

## Rules of Behavior

Office of the Secretary Local Area Network  
Department of the Interior

The rules of behavior contained in this document are to be followed by all users of the Office of the Secretary (OS) Local Area Network (LAN): users are expected to comply with this and all other DOI policies and will be held accountable for their actions on the LAN. If an employee violates these Rules of Behavior, he or she may be subject to disciplinary action at the discretion of OS management. The Technology Services Division of the National Business Center (TSD/NBC) may revoke a person's system access for a specific period of time if an employee violates these Rules of Behavior. In addition, OS management may take disciplinary actions in conformance with the Department's Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1, dated 6/27/01.

**Connection to the Internet** - OS personnel have access to the Internet. The equipment and Internet connection are provided to accomplish the work of the Department of the Interior. Limited personal use of the Internet is governed by the Department of the Interior (DOI) Policy on Limited Personal Use of Government Office Equipment (available on the DOI home page at <http://www.doi.gov/ethics>). Briefly, this policy states that employees on non-duty time are allowed to use the Internet for personal use as set forth in and in accordance with the Internet Acceptable Use Policy (IRM Bulletin 1997-001, available on DOI home page, <http://www.doi.gov/orim/bulletins>). Except as prohibited by this policy, employees are allowed to make personal purchases through the Internet, but only during non-duty time. Non-duty time is determined by management and is limited to official breaks, lunch, before and after duty hours. When making such purchases, however, employees must have the purchases sent to a non-Government address. Employees are prohibited from using Government office equipment at any time to make purchases for personal commercial gain activity. Please refer to the web sites listed above for the details of the following prohibited activities including but not limited to:

- § 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.
- § 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.
- § using Government office equipment, at any time, for activities that are illegal; e.g., gambling (5CFR 735.201), or that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit material or, material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin or sexual orientation.

**Protection of copyright licenses (software)** - LAN and PC users are not to download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs will also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited. Users are not to download software from the Internet for installation on their PC or to install software they have privately purchased. Users may not install an off-the-shelf software package on any machine other than those for which a valid license has been purchased. In other words, a user may not purchase a single copy of (license) for an off-the-shelf software package and install it on multiple machines.

**Record Retention Requirements** - Users must follow DOI records management policies. Any 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. Norton litigation** – Users must print and file, in accordance with applicable Court and Departmental directives, any documents they have or create and any electronic 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. Norton litigation; or
- administration of Individual Indian Money (IIM) accounts.

In addition, users must to the best of their abilities protect any files or data related to individual Indian trust data from unauthorized access.

**Unofficial use of government equipment** - Users should be aware that the Department of the Interior (DOI) Policy on Limited Personal Use of Government Office Equipment governs personal use of information resources (e.g., computers, printers, e-mail, Internet, etc).

**Use of passwords** - Users are to use passwords of a length specified by the LAN system administrators - a mix of eight (8) alpha and numeric characters, they are to keep passwords confidential and are not to share passwords with anyone.

**System privileges** - Users are given access to the LAN based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

**Individual accountability** - Users will be held accountable for their actions on the LAN. If an employee adversely impacts the operation of the LAN, TSD/NBC may remove the employee's access without notice to ensure the operation and availability for the rest of the OS.

**Restoration of service** - The availability of the LAN is a concern to all users, and we will do our best to ensure that the LAN is available at all times during normal working hours. However, Offices are responsible for ensuring that they are able to provide critical services in the event the LAN is unavailable in accordance with continuity of operation plans. In addition, users are asked to cooperate with LAN management staff during outages, so that service can be restored for all users in a timely manner.

I acknowledge receipt of and have read the rules of behavior for the OS LAN.

\_\_\_\_\_  
Signature of User

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Office

PLEASE NOTE: These rules are subject to change. Users will be notified of updates via e-mail.

Revised January 14, 2003