

UNITED STATES
DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT
Idaho

Individual Computer User's Statement Of Responsibility

I, the undersigned, understand that when I use any of the BLM General Support Systems and/or applications or gain access to any information therein, such use or access is limited to official Government business. Further, I understand that any use of the aforementioned systems or information that is not official Government business may result in disciplinary action consistent with the nature and scope of such activity.

I have read the "General Rules and Guidelines Governing the Use of BLM General Support Systems" attached hereto. I understand and agree to comply with them.

Federal Employee

Agency / Organization / Mail Code

Non-Federal

Name of Organization / Company

Contractor Employee

Contract Company Name

Individual's Typed or Printed Name

Individual's Signature

Date

NOTE: Submit this signed statement to the local System Administrator or the Information Technology Security Manager

PRIVACY ACT STATEMENT

This information is collected according to The Computer Security Act of 1987 (P.L. 100-235) that requires agencies to protect information residing in computers from misuse and unauthorized access; The Privacy Act of 1974, as amended (5 U.S.C. 552 (a), and 43 CFR Part 2, Subpart D. This information is covered by Privacy Act System Notice INTERIOR/OS-58 and is subject to Privacy Act requirements. The primary uses of the records are administrative in nature and reflect the requestor's relationship to the General Support System and/or the Administrative Information Systems for which access is requested. Records may be maintained in paper or electronic form. Disclosure is restricted to persons and situations identified in 43 CFR 2.56. Furnishing the information on this form is voluntary but failure to do so may result in disapproval of the request.

GENERAL RULES AND GUIDELINES GOVERNING THE USE
OF
BUREAU OF LAND MANAGEMENT
GENERAL SUPPORT SYSTEMS

According to the Department of Interior Manual 375 DM 19.10B, "It is the responsibility of each employee to report all suspected, actual or threatened incidents involving automated information systems to the authorities indicated below."

- \$ Bureau of Land Management (BLM) employees will report observed computer security incidents or suspected computer security violations immediately to the Installation Information Technology (IT) Security Manager and to their supervisors.
- \$ The BLM Installation IT Security Manager may recommend the removal of any individual's User ID and password from any BLM computer system and/or application system in the event of a security incident.
- \$ Unauthorized access or misuse of BLM General Support Systems may subject violators to criminal, civil or administrative action. Criminal Penalties include fines and/or imprisonment of up to 20 years. Disciplinary action for administrative violations of the following rules may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or other action as deemed appropriate.

Violations of the following rules are considered computer security incidents:

1. CLASSIFIED INFORMATION. Do not enter any classified National Security information into any BLM General Support System.
2. GOVERNMENT PROPERTY. Computer hardware, software, and data of the BLM are considered to be the property of the U.S. Government. BLM computer systems are used for official business only. Do not use games, personal software, private data, unlicensed proprietary software, or otherwise non-government information or enter them into any Government-owned computer system. Any use of computers, software or data for other than official business is expressly prohibited, except as permitted by the BLM Internet Acceptable Use Policy and the Department's Policy on Limited Personal Use of Government Office Equipment and Telephone Use.
3. PROPRIETARY PROPERTY. Commercially developed and licensed software is treated as proprietary property of its developer. Title 17 of the U.S. Code states, "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 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 five years.
4. ACCOUNTABILITY. Individual User IDs and passwords are assigned only to persons having a valid requirement to access BLM General Support Systems and local/wide area networks. All activity accomplished under this User ID is directly attributable to the user to whom it is assigned.

GENERAL BUSINESS PRACTICES, if not followed, can lead to security incidents as listed below. Noncompliance with these practices may result in removal of access and/or disciplinary or legal action being taken, consistent with the nature and scope of such activity.

1. INDIVIDUAL USER IDs AND PASSWORDS. Do not share your individual User IDs and passwords. They are to be used only by the individual owner. Do not write down user IDs and passwords, except on the original assignment document. Destroy this document once memorized, or at a minimum, keep it in a locked safe or cabinet.

Under no circumstances should User IDs and passwords be posted ANYWHERE! Do not keep them in accessible locations. Never use personal information (e.g., telephone numbers, names of family members, pets, etc.) or dictionary words for your passwords. Passwords are six to eight characters in length and consist of at least one numeric character and a special character. Passwords are changed at required intervals. If you believe your User ID and password have been compromised, change your password, notify your supervisor, and report the incident to the Installation IT Security Manager.

2. UNAUTHORIZED ACCESS. Access to BLM computer systems requires management approval. Do not attempt to gain access to any Information Technology system for which you do not have an approved and authorization to access.
3. LOG OFF when not actively working on the computer system. At a minimum, lock your workstation when leaving your work area for short periods of time or invoke the computer system's locking screen saver. Remember, you are responsible for all activity logged under your User ID.

FAILURE TO SIGN AND RETURN THE ATTACHED INDIVIDUAL COMPUTER USER'S STATEMENT OF RESPONSIBILITY TO THE INSTALLATION IT SECURITY MANAGER within two weeks of issue will result in the removal of the User ID and password from the system(s).

USER: DETACH AND RETAIN GENERAL RULES AND GUIDELINES FOR YOUR FUTURE REFERENCE