Office of Natural Resources Revenue
External User Acceptable Use Policy

Updated: December 2012

Purpose

This document is to establish the Acceptable Use Policies expected and computing practices as well as define inappropriate and prohibited actions. ONRR data, hardware and software are the property of the Federal Government and must be protected at all times. The purpose of this document is to assert required Acceptable use policies as specified by OMB Circular A-130, DM 375 Chapter 19, and other related laws, policies, directives, memorandums, and bulletins.

Scope

Acceptable Use Policies apply to all authorized users of any ONRR Information Technology (IT) system or resource. All users shall be aware of their responsibilities, acknowledge their actions, and comply with these Acceptable Use policies. IT resources include electronically-stored information, computer equipment, software, output, and storage media.

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

- DOI and ONRR defined approvals for your access have been obtained, reviewed, and accepted by ONRR.
- You read, acknowledged, and documented your consent to abide by the ONRR Acceptable Use Policies

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 this Policy at any time without prior notice, effective upon posting of the modifications on ONRR's website. ONRR will make every effort to notify users of the updated policy through its public website.

Penalties for Noncompliance

The Acceptable Use Policy is founded on the 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 in the Purpose section.

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 your use of ONRR IT system or resource. 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 ONRR Acceptable Use policies and the DOI Rules of Behavior for Computer Network Users and the associated Reference Guide

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 its 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, 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

This is a U.S. Federal 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. Absence of access controls IS NOT authorization for access! ONRR information systems and information are intended for 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.
- Do not post DOI information on the internet without prior appropriate permission. Only authorized personnel are allowed to distribute/post DOI information on internet sites (i.e. Blogs, Social networking Sites, message boards, etc)

Integrity

You are responsible for protecting the integrity of the system environment by preventing the unauthorized alteration, damage, unauthorized 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

A security incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Any action that breaks the rules in this document is defined as a security incident. You will cooperate willingly with official DOI and/or US government actions during the research of, and response to, security incidents and/or 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 you password has been compromised (become know 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 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 1-877-256-6260.
- Construct good passwords:

  <u>Good Passwords</u>

  - Use mixed-case letters, numbers and with non-alphabetic characters (include characters from the keyboard reached by your right little finger ([ ] \ { } | : ” ; ’ < > ? , . /)).
  - 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.
  - You can remember the password without writing it down.

  <u>Poor Passwords</u>

  - Your login name; e.g., smithj, in any form (as is, reversed, capitalized, doubled, etc.).
  - Your first or last name in any form.
  - 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.
  - Words in English or foreign language dictionaries, spelling lists, or other lists of words.