Rules of Behavior for National Fire Plan Operations and Reporting System (NFPORS) Developers

These rules are based on Office of Management and Budget (OMB) Circular A-130, Appendix III, Department of the Interior (DOI) Departmental Manual 375, Chapter 19 (375 DM 19), and the NBC Computer and Information Security Policy (NBC-CIO-POL-001). These rules apply to all users of NBC computer systems.

This document establishes a minimum set of rules of behavior while using IT (Information Technology) resources that are owned, leased, or managed by the Department of the Interior (DOI). IT resources include, but are not limited to, computers, networks, data, communications media, transportable data storage media, etc. Managers of Federal and contract employees are responsible for ensuring that these rules are implemented in their organizations and that all users are made aware of their responsibilities. All users are expected to comply with this and referenced DOI policies and will be held accountable for their actions while using NFPORS.

Employees who violate these Rules of Behavior may be subject to disciplinary action at the discretion of the appropriate DOI management in conformance with the DOI Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1. Additionally, the local IT Security Manager may remove or disable the user's access to systems in the event of a violation, in accordance with DOI and NBC IT Security policies referenced in these Rules of Behavior.

Network-based systems are inherently insecure and cannot guarantee privacy. In order to underscore this fact, NFPORS displays a logon warning banner that states, in part, that:

"This is a United States Government computer application, which may be accessed only for official government business by authorized personnel. Unauthorized users who access this application may be subject to criminal, civil, and/or administrative action.

"Access to this computer application may be monitored, intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations.

"Access or use of this computer application by any person constitutes consent to these terms."

COMPUTER USE

- **National Security Information (NSI Classified Data) may NOT be entered into any computer system.** In the event that National Security Information is accidentally transmitted to a system, the local IT Security Manager must be contacted immediately.
- **DOI computer hardware, programs, and data are considered to be the property of the U.S. Government.** Except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at http://www.doi.gov/ethics/personaluse.pdf), Government-owned or Government-leased computers, software, and telecommunications systems are to be used for work-related purposes only. Resources are not to be used to conduct or support a personal business; and no personally owned data or software shall be entered into a DOI system, LAN, or personal computer.

PASSWORDS AND USER IDS

- **Passwords** for all Government-owned computer systems:
  - Are considered private and confidential. Users are prohibited from sharing any of their system passwords with anyone.
  - To minimize the risk of having the system compromised as a result of poor password selection, users are responsible for selecting passwords that are difficult to guess. Wherever technically supported, as many as possible of the following password selection criteria should be employed:
    - Passwords must be at least eight or more characters in length.
    - Passwords should contain a mix of both upper and lower case letters.
    - There must be at least one numeric character (0, 1, 2, 3...9).
    - New (changed) passwords must not be revisions of an old password. Reuse of the same password with a different prefix or suffix (A, B, C, etc.) is not permitted.
    - Dictionary words, derivatives of User IDs, and common character sequences such as "123456" may not be used.

- Personal details such as a spouse's name, license plates, social security numbers, and birthdays should not be used unless accompanied by additional unrelated characters.
- Proper names, geographical locations, common acronyms, and slang should not be used.

- If exposed or compromised, passwords must be changed immediately.
- **User Identifiers (User IDs)** are required for all users for access to computer systems. Each user must be uniquely identified. **The User ID possesses privileges that are tailored to the duties of the individual user's job and to the individual user's level of "need-to-know".** Each change in access must be approved.
    - If duties or job requirements change, accesses no longer needed must be removed and new accesses must be requested. Supervisors are responsible for notifying the Security Point of Contact (SPOC) whenever such changes occur so that the user's accesses can be changed to suit the new duty or job requirements.
    - When employment terminates, each system to which a user has access must be identified and the access terminated. This is accomplished on the checkout form completed by the user and supervisor on the last day of employment during the exit/clearance process. When employment termination is involuntary, is a result of natural or accidental death, or is caused by any other circumstance that precludes the user from performing the exit/clearance process, then it is the responsibility of the employee's immediate supervisor to expediently provide the notification(s).

    NOTE: The terms "Security Point of Contact" and "SPOC" refer to any individual who has been delegated security responsibilities for administering user accounts (User IDs, passwords, access authorities, etc.), regardless of platform. When the user is a contractor, the Government responsible manager or Contracting Officer's Representative is the supervisor for the purposes of these Rules of Behavior.
- If problems are encountered with a User ID, the supervisor or SPOC must be contacted.

USER ACCOUNTABILITY

- **Auditing of user access and of on-line activity is tied directly to the User ID.** Users are accountable for all actions associated with the use of their assigned User ID and may be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Each user must protect his/her User ID by:
    - Never allowing another person to use or share his/her logon session. Because the logon session is directly associated with an individual User ID, the user is personally accountable for all actions performed with the User ID.

NOTE: In the process of remotely trouble-shooting a difficult customer problem over the telephone, an FPPS or other Help Desk Technician may require the employee to reveal their secret password and explain that the problem cannot be resolved via any other means. Employees who need the assistance of a Technician to solve an IT-related problem are not expected to know whether the advice or request of a Technician is valid or whether the Technician is accurately recording the problem and attempted solutions in the Help Desk log. Therefore, if the employee has any reason to question any aspects of the manner in which the Technician is handling or documenting the situation, he/she should request to speak with the Technician's supervisor before providing their secret password. In any event, if an employee does provide their secret password to the Technician as part of the problem resolution process, the employee is responsible for changing his/her secret password immediately following resolution of the problem.

- Locking the workstation or logging off an active session when leaving the workstation for any reason (e.g., going to a meeting, lunch, restroom, etc.) to prevent unauthorized use of the user's logon session. A password-controlled screensaver is an acceptable means for satisfying this requirement, provided the screensaver is activated before leaving the workstation and the screensaver password complies with the password rules spelled out in the Passwords and User IDs section above.

AUTHORIZED ACCESS

- **Users are responsible for the appropriate use and protection of sensitive information to which they have authorized access.** The use of such information for anything other than "official Government business" is expressly prohibited. Users are responsible for adequately protecting any sensitive or Privacy Act data entrusted to them. Users are prohibited from disclosing, without proper authorization, sensitive or Privacy Act information to individuals who have not been authorized to access the information.
- **Due to the high sensitivity of Individual Indian Trust Data (IITD) and Tribal Trust Data (TTD)**, users must take extra care and precautions to protect any files or data entrusted to them related to IITD/TTD from unauthorized access.
- **Casual browsing of sensitive or Privacy Act information, such as personnel data, is not appropriate and is prohibited.** Users should **only** access this data when there is an official business reason.

UNAUTHORIZED ACCESS

- **Users are prohibited from accessing or attempting to access systems or information for which they are not authorized.** Users are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges. Users may not imitate another system, impersonate another user, misuse another user's legal user credentials (User IDs, passwords, etc.), or intentionally cause a computer or network component to function incorrectly. Users

may not read, store, or transfer information for which they are not authorized.

DATA PROTECTION

- **Users are prohibited from intentionally adding, modifying, or deleting information or programs** on any Government-owned computer system or component thereof without a documented and approved form or request for the addition, modification, or deletion.

  NOTE: This prohibition is not intended to include user-owned work files on individual workstations or on shared storage devices designated specifically for non-production use by individual users or groups. Nor is it a prohibition on user modifications to customizable software features such as “Preferences” or “Options”, etc., unless such customization is not allowed by local policies, procedures, or standards. When unsure, users should consult with their supervisor or SPOC.

- **Users who establish individual files** must ensure that security of the files is commensurate with the sensitivity or criticality of their content. Users should contact their supervisors or SPOCs for assistance in protecting individual files.

- **Data requiring protection under the Privacy Act**, proprietary data, other sensitive data or official Agency documents may not be copied or otherwise removed from Government-owned systems for the purpose of sharing such data outside the authorized user’s immediate work group, unless the information sharing has been authorized in writing by the Data Owner. Refer questions regarding Privacy Act information to the Departmental Privacy Officer at (202) 219-0868, or the Office of the Secretary Privacy Officer at (202) 208-6045.

DENIAL OF SERVICE

- **Users may not initiate actions, which result in limiting or preventing other authorized users or systems from performing authorized functions,** by deliberately generating excessive network traffic, and thereby limiting or blocking telecommunications capabilities. This prohibition includes the creation or forwarding of unauthorized mass mailings such as “chain letters”, or messages instructing the user to “send this to everyone you know”, or any messages with excessively large attachments or embedded graphics that consume large quantities of network bandwidth.

MALICIOUS (HOSTILE) SOFTWARE

- **Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce** any computer code designed to self-replicate, damage, or otherwise hinder the performance of any DOI computer system. Examples of these would be computer viruses, worms, and Trojan horses.

BYPASSING SYSTEM SECURITY CONTROLS

- **Unless specifically authorized by the IT Security Manager**, workers must **not** acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls. Examples of such tools include those that defeat software copy protection, discover (crack) secret passwords, or identify security vulnerabilities, etc. Additional examples include employing specialized system software mechanisms to bypass system security controls as a convenience measure.
- **Workers must not test or probe security mechanisms** unless they have first obtained permission from the IT Security Manager.

COPYRIGHT LAWS AND LICENSE REQUIREMENTS

- **Commercially developed software.** Commercially developed software must be treated as the 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 the manufacturer does not provide one. It is illegal to make copies of software for any other purposes without the written permission of the copyright owner. Making or using unauthorized copies of copyrighted products from a DOI or NBC computer system is illegal and is expressly prohibited.
- **DOI-owned computer systems.** Users may only install commercial software that is acquired through an approved procurement process. Vendor licensing requirements must be followed.
- **Personally owned software.** Users may not install personally owned software on DOI-owned computer systems. This includes but is not limited to personally owned screensaver software. An employee who has any doubt as to the appropriateness of installing personally owned software should check with his or her supervisor for guidance.

COMPUTER SECURITY INCIDENTS

- **Users and management are required to report all computer security incidents** (viruses, intrusion attempts, system compromises, offensive E-mail, inadequate protection of sensitive data, etc.) to their local IT Security Manager as follows:

Denver	(303) 969-7126
Reston	(703) 390-6726
Main Interior Building	(202) 208-5713
Boise	(208) 433-5050

- **Users are responsible for cooperating with System Administration and IT Security staff and the local IT Security Manager** during the investigation of a computer security incident.

USER RESPONSIBILITY

- **Users are responsible for following all the general computer use and IT security rules included in these Rules of Behavior** and for implementing appropriate controls to protect the resources and information under their control (as described in policies referenced in these Rules of Behavior). Local organizational units or systems may require additional levels of security controls. Resources permitting, users are responsible for implementing controls as requested by the local IT Security Manager.
- **Individual accountability.** Users will be held accountable for their actions on DOI IT systems. If a user adversely impacts the operation of a DOI IT system, the employee's access may be removed without notice to ensure the operation and availability for the rest of the system users.

INDIVIDUAL COMPUTER USER'S
ACKNOWLEDGEMENT OF RESPONSIBILITY
FOR USE OF NBC COMPUTER SYSTEMS

I understand that when I use any of the Government-owned computer systems or Information Technology (IT) resources or gain access to any information therein, such use of access shall be limited to official Government business (except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment, available on the DOI Web site at http://www.doi.gov/ethics/personaluse.pdf). Further, I understand that any use of the aforementioned systems or information that violates these Rules of Behavior may result in disciplinary action consistent with the nature and scope of such activity.

NOTE: Security policy infractions committed by contractors or vendors who are working for, and being paid by, the DOI will be handled in accordance with the provisions of their respective contracts concerning disciplinary or punitive actions, except in the case of criminal acts, which will be turned over to local law enforcement or Federal investigators.

I have been provided with and have read the "Rules of Behavior for National Fire Plan Operations and Reporting System (NFPORS) Developers". I understand these Rules of Behavior and agree to comply with these Rules.

Print Full Name: _____

Signature: _____

Federal Employee: ☐

DOI Office: _____

Date: _____

Contractor: ☐

Company Name: _____

Date: _____

NOTE – AFTER COMPLETING THE ABOVE SIGNATURE PAGE, SUBMIT THE ENTIRE 9-PAGE DOCUMENT TO THE NFPORS PROJECT MANAGER.