

CNA E-TOOL RULES OF BEHAVIOR

CNA E-TOOL RULES OF BEHAVIOR

SECTION I - RESPONSIBILITIES

This section describes what ROB are, why they are needed, what users can expect, and the consequences for violating the ROB.

What are Rules of Behavior?

Office of Management and Budget (OMB) Circular A-130 Appendix III requires every System Security Plan (SSP) to contain a Rules of Behavior (ROB). ROB apply to the system users and list specific responsibilities and expected behavior of all individuals with access to or use of the named information system. In addition, ROB outlines the consequences of non-compliance and/or violations.

Why are Rules of Behavior Needed?

ROB is part of a complete program to provide good information security and raise security awareness. ROB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Who is Covered by the Rules of Behavior?

The ROB covers all government and non-government users of the named information systems. This includes contract personnel and other federally funded users.

What are the Consequences for Violating the Rules of Behavior?

Penalties for non-compliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

SECTION II - APPLICATION AND ORGANIZATION RULES

This section identifies the Rules of Behavior measures that will apply to Capital Needs Assessment Electronic Tool end-users. Section 3.1 lists the most common and minimal set of ROB as recommended by NIST 800-18. Section 3.2 lists other ROB that may apply to your organization. Section 2h includes ROB for system administrators. Each section is discussed in detail below.

A. Passwords

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as *#\$ %). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other's password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.
5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

B. Encryption

1. Extremely sensitive data should be encrypted prior to transmission.
2. The sensitivity of the information needing protection, among other considerations, determines the sophistication of the encryption technology. In most circumstances, only the most sensitive or compartmentalized information should be encrypted.
3. Files that contain passwords, proprietary, personnel, or business information, and financial data typically require encryption before transmission, and should be encrypted while stored on the computer's hard disk drive.
4. Sensitive information that travels over wireless networks and devices should be encrypted.

C. Internet Usage

1. Downloading files, programs, templates, images, and messages, except those explicitly authorized and approved by the system administrator, is prohibited.
2. Visiting websites including, but not limited to, those that promote, display, discuss, share, or distribute hateful, racist, pornographic, explicit, or illegal activity is strictly prohibited.
3. Because they pose a potential security risk, the use of Web based instant messaging or communication software or devices are prohibited.
4. Using the Internet to make non-work related purchases or acquisitions is prohibited.
5. Using the Internet to manage, run, supervise, or conduct personal business enterprises is prohibited.

D. Email

1. Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited.
2. E-mail addresses and e-mail list-serves constitute sensitive information and are never to be sold, shared, disseminated, or used in any unofficial manner.
3. Using an official e-mail address to subscribe to any non-work related electronically distributed newsletter or magazine is prohibited.

E. Working from Home/Remote Dial-up Access

All CNA E-TOOL users are responsible for attending annual IT Security certification training. Failure to attend will result in having system access privileges revoked.

1. Users may dial into the network remotely only if pre-approved by the system administrator.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. At no time should a "live" dial-up connection be left unattended.
4. Web browsers must be configured to limit vulnerability to an intrusion and increase security.
5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install a hardware or software firewall.
6. No official material may be stored on the user's personal computer. All data must be stored on a floppy disk and then secured in a locked filing cabinet, locker, etc.
7. Operating system configurations should be selected to increase security.

F. Unofficial Use of Government Equipment

Except for limited personal use, government equipment including, but not limited to, fax machines, copying machines, postage machines, telephones, and computers are for official use only.

G. Other Rules of Behavior

To properly safeguard the Department's information assets while using information technology, it is essential for all employees to be aware of procedures for destroying sensitive information. Sensitive information within HUD that must be protected includes, but is not limited to, financial management information (budgeting, accounting, etc.); investigative information; contract sensitive information (pre-solicitation procurement documents, statements of work, etc.); and security management information (i.e., identification of systems security controls and vulnerabilities).

Of particular concern is Personally Identifiable Information (PII), which includes social security numbers, names, dates of birth, places of birth, parents' names, credit card numbers, applications for entitlements, and information relating to a person's private financial, income, employment, tax records, etc.

To assist you in determining what type of information should be considered sensitive, here are a few examples:

1. Personnel data
2. Travel vouchers
3. Procurement documents
4. Statements of Work or related procurement documents
5. Loan applications or files
6. Grant applications or files
7. COOP data

The May 25, 2006 memorandum from the Deputy Secretary and the June 6, 2006 broadcast email from the CIO to all HUD employees stated "Protect all electronic/optical media and hard copy documentation containing sensitive information and properly dispose of it by shredding hard copy documentation, or by contacting the HITS Help Desk to dispose of electronic/optical media".

In each Regional Office a location will be set up, in the Information Technology Division, where media containing sensitive data will be destroyed.

Please use the following procedures to properly destroy sensitive data stored on electronic/optical media that are no longer in need of maintaining:

1. Contact your supporting IT staff if you need media destroyed that contains sensitive information (CDs, DVDs, flash drives, Personal Verification Cards (PVC), external hard drives, etc.) and you will be provided with instructions.

In addition, absolutely no media containing sensitive information will be sent through the mail or released from the Department.

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.
2. Users who no longer require IT system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the system administrator.
3. When not in use, workstations must be physically secured. Users must also log-off or turn-off the system.
4. Screen-savers must be password protected.
5. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
6. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
7. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.

H. Additional Rules of Behavior for CNA e-TOOL System Administrators

CNA e-TOOL system administrators have a unique responsibility above and beyond that of regular users. In addition to being regular system users, they also have special access privileges that regular users do not have. Therefore, they need to be susceptible to additional Rules of Behavior over and above the common user.

1. CNA e-TOOL System administrators may only access or view user accounts with the expressed consent of the user and/or management.
2. CNA e-TOOL System administrators may not track or audit user accounts without the expressed consent of the user and/or management.
3. CNA e-TOOL System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. It is the CNA e-TOOL system administrators' responsibility to account for all system hardware and software loaned to system users for the execution of their official duties.
5. CNA e-TOOL system administrators are responsible for attending annual IT Security certification training. Failure to attend will result in having system access privileges revoked.



SECTION III - ACKNOWLEDGMENT

Prior to receiving authorization for CNA E-TOOL system access, every user should read and sign the ROB (this applies to system administrators since they are also "users" of the system). By signing the signature page, the user agrees to abide by the ROB and understands that failure to do so might be grounds for disciplinary action. Please retain a signed copy of the ROB for your personal records and submit the original signed copy to the CNA E-TOOL System Administrator for your local office.

I have read and understand the Rules of Behavior (ROB) governing my use of the Capital Needs Assessment Electronic Tool (CNA E-TOOL) and agree to abide by them. I understand that failure to do so may result in disciplinary action being brought against me.

NAME (PRINT)	ORGANIZATION
SIGNATURE	DATE SIGNED