



United States Department of the Interior

BUREAU OF LAND MANAGEMENT

California State Office
2800 Cottage Way, Suite W1834
Sacramento, California 95825
www.ca.blm.gov

January 22, 2002

In Reply Refer To:
1280P
(CA-946)

EMS TRANSMISSION: 1/22/02
Instruction Memorandum No. CA-2002-023
Expires 09/30/2003

To: All CA Employees
From: State Director
Subject: Policy on the Use of Strong Passwords

This Instruction Memorandum (IM) provides direction established by Washington Office IM No. 2002-064, Policy on the Use of Strong Passwords. The direction is intended to strengthen Information Technology (IT) measures designed to protect against unauthorized disclosure of information.

You are directed to use the strictest protection to prevent unauthorized access to information stored on BLM computers. This policy applies to all computers, including those used on the desktop, portable computers, devices and computers used offsite.

The following Password Policy is now in effect for BLM systems:

- Passwords will be eight or more characters in length.
- Passwords must contain a mix of uppercase and lowercase letters.
- There will be at least one numeric character (0,1,2,3...9).
- There will be at least one special character (e.g., %, &, #, *, etc.)
- Passwords are to be changed at required intervals or, at a minimum, every 90 days.
- System Administrator passwords will be changed every 30 days.
- There will be no reuse of passwords allowed for at least 8 changes.
- Your account will be locked out after five failed password entries and can only be cleared by the IT Security manager or his/her delegated authority.
- Passwords may not be used until 180 days have passed since their last usage.
- When changing your password, at least two characters must be unique, meaning they were not used in the previous password. Reuse of the same password with a different suffix (1, 2, 3) shall not be permitted.

Specific directions for changing your password can be found on California's Intranet Site at: <http://web.ca.blm.gov/casys/NTadministration/ChgPasswordsAuto/chgpasswordsauto.html>. You are responsible for all activity logged under your User ID. Violations of this password policy can result in

cancellation of an account, loss of future access and disciplinary actions when appropriate. State Office and Field Office system administrators shall ensure that all Windows NT servers and workstations are configured to automatically lock after 15 minutes of inactivity (requiring users to re-authenticate). Other operating systems in use by the BLM should be configured similarly if technically possible.

2

User IDs and passwords are not to be disclosed or shared with anyone, including BLM systems administration personnel. If you believe your User ID or password have been compromised, immediately change your password and notify the IT Security Manager, Chuck McCoy at (916) 978-4543. Passwords will be changed at required intervals or any time you feel the possibility exists that it may have been compromised. Here are some basic rules when creating passwords:

1. **Do not use personal information (e.g., telephone numbers, names of family members, pets, etc.) for your passwords.**
2. **Do not tape user IDs and passwords to desks, walls, or monitors, or write them down and store them in list finders, desk drawers, etc.**
3. **Do not store user IDs and passwords in an unsecured computer file. This is especially important for laptop, notebook, and handheld computers since they are easy targets for theft.**
4. **Do use passwords that are hard to guess but easy to remember.**

An excellent method of creating a very strong password is to combine, rearrange, and jumble a two-word phrase. For example, use the two-word phrase "hot cat". "Hot cat" contains six characters so put the number "6" in the middle of the password, then reverse the spelling and capitalize the first letter of the first word to get "Toh6tac". If you add an * to the end of the password you get the very strong password "Toh6tac*", which meets all of the password rules and can be easily remembered.

This IM is effective upon receipt. Employees will be required to change passwords on their desktop computers the first time a login attempt is made after close of business January 22, 2002. Local IRM staff will assist as needed to implement this policy on other BLM computers.

BLM is currently updating its security policy, including its policy of access and authentication, through its Manual and Handbooks. These incorporate the latest guidance from the Office of Management and Budget, the National Institutes of Standards and Technology, and the Department of the Interior. In light of the threats to sensitive BLM information, certain recommended practices concerning password protection are being implemented in order to ensure that proprietary data is not tampered with or inadvertently or otherwise disclosed. While there are controls in place to protect the physical security of our information infrastructure, the BLM recognizes that each networked computer is a potential source of intrusion from hackers. Since user names and passwords are the first line of defense against such intrusion, the BLM has elected to adopt this policy to protect BLM corporate data.

For questions regarding this IM, please contact Rob Cervantes at (916) 978-4541.

Signed by:
James Wesley Abbott
Associate State Director

Authenticated by:
Richard A. Erickson
Records Management