# Office of Natural Resources Revenue
# Acceptable Use Policy for External Users
**Updated: 12/2010**

## Purpose

The ONRR Acceptable User Policy is intended to establish the acceptable use policies and computing practices expected of external users who access ONRR systems, and to define inappropriate and prohibited actions. ONRR data, hardware and software are the property of the Federal Government and must be protected at all times. This document establishes required acceptable use policies as specified by OMB Circular A-130, DM 375 Chapter 19, and derived from other related laws, policies, directives, memorandums and bulletins.

## Scope

The ONRR Acceptable Use Policy applies to all authorized users of any ONRR Information Technology (IT) systems or resources. IT resources include electronically-stored information, computer equipment, software, output, and storage media. All users shall be aware of their responsibilities, acknowledge their actions, and comply with the ONRR Acceptable Use Policy.

Access to ONRR IT systems shall not be granted to anyone until:

- Approvals for your access, as defined by the Department of the Interior (DOI) and the Office of Natural Resources Revenue (ONRR), have been obtained, reviewed, and accepted by ONRR.
- You have read, acknowledged, and documented your consent to abide by the ONRR Acceptable Use Policy.

Because written guidance cannot cover every contingency, you are expected to use sound judgment and the highest ethical standards in your decision making.

## Updates

ONRR reserves the right to add, delete or modify any provision of the ONRR Acceptable Use Policy at any time without prior notice, effective upon posting of the modifications on the ONRR web site. ONRR will make every effort to notify users of updated policies through its public web site.

## Penalties for Noncompliance

The ONRR Acceptable Use Policy is founded on principles described in the Department of the Interior (DOI) and ONRR published security policies, and other regulatory documents such as OMB regulations and NIST publications. These rules carry the same authority for compliance as the official documents cited above.

The ONRR shall enforce the use of penalties against any user who willfully violates any ONRR, DOI, or Federal system security policy or privacy policy.

Penalties may include, but are not limited to:

- Revocation of system account access
- Suspension of system account access
- Possible administrative, civil and/or criminal prosecution.

## Consent to Monitoring

There should be no expectation of privacy with respect to the use of ONRR IT systems or resources. ONRR IT systems, including all software systems and/or all related equipment, networks, and network devices (including Internet access), are provided by the ONRR for the explicit use of authorized users in accordance with the ONRR Acceptable Use Policy and IT Rules of Behavior.

***All ONRR computer systems may be monitored for all lawful purposes including, but not limited to, ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security.***

Your access and/or use of ONRR computer systems and information are subject to being examined, recorded, copied, and used for DOI and/or ONRR authorized purposes at any time. All information, including personal information, that is placed, created, and/or transmitted over ONRR systems will be monitored.

By logging into ONRR computer systems, you acknowledge and consent to the monitoring of all systems. Evidence of your use – authorized or unauthorized – collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to criminal prosecution.

## Data Protection

The ONRR IT system is a U.S. Government information system that is "FOR OFFICIAL USE ONLY". Unauthorized access is a violation of U.S. Law and may result in criminal or administrative penalties. Users will not access other users' or system files without proper authority. The absence of access controls IS NOT an authorization for access! ONRR information systems and information are intended for the communication, transmission, processing, and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by law enforcement and authorized officials. Use of this system constitutes consent to such monitoring.

- Only use data for which you have been granted authorization.
- Do not retrieve information for someone who does not have authority to access the information; only give information to personnel who have access authority and have a need to know in the performance of their duties.
- Do not access, research, or change any user account, file, directory, table, or record not required to perform your OFFICIAL and authorized duties.

## Integrity

You are responsible for protecting the integrity of the ONRR IT system environment by preventing the unauthorized alteration, damage, destruction, and/or tampering with the system resources and/or information.

- Use of the system is restricted to authorized use only, and must be used for its ONRR intended function only.
- Data entry is restricted to data that is requested through input forms or specific system input descriptions. Never enter unauthorized, inaccurate, or false information into a system.
- Never introduce additional functionality, attempt to alter functionality, or add external applications into the ONRR system environment.
- Never introduce malicious software (i.e., viruses, worms, Trojans, etc) and/or any other forms of malicious code or data.

## Incident Response

You will cooperate willingly with official government actions during the research of, and response to, security violations.

## Passwords

You are responsible and accountable for any actions taken under your user ID. These actions are tracked, monitored, and audited.

- Protect passwords from discovery or use by other individuals at all times.
- Never give your password to another person (including your supervisor, the Help Desk, or anyone else requesting it.).
- If you believe your password has been compromised (become known to someone else), immediately notify the Help Desk at 1-877-256-6260 and change your password.
- If you write your password down, you are responsible to secure it in a locked place. Do not leave it in plain sight for other to see or access. Do not store it with your user ID.
- Do not ask anyone else for their password.
- Do not enter passwords for other people.
- Do not program user IDs or passwords into any form of automation, including script routines or programs, or keyboard function keys.
- Change passwords at least every 60 days, or immediately when they may have been disclosed.
- Never attempt to bypass or automate login procedures that require your input of a user ID and password.
- Be alert to unauthorized attempts to use your user IDs and passwords; immediately report unauthorized access attempts to the Help Desk at 1-877-256-6260.

- Construct good passwords:

  A Good Password
  - Contains mixed-case letters, numbers and with non-alphabetic characters (include characters from the keyboard reached by your right pinky ( [ ] \ { } | : ” ; ’ < > ? , . / )).
  - Can be typed quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
  - Can be remembered without writing it down.

  A Poor Password
  - Would contain your login name, e.g., smithj, in any form (as is, reversed, capitalized, doubled, etc.).
  - Would contain your first or last name in any form.
  - Would be easily obtained information about you. This includes license plate numbers, telephone numbers, name of favorite sports team, the brand of your automobile, your spouse’s or child’s name, pet, etc.
  - Would contain words in English or foreign language dictionaries, spelling lists, or other lists of words.