Appendix D security requirement reference - Para D6.3)