Form 1264-3
(February 2004)

UNITED STATES
DEPARTMENT OF THE INTERIOR

BUREAU OF LAND MANAGEMENT

National Information Resources Management Center (NIRMC)
Building 40, Denver Federal Center
P.O. Box 25047
Denver, CO 80225-0047

INDIVIDUAL COMPUTER USER'S STATEMENT OF RESPONSIBILITY

I, the undersigned understand that when I use any of the BLM Computer Systems and/or Automated Information Resources or gain access to any information therein, such use of access shall be in accordance with current policy. Further, I understand that any use of the aforementioned systems or information that is not in accordance with current policy may result in disciplinary action consistent with the nature and scope of such activity.

I have read the "IT SECURITY RULES OF BEHAVIOR" attached hereto. I understand and agree to comply with them.

□ Federal Employee □ Other Non-Federal ______________________________
(User Organization/Name of Company/Agency & Mail Code)

□ Contractor Employee ______________________________
(Contractor Company Name)

____
(Employee's Typed or Printed Name)

____
(Signature) (Date)

***Failure to sign and return the Individual Computer User's Statement of Responsibility (Form 1264-3) to the IT Security Manager will result in a User-ID not being established. A copy of the signed statement will be made a part of your Official Personnel File.**

Form 1264-3
(February 2004)

IT SECURITY RULES OF BEHAVIOR

Violations of the following rules are considered security incidents. According to the Department of the Interior Manual 375 DM 19, “all suspected, actual, or threatened incidents involving the destruction, physical abuse or loss of technological resources shall be reported to the appropriate authorities.” BLM employees shall report observed security incidents to their supervisors or to the local IT Security Manager. The local installation Information Technology Security Managers (ITSM) may recommend the removal of any individual’s User ID and password from any BLM computer system and/or automated information resources system in the event of a security incident.

1. No classified National security information will be entered into any BLM computer system.

2. Computer hardware, software, and data of the BLM are considered to be the property of the U.S. Government. BLM computer systems shall be used for official business only. No personal software, private data, unlicensed proprietary software, or otherwise nongovernmental information will be used on or entered into any Government-owned computer system.

3. Commercially developed and licensed software shall be treated as proprietary property of its developer.
   Title 17 of the U.S. Code states that “It is illegal to make or distribute copies of copyrighted material without authorization.” The only exception is the user’s right to make a backup for archival purposes, assuming one is not provided by the manufacturer. It is illegal to make copies of software for any other purpose without the permission of the publisher. Unauthorized duplication of software is a Federal crime. Penalties include fines of up to $100,000 per infringement and jail terms of up to 5 years.

4. Individual User IDs and passwords are assigned to each person having a valid requirement to access any BLM computer and local/wide area networks. All activity accomplished under this User ID is directly attributable to the user to whom it is assigned. It is, therefore, to be used only by the individual user.

   Remember, you are responsible for all activity logged under your User ID.

5. Do not attempt to access any data contained on BLM computer systems for which you do not have authority to access or do not have a specific need-to-know. If the need to access a computer system has been established through the appropriate supervisory channel, the request to grant access shall be made to the system owner.

6. User IDs and passwords are not to be shared with or disclosed to anyone. If you believe your User ID and password have been compromised, immediately change your password and notify the local ITSM. Passwords should be changed at required intervals or any time you feel the possibility exists that it may have been compromised.

7. Never use personal information (e.g. telephone numbers, names of family members, pets, etc.) for your passwords. Password characteristics are listed in IM No. 2002-064, dated 01/04/02. For example:

   - 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.
   - There will be at least one special character (e.g., %, &, #, *, etc.).

8. User IDs and passwords should not be written down, except on the original assignment document. This document should then be destroyed or, at a minimum, be kept in a locked safe or cabinet. Under no circumstances should User IDs and passwords be posted ANYWHERE!

***Failure to sign and return the Individual Computer User’s Statement of Responsibility (Form 1264-3) to the IT Security Manager will result in a User-ID not being established.**

A copy of the signed statement will be made a part of your Official Personnel File.