Rules of Behavior for Office of the Secretary and National Business Center Users of Information Technology Resources

These rules are based on Office of Management and Budget (OMB) Circular A-130, Appendix III and Department of the Interior (DOI) and National Business Center (NBC) Information Security and Privacy Policies. These rules apply to all users of Office of the Secretary and National Business Center computer systems and individuals who access sensitive DOI and NBC information.

This document establishes the Rules of Behavior while using Information Technology (IT) resources or accessing sensitive information that are owned, leased, or managed by the DOI, Office of the Secretary (OS) or the NBC. IT resources include, but are not limited to, computers, networks, data, communications media and transportable data storage media. Further, the Rules of Behavior outline the requirements for the protection of agency sensitive information, whether in electronic or paper format. Managers of Federal and contract employees must ensure that these rules are implemented in their organizations. All users must comply with these rules and DOI and NBC security policies and will be held accountable for their actions while using OS/NBC IT systems. Users are defined as any person accessing IT resources. Users include, but are not limited to, Federal employees, contractors and vendors.

Use of OS/NBC systems constitutes consent to monitoring, retrieval, and disclosure by authorized personnel.

Penalties:

Federal employees who violate these Rules of Behavior may be subject to disciplinary action at the discretion of the appropriate DOI or NBC management in conformance with personnel policies and the DOI Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1. Prior to taking adverse disciplinary action, supervisors must consult the Human Resources Office. Additionally, the local Information Security Manager may remove or disable the user’s access to systems.

Contractors and vendors must comply with all applicable Federal and DOI rules, procedures and guidelines. Failure to do so may result in: removal of access to DOI systems; removal from the contract; and criminal prosecution where appropriate.

Rules:

PROTECTION OF SENSITIVE INFORMATION

- Users must take appropriate measures to protect OS/NBC IT resources and sensitive documents/data. Sensitive documents/data are agency documents/data which, while not classified for national security reasons, require special protection due to the ***significant*** risk of harm that could result from their inadvertent or deliberate disclosure, alteration or destruction. Typically, the release of these documents/data to the public is prohibited by statute or regulation.
- Documents and data must be protected in all forms – electronic, verbal, and paper. All electronic files which include sensitive information must be protected by encryption, when available. All paper files which include sensitive information are to be protected from unauthorized disclosure through the use of appropriate locked containers and disposal procedures.
- Users must inform their supervisor when processing sensitive information on systems that previously did not contain sensitive information so that appropriate security measures can be implemented.
- Sensitive documents/data include, but are not limited to, the following categories:
  - Documents/data requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, e.g., individually-identified medical, benefit and personnel information.
  - Personally identifiable information maintained in files not protected by the Privacy Act.
  - Information compiled for law enforcement, investigatory, or security purposes.
  - Critical infrastructure (physical and information technology) information as defined in 444 DM 1, Department of the Interior Departmental Manual, dated 7/7/99, Physical Protection and Building Security and Homeland Security Act of 2002: Critical Infrastructure Information Act.
  - Continuity of operations and other emergency preparedness plans.
  - Indian Fiduciary Trust information.
  - Credit card numbers.
  - Attorney-client communications.
- No user may knowingly enter National Security Information (NSI Classified Data) into any OS/NBC computer system. Any user who discovers National Security Information that has been transmitted to an OS/NBC system must immediately contact the NBC Information Security Division, Computer Security Incident Response Team (CSIRT).
- Users must protect sensitive data to which they have authorized access and must not disclose, without proper authorization, sensitive data to individuals who have not been authorized to access the data. Sensitive information must be encrypted

when electronically transmitted to prevent unauthorized disclosure of sensitive information.

- Users must only access sensitive data, such as personnel data, when there is an official business reason.
- 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.
- 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 supervisor or Security Points of Contact (SPOC) for assistance in protecting individual files.

SYSTEM USE AND PROTECTIONS

- Except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment, Government-owned or Government-leased computers, software, and telecommunications systems are to be used for work-related purposes only.
- All users must protect computing equipment, including mobile devices, from physical dangers. For example, users must not keep open drink containers near computing equipment and must ensure proper ventilation and cooling for computing equipment.
- Users must not move or reconfigure hardware components without approval from OS/NBC IT.
- Users must not create file shares on OS/NBC systems without approval from OS/NBC IT.

PASSWORDS

- To minimize the risk of having the system compromised as a result of poor password selection; users must select passwords that are complex and difficult to guess. <u>Wherever technically supported by the system</u>, 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 upper and lower case letters, numeric characters (0, 1, 2, 3…9) and special characters (#, $, %, etc.).
    - New (changed) passwords must not be revisions of an old password (i.e., changing one character from the previous password).
    - 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, pet names, and birthdays should not be used.
    - Proper names, geographical locations, common acronyms, and slang should not be used.

- Passwords must be changed on a regular basis, 60 days for normal users and 30 days for accounts with elevated privileges.
- Passwords must be changed immediately if exposed or compromised. If your password is compromised, immediately notify your supervisor and the NBC Help Desk.
- User Identifiers (User IDs) are required for all users to access OS/NBC computer systems. Each user must be uniquely identified.
    - 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 and system passwords.
        - Users must not share system passwords with anyone.
        - Users must not allow another user to use or share his/her logon session.
        - Users must lock the workstation or log off an active session when leaving the workstation to prevent unauthorized use of the user's logon session.
        - Users must not store system passwords in electronic files unless the password data is encrypted.
        - Users should avoid storing passwords in written form. If passwords must be stored in written form, users must ensure that passwords are stored in an appropriately secured location (i.e., safe, locked cabinet or locked drawer, etc.)
    - 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 documented in an access request and approved.
    - If duties or job requirements change, accesses no longer needed must be promptly removed and new accesses must be requested. Supervisors must notify 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. The term Security Point of Contact refers to any individual who has been delegated security responsibilities for administering user accounts.
    - Users must comply with the exit/clearance process on their last day of employment. When employment terminates, each OS/NBC system to which a user has access must be identified via the exit/clearance process and the access terminated. Supervisors must provide the notification of access termination to the appropriate SPOC in cases that precludes the user from performing the exit/clearance process.

UNAUTHORIZED ACCESS

- Users must not access or attempt to access systems or information for which they are not authorized. Users must not change access controls to allow themselves or others to perform actions outside their authorized privileges. Users must not imitate another system, impersonate another user, misuse another user's access credentials (User IDs, passwords, etc.), or intentionally cause a computer or network component to function incorrectly. Users must not read, store, or transfer information for which they are not authorized.

- Users must not use sensitive data for anything other than "official Government business".
- Data requiring protection under the Privacy Act, proprietary data, other sensitive data or official Agency documents must not be copied or otherwise removed from OS/NBC 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.
- Users must not remove Government property from OS/NBC premises for personal use.
- Personally owned data or software must not be installed on or entered into an OS/NBC system, LAN, or personal computer.
- Personally owned removable storage media must not be used to download and store DOI documents, files, or data.
- All non-Government issued laptop computers must be inspected and authorization granted by OS/NBC IT prior to connecting to any OS/NBC network or computer resource. The inspection shall include scans and system checks to ensure all devices are safe and meet DOI standards. Authorizations for use must expire after five working days or after the laptop computer leaves the Government premises that issued the authorization.
- Non-Government owned Portable Electronic Devices (PED) must not be connected to any OS/NBC network or computer resource.
- Users must not install, activate or use Instant Messaging (IM), Internet Relay Chat (IRC), Web Conferencing, and Peer-to-Peer (P2P) without prior authorization.
    - Examples of IM software include, but are not limited to: AOL, Yahoo, and MSN Instant Messenger.
    - Examples of IRC include, but are not limited to: Undernet, Galaxynet and ERNet.
    - Examples of P2P software include, but are not limited to: Ares, Bearshare, Blubster, Cheetah, Crapster, DC++, Direct connect, eDonkey, File Miner, File Navigator, Filetopia, Freewire, Gnucleus, Gnutella, GoMP3, Grokster, iMesh, KaZaA, Limewire, Morpheus, MyNapster, WinMX, PHEX, Piolet, Shareaza, Prune Baby, SwapNut, URLBlaze, XoLoX and Yaga.
- Users must 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.

- 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 or NBC computer system. Examples of these would be computer viruses, worms, and Trojan horses.
- Unless specifically authorized by the NBC Chief Information Security Officer (CISO), users 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.
- Users must not employ specialized system software mechanisms to bypass system security controls as a convenience measure. This includes attempts to access information on how to bypass security controls, such as searching online for ways to bypass corporate firewalls to access blocked web sites.
- Users must not test or probe security mechanisms at either the OS/NBC or external installations unless they have first obtained authorization from the NBC CISO.

COPYRIGHT LAWS AND LICENSE REQUIREMENTS

- 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. Users must not make or use unauthorized copies of copyrighted products from a DOI or NBC computer system.
- Users may only install commercial software that is acquired through an approved DOI or NBC procurement process. Vendor licensing requirements must be followed.
- Use of non-commercial software, such as freeware, shareware, and open source software, is prohibited without the written consent of the user’s supervisor and OS/NBC IT. Also note that many freeware products are free only to individual persons and require purchase for commercial or government use.

CONNECTING TO THE INTERNET

OS/NBC personnel are provided with the equipment and Internet connection to accomplish the work of the OS/NBC. Limited personal use of the Internet is governed by the DOI Policy on Limited Personal Use of Government Office Equipment. Users may make limited personal use of government equipment as long as it occurs on non-duty time, does not interfere with official business, does not adversely impact electronic systems, is not commercial gain activity or is not otherwise prohibited, and the expense to the government is negligible. The prohibited activities listed in the DOI Internet Acceptable Use Policy include but are not limited to:

- Using Government office equipment to conduct transactions for personal commercial gain/loss activity (e.g., using an office computer to purchase stock shares on the stock market or to conduct transactions and correspondence for a personal business outside of NBC/OS).
- Using Government-provided access to the Internet to present their personal views in a way that would lead the public to interpret it as an official Government position.
- Using the Internet as a radio or music player (e.g., use of "streaming audio or video") unless specifically authorized by the NBC/OS CISO.
- Using "push" technology on the Internet or other continuous data streams, unless they are directly associated with the employee's job.
- Using Government-provided E-mail for personal use except as authorized by Departmental policy as referenced in these Rules of Behavior.
- Using Government office equipment at any time for activities that are illegal (e.g., gambling) or that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit material, material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation.
- Using Government-provided equipment for the creation, storage, or transmission of copyrighted material, such as ripping CDs to MP3, transmitting or sharing MP3, software, music, or video files.
- Unless authorized by the NBC/OS CISO, users shall not visit sites that discuss techniques for bypassing or testing security controls, such as hacking websites, forums, or other malicious behavior. Visiting news and discussion sites that discuss current events and threats is authorized, so long as those sites do not discuss the details of how to utilize those techniques to bypass or test security controls.

E-MAIL

- All email that contains sensitive information must be encrypted. Examples of sensitive information commonly transmitted via email:
    - Social Security Numbers, Credit Card Numbers and other non-public Personally Identifiable Information (PII).
    - Risk Assessments, vulnerability scan results
    - Security Incident information
    - IP addresses, port numbers, dial-in information
    - Passwords
- Users must not click on attachments with the following extensions. If you receive an email with one of the following attachments, DO NOT open the attachment. Immediately contact the Help Desk or Customer Support Center.

  ade, adp, bas, bas, bat, chm, cmd, com, cpl, crt, exe, hta, ins, isp, lnk, mda, mde, mdz, mp3, msc, msi, msp, mst, ocx, pcd, pif, reg, sct, shs
- Uses must not subscribe to non-business-related listservs.

- Users must not click on web links or open attachments contained in unexpected emails. These are common methods used to deliver malicious software to unsuspecting users.
- Users must use notepad or another text editor to open potentially hostile scripting files, such as .vb, .vbs, .js, etc.

HANDLING OF PRIVACY ACT RECORDS

This section outlines standards of conduct for personnel in implementing requirements of the Privacy Act of 1974 (5 U.S.C. 552a). Individuals to whom these standards are applicable include all personnel who have access to systems of records subject to the Privacy Act, such as Quicktime, or who are engaged in the development of procedures or systems for handling such records (i.e. those engaged in personnel management, records/paperwork management, computer systems development and operations, communications, statistical data collection and analysis, and program evaluation).

- Individuals must follow OPM, DOI and NBC Privacy Act policies.
- Program officials and system managers must ensure that no irrelevant or unnecessary personal information is collected.
- Individuals must make all reasonable efforts to maintain accurate and timely records.
- Individuals must protect the integrity, security, and confidentiality of these records.
    - Minimum safeguards for hard copy (non-automated) records subject to the Privacy Act:
        - Records system areas must be posted with warnings to include access limitation, standards of conduct for employees in handling Privacy Act records, and possible criminal penalties for violations.
        - Access to records must be restricted at all times by storing the records in a locked metal file cabinet or locked room, except when the room is occupied by authorized personnel.
        - Where a locked room is the method of security, master keys must not be available to unauthorized personnel.
    - Safeguards for automated records subject to the Privacy Act must follow National Institute of Standards and Technology (NIST) requirements.
    - Appropriate safeguards must be taken when records subject to the Privacy Act are transferred within or outside the agency. Steps must be taken to assure the integrity and confidentiality of the records while in transit.
    - Records subject to the Privacy Act must be disposed of in accordance with the provisions of National Archives and Records Administration regulations, 36 CFR 1228.74.
        - Records may be burned, shredded or pulped within the organization
        - Records may be pulped, macerated, or shredded by a wastepaper contractor; however, a Federal employee must witness the destruction.

- Individuals must protect personal information contained in systems of records subject to the Privacy Act from disclosure for any purpose other than that for which the information was gathered, or under exceptions provided in the Privacy Act and to any external parties other than those specified in the applicable Privacy Act System of Records Notice.
- Individuals must not alter or destroy a record subject to the Privacy Act unless it is undertaken in the course of his/her regular duties, required by a decision under the Department's regulations, or pursuant to a court decision.
- Any officer or employee who knowingly and willfully makes an unauthorized disclosure of records subject to the Privacy Act, or who willfully maintains a system of records without meeting the Privacy Act's notice requirements, is guilty of a misdemeanor and may be fined up to $5,000.

RECORD RETENTION REQUIREMENTS

- Users must follow DOI and NBC records management policies. Documents or E-mail created may be considered Federal records that must be preserved by being printed and filed and may not be deleted from the system before being saved in the system's backup process.
- **Record Retention Requirements for Cobell v. Salazar litigation.** Users must print and file, in accordance with applicable Court and Departmental directives, any documents they have or create and any E-mail messages they send or receive, including attachments, that relate to the three functional areas of:
  - American Indian Trust Reform, including the High-Level Implementation Plan or any of its subprojects;
  - The Cobell v. Salazar litigation; or
  - Administration of Individual Indian Money (IIM) accounts.
- Users must print and file the weekly e-mail notification of the backup of e-mail records. The subject of this email is titled "Notification of Capture of E-mail Messages on Backup Media".
- All official records, including printed copies of emails, must be turned over to the employee's supervisor or other designated individual at termination of employment.

MEDIA LABELING AND SANITIZATION

- Users must ensure that all sensitive data, electronic and printed, is labeled with the appropriate sensitivity and handling label.
- All sensitive information, both electronic and printed, must be properly sanitized, stored, or disposed of when no longer needed.

COMPUTER SECURITY INCIDENTS

- Users must promptly report all computer security incidents to their local Information Security Manager, the NBC Information Security Division, CSIRT or their Help Desk or Customer Support Center. Examples of computer security incidents include, but are not limited to, unauthorized disclosure of information, computer viruses, theft of equipment, software or information, inappropriate use, and deliberate alteration or destruction of data or equipment.

- Federal Agencies are required to report all incidents involving Personally Identifiable Information (PII) to U S CERT within one hour of discovering the incident. Agencies must not distinguish between suspected and confirmed breaches and must report all incidents involving PII in electronic or physical form. Users must immediately report all PII incidents to the NBC Information Security Division, CSIRT so that NBC can meet the required OMB reporting requirement.
- For additional assistance, users may contact their local Help Desk or Customer Support Center.
- Users must cooperate fully with the NBC Information Security Division, CSIRT during the investigation of a computer security incident. The CSIRT Incident Manager is authorized to confiscate any and all government owned equipment deemed necessary during the course of the investigation. If the CSIRT confiscates equipment, the user's supervisor will be informed and alternate computing resources will be arranged.

SPECIAL CONSIDERATIONS FOR REMOTE ACCESS

Access to agency resources from a location not under the direct control of the Office of the Secretary or the National Business Center is considered "Remote Access". New technical solutions are being implemented to secure and protect agency data, especially if it is being carried outside of the OS/NBC's physically protected areas. With these new requirements also come new responsibilities for user behavior regarding the protection of agency data. Users must secure and protect agency data as follows:

- Users must physically protect all hardware or software based tokens entrusted to them for authentication or encryption purposes. (A token is usually a physical device that an authorized user is given to provide additional higher level security and to verify the user is who they say they are when logging in to the network.)
- Users must encrypt all agency data stored on any equipment, including but not limited to computers, external hard drives, PDAs, and thumb/flash drives, anytime they are outside of OS/NBC protected facilities. This requirement is only applicable once NBC or the Office of the Secretary provides an encryption solution for end-users.
- Per OMB requirements, users must ensure that all agency data downloaded using remote access is erased after 90 days or when it is no longer needed. Where more stringent requirements are defined by organizational policies, users must follow the more stringent requirements.
- Users should refer to their Information Security Manager for standards and approved methods for encrypting and deleting data.
- Users must use only an OS/NBC approved method of remote connectivity, such as a Virtual Private Network (VPN).

REFERENCES:

DOI:

http://www.doi.gov/ethics/docs/personaluse.pdf

DOI Policy on Limited Personal Use of Government Office Equipment

http://elips.doi.gov/app_dm/index.cfm?fuseaction=home

DOI DM 375, Chapter 19, Information Technology Security Program

DOI DM 383, Policies and Procedures for Implementing the Privacy Act of 1974

NBC:

https://mynbc.nbc.gov/PFTGF/policies/policies.cfm?LOB=ITD

NBC Computer and Information Security Policy (NBCM-CIO-6300-001)

OS/NBC Information Classification and Handling Policy (NBCM-CIO-6300-003)

CONTACTS:

NBC Customer Support Center	1-888-FOR-1NBC (1-888-367-1622)

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

I understand that when I use any of the Office of the Secretary's (OS) or National Business Center's (NBC) 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). 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 OS or the NBC 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 (ROB) for Office of the Secretary and National Business Center Users of Information Technology Resources, Version 2.0.2 dated j, 2011". I understand these Rules of Behavior and agree to comply with these Rules.

Federal Employee □ Contractor or Vendor □

Print Full Name: ____

Signature: ____

Date: ______________________________

Directorate, Division, Branch: ____

Company Name
(for Contractors/Vendors): ____

Employees – Supervisor's Name
Contractors – COTR's Name: ____