Office of Natural Resources Revenue
External User Acceptable Use Policy
Updated: March 2018

Purpose
This document establishes the Acceptable Use Policy for expected computing practices and defines inappropriate and prohibited actions as specified by OMB Circular A-130, DM 375 Chapter 19, and other related laws, policies, directives, memorandums, and bulletins. ONRR data, hardware, and software are the property of the Federal Government and must be protected at all times.

Scope
The Acceptable Use Policy applies to all users of any ONRR Information Technology (IT) systems or resource. All users shall be aware of their responsibilities, acknowledge their actions, and comply with this Acceptable Use Policy. 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 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 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.

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 into or by, processed, or stored in this system by law enforcement and authorized officials. Use of this system constitutes consent to such monitoring, acquisition, and analysis.

- Only access and 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, disseminate to unauthorized persons, 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. Only specifically authorized personnel are allowed to distribute/post DOI information on internet sites (i.e. blogs, social networking sites, message boards, etc.).

Consent to Monitoring
There should be no expectation of privacy with respect to your use of ONRR IT systems or resources.
ONRR IT systems are provided by ONRR for the explicit use of authorized users.

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 authorized purposes at any time. All 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. Information collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to criminal prosecution.

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 or the Help Desk) and do not ask anyone else for their password.
- If you believe you password has been compromised (become known to someone else), immediately notify the Enterprise IT Service Desk at **1-877-256-6260** and change your password.
- Do not enter passwords for other people.
- Do not attempt to bypass login procedures or program user IDs/passwords into any form of automation, including script routines or programs, or keyboard function keys.
- Be alert to unauthorized attempts to use your user IDs and passwords; immediately report unauthorized access attempts to the Enterprise IT Service Desk **1-877-256-6260**.

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 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 with official US government or law enforcement actions during security incidents.

Penalties for Noncompliance
ONRR shall enforce penalties against any user who willfully violates any ONRR, DOI, or Federal system security or privacy policy.

Penalties may include, but are not limited to:

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