

NOAA'S INFORMATION TECHNOLOGY SYSTEM
RULES of BEHAVIOR
January 2006

NOAA provides access to computing resources (hardware, software, data) to its employees and contractor staff. These resources are provided to facilitate completion of assigned responsibilities, with prior authorization. The policies and procedures governing use of NOAA computing resources are detailed in NOAA Management Directives. Individuals who are authorized to use NOAA computing resources must comply with NOAA Management Directives and the specific Rules of Behavior listed below.

End User Responsibilities

- **Security Incident Handling and Reporting.** Users are required to report known or suspected incidents, including unauthorized use of NOAA computer resources, to their local ITSSO, and to the NOAA Computer Incident Response Team (N-CIRT), by calling (301) 713-9111 and using NOAA Form 47-43. All incidents must be reported with 24 hours of detection.
- Use NOAA computers only for lawful and authorized purposes.
- Comply with safeguards, policies, and procedures to prevent unauthorized access to NOAA computer systems.
- **Passwords.** User passwords are required to comply with the DOC IT Security Program Policy and Minimum Implementation Standards Policy for Password Management (Appendix G). User passwords must be changed at least every 90 days and at a minimum contain at least 8 characters consisting of numbers, letters and special characters. Passwords cannot be reused for 2 years and can't contain dictionary words (spelled forward and backwards.) Do not write down or share your logon or account password with anyone (including the Help Desk). Users will ensure that they log-off, or use a password-protected screen saver whenever the workstation is left unattended.
- **Individual Accountability.** Recognize the accountability assigned to your User ID and password. Each user must have a unique ID to access NOAA systems. Recognize that User IDs are used to identify an individual's actions on NOAA systems and the Internet. Individual user activity is recorded, including sites and files accessed on the Internet (recorded as the files go through the firewall).
- **E-Mail.** Chain letters, games, union announcements and threatening, obscene, or harassing messages are not allowed. Management must approve use of broadcast features. Do not open unsolicited or suspicious e-mail messages or their attachments, do not forward chain mail, and do not generate or send offensive or inappropriate e-mail messages, graphical images, or sound files. Limit distribution of e-mail to only those who need to receive it.

- **Anti-Virus Protection.** Users are required to use regular updated anti-virus software while using or accessing government IT systems and resources. When your workstation begins an update of its anti-virus software, let that update finish. Use authorized virus scanning software on your workstation or PC and your home computer. Know the source before using diskettes or downloading files. Scan files for viruses before execution. Minimize the threat of viruses: (1) Write-protect diskettes and CD's, (2) Virus check any foreign data source, and (3) Never circumvent the anti-virus safeguards on the system.
- **Data Backups.** Ensure that data are backed up, tested, and stored safely.
- **Protection of copyright licenses (software).** Users using government-owned equipment are not permitted to download and/or install any software application(s) on systems without prior System Owner approval. All software must be properly licensed prior to installation on any government-owned equipment. Audit logs will be reviewed to determine whether employees attempt to access government owned systems or IT resources on which valuable, commercial-off-the-shelf or government software resides, but to which users have not been granted access.
- **Copyrighted Software.** Unauthorized copying of copyrighted software is also prohibited. Users are required to comply with the DOC Copyrighted Software Policy and Title 17, United States Code, Section 106.
- **Connections to the Internet.** All desktop PC's, workstations and servers that have access to the Internet and its use must be in accordance with the DOC and NOAA Internet Use Policies.
- **Use of Government Equipment.** Users have been educated regarding the use of government equipment and IT resources for personal use. Users are permitted to use government-owned equipment during non-duty hours (before scheduled work hours, lunch times, and after work hours) for personal use. Personal use of government-owned equipment and IT resources must not incur any additional costs to the government and/or violate any federal regulations, DOC or NOAA policies. Activities specifically not permitted on government-owned IT resources include but are not limited to the following: a) private commercial business activities or profit making ventures; b) engagement in matters directed toward the success or failure of a political party; c) engagement in any prohibited direct or indirect lobbying; d) use that could generate or result in an additional charge or expense to the Government; e) viewing, obtaining, creation, distribution, or storing of sexually explicit material; f) participation in or encouragement of illegal activities or the intentional creation, downloading, viewing, storage, copying, or transmission of materials that are illegal or discriminatory; g) Use of Government e-mail addresses in a manner that will give the false impression that an employee's otherwise personal communication is authorized by the Department; h) engagement in unauthorized charitable fund raising (see the Broadcast E-Mail Policy) or soliciting volunteers to raise funds; and/or i)

activity that would bring discredit on the Department or violation of any statute or regulation, including applicable copyright laws. Personally purchased software is not allowed on government equipment. DOC IT Security Program Policy and Minimum Implementation Standards Policy for Peer-to-Peer File Sharing (Appendix I) restricts the use of Peer to Peer file sharing. Users will not use Peer to Peer (P2P) connection sharing for transferring copyrighted files.

- **Remote Access.** Designated managers may authorize remote access to specific IT systems and resources of specific systems for remote user access. All remote users are required to review and comply with all aspects of the DOC and NOAA Remote Access Policy and sign the Remote Access Agreement. These rules of behavior apply for all remote accesses.
- **Data Destruction.** Properly dispose of unneeded data: (1) Do not throw sensitive hard copy into a wastebasket (shred or burn). (2) Delete sensitive information from memory on hard drive and diskettes permanently by overwriting. Ask ITSO for aid.
- **NOAA Security Awareness Training.** Users are required to complete the NOAA IT Security Awareness course annually.
- Users need permission from appropriate NOAA officials before they discuss security practices or anti-piracy practices with external organizations or individuals.

Supervisor/Management Responsibilities

NOAA supervisors and management officials are responsible for ensuring an adequate level of protection is afforded to IT resources through an appropriate mix of managerial, operational, and technical controls.

In addition to the rules that apply to all end users, each supervisor/application system manager is responsible to ensure that:

- All employees/contractors belonging to or performing work within her/his organization:
 - Have appropriate security clearances.
 - Behave in a manner consistent with the protection and security of information, data, software, hardware, and systems assigned to or used by them.
- Employee/contractor access privileges are granted to information and systems, being mindful that:
 - Users should not have access privileges (or software) for other than official business.
 - Access privileges must be removed as soon as the need expires or within 24 hours of separation from NOAA.

- All employees/contractors have current knowledge of these Rules of Behavior, including specialized rules for specific data sets and systems that govern the use of workstations, the network, databases, and other systems, and for instructing all who are assigned to or work within his/her organization regarding the existence and application of these rules.

Systems/Network/LAN Administrators Responsibilities

In addition to the rules that apply to all end users, each system/network/LAN administrator is responsible for:

- Supporting supervisors in their efforts to ensure employee compliance with DOC and NOAA Rules of Behavior. This includes specialized rules for specific information files and systems, for use of workstations, network privileges, databases, and other system features and functions, as well as legal requirements government use of proprietary software.
- Monitoring the security status of their systems, auditing activities, and reporting findings to the appropriate manager. The conduct of these activities has two basic components:
 - Routine/Regular:
 - Regular security monitoring (e.g., intruder detection).
 - Report violations.
 - Audit per NOAA standards and security plan.
- Ad Hoc/Special efforts requested by management. Maintaining documented authorization from the appropriate supervisor(s) for granting or expanding access to system assets for NOAA employees, as well as for other individuals, organizations, or systems (For all items on the system/network/LAN that require controlled access control should be restricted according to group membership rather than individual permissions. This will provide easy accounting of who has access to what.)
- Dedicated account(s) for performing “root” or “superuser” functions are to be used only when required.
 - Administrators should log in with the least amount of authority required to perform the task; i.e, not use “superuser” status unless required.
 - Standard user account(s) for performing day-to-day activities that don’t require administrator authority are to be used.
- Obtaining authorization from (or adhering to a protocol established by) the appropriate supervisor(s) for the reconfiguration of equipment or software, and maintaining documentation of the changes and the authorization thereof. There must be management control over changes and reconfiguration that compromise security. The administrator should operate within a standard range of previously agreed upon decision-making authority.

- The system/network/LAN administrator's responsibility is limited to those things that she/he could be reasonably expected to control. For example, changes to the CONFIG.SYS on a workstation attached to the LAN are not something for which the LAN administrator would be held liable either for authorization or for documentation. Corporate accounts may be established, with proper authorization, to be used by supervisors and managers to establish the requested access privileges for employees, in lieu of authorizing the LAN administrator to do so.