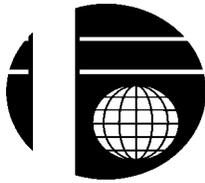


9 April 1999



Communications and Information

**INDIVIDUAL NETWORK USER
INSTRUCTIONS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFRC WWW site at <http://www.afrc.af.mil>. and the AFRCEPL (CD-ROM), published monthly.

OPR: 305 RQS/SC (Kathy Cramb)

Certified by: 305 RQS/MS
(Lt Col Gregory D. Hofacre)

Pages: 4

Distribution: F

This instruction implements AFPD 33-1. It establishes user understanding of policies, procedures, and guidelines for operation of Department of Defense (DOD) computers. It applies to all 305 RQS DOD computer systems used by Air Force organizations, personnel, and contractors. Users are subject to disciplinary action for any violation or abuse of this instruction. If clarification is needed for information contained in this instruction, contact the 305 RQS system administrators (305 RQS/SC).

1. Monitoring Policy:

- 1.1. The 305 RQS Network is a DOD computer system. DOD computer systems are provided and used only for OFFICIAL US Government business. All other uses are a violation of Federal law.
- 1.2. All information contained on a DOD computer system is owned by the DOD. Connecting (logging in) to the 305 RQS or Davis-Monthan Air Force Base Network by any authorized or unauthorized user constitutes express consent to monitoring, interception, recording, reading, copying, and disclosure without further notice. If this monitoring reveals possible evidence of criminal activity, this evidence may be provided to Federal law enforcement officials for possible prosecution.

2. Security Policy:

- 2.1. There is no right of privacy in this system. System personnel may give law enforcement officials any potential evidence of crime found on DOD computer systems.
- 2.2. If a user does not log-in, they will be denied access to this and other DOD-owned computer systems.
- 2.3. Do not leave terminal "logged in" and unattended under any circumstances. When leaving the terminal area, enable the password-protected screen saver on the system (if so equipped) and/or properly log off.

2.4. All users are required to complete a National Agency Check to be assigned by an official representative before receiving a network account.

2.5. All users are required to complete initial Security Awareness, Training, and Education (SATE) before a login account is granted. Once complete, users must complete annual SATE training. The Unit SATE Manager will help schedule this training.

2.6. This computer system and any software installed on it or any computer system connected to it by whatever means may only be used for processing official unclassified business of the DOD. Storing or processing classified information on any system not explicitly approved for classified processing is prohibited.

2.7. User will protect all sensitive unclassified data [Privacy Act (PA) and For Official Use Only (FOUO) information] processed, displayed, printed, or stored at user's terminal. PA information will not be stored on any server.

2.7.1. Mark and protect any removable storage media (i.e., disks) containing sensitive unclassified data. The Standard Form (SF) 711, **ADP Media Data Descriptor Label**, will contain the classification of data, the name, organization, and telephone number of the owner of the media, and a brief description of the contents of the data.

2.7.2. When no longer needed, destroy printed material containing **sensitive unclassified data** by tearing, shredding, or incineration.

2.7.3. When no longer needed, clear or purge any magnetic storage media containing FOUO information or PA data.

2.7.4. When not in use, store FOUO and PA data in a secure area.

2.8. Software or hardware will not be imported (to either the personal computer or server) without authorization from the 305 RQS System Administrators.

2.9. This system and its resources may be used for the processing of information directly related to classes or courses the user attends, only with written permission from the unit commander.

2.10. User must have the most current anti-virus software installed and running at all times. All software, floppy disks, or data files must be scanned for viruses before loading them to any DOD computer system, or uploading a file to the server (this includes any files received via E-mail).

2.11. If user observes anything, which indicates inadequate security for DOD computer system, the user will notify the 305 RQS/SC immediately.

2.12. User must comply with all security guidance issued by the 305 RQS/SC.

3. E-mail, Internet, and Storage Policy:

3.1. Air Force E-mail systems are provided to support Air Force missions. Only use E-mail systems for official, authorized, and ethical activities that are in the best interest of the Air Force. "Agency designees" (the first supervisor who is a commissioned officer or a civilian above GS/ GM-11 or supervision of the employee concerned) can allow limited personal use of E-mail. Limited personal use must conform to Air Combat Command or Air Force Reserve Command policies.

3.2. Users must comply with basic standards for using E-mail, which are common sense, common decency, and civility applied to the electronic communications environment. This includes following traditional military protocols and courtesies.

3.3. DOD systems will not be used to download, store, transport, distribute, relocate, or display pornography in any form. Pornography is defined as ANY erotic behavior or nude depiction of human form, whether in the form of a digitized picture, altered or “morphed” digitized picture, drawing, or any other characterization of the human body, which is not fully clothed. This includes depictions in any form, which displays the individual in “bikini” type clothing or garments which are designed or intended to be worn under clothing. The term “download” means transferring data or pictures from one computer system to another, either via, but not limited to, Internet connections, telephone connections, or copying to or from any other transportable electromagnetic medium.

3.4. Any other storing, processing, or displaying of offensive or obscene materials is prohibited.

3.5. Users are not allowed to annoy or harass another person, i.e., by sending uninvited E-mail of a personal nature or by using lewd, offensive, harassing, or intimidating language. User will not send mass E-mails to personnel outside the user’s squadron without proper coordination and approval of either user’s Unit Commander or Organizational Computer Manager (OCM).

3.6. Storage space on the Squadron Network is limited in quantity. When items are no longer needed for shared use or are archived, they should either be deleted or stored to floppy disk or some other medium off the Squadron Network. Additionally, even though the Squadron Network is backed up, the user should back up critical information.

3.7. Each user has a storage quota or limit of 20 Megabytes in their Microsoft Windows NT Exchange service. Exceeding this quota will result in blocking the user’s account.

3.8. There will not be any illegal, fraudulent, or malicious activities on or through government computers. These activities include but are not limited to: partisan political activity and political or religious lobbying or activities on behalf of organizations having no affiliation with the United States Air Force.

3.9. Activities for the purpose of personal or commercial financial gain are prohibited. This includes but is not limited to chain letters, solicitation of business or services, and sales of personal property.

3.10. No games will be used on Government systems. This includes all Windows, DOS, or Internet games. All games are to be removed.

3.11. Users are not allowed to maintain adult material or visit sites that maintain and/or distribute adult material while using this account and DOD- or Air Force-owned hardware and software.

4. Password and User Identification Policy:

4.1. Passwords are to be at least 8 characters in length, alphanumeric combination, and contain at least one special character. Passwords will not contain common names, foreign words, dictionary words, slang words, and profanity.

4.2. If user is on 305 RQS Network, you can only use the special characters: . ; : * & % !

4.3. Passwords will not contain information closely associated with the user’s own personal identity, history, or environment (i.e., birth date, dog’s name, license plate, relatives’ name, hometown and etc.

- 4.4. User identification (ID) and Password are considered FOUO and will be protected as such. User will not compromise their user ID or Password to other individuals or sources. User accepts full responsibility for all actions taken within the system under the assigned user ID.
- 4.5. User must memorize his or her password. Passwords are not to be stored anywhere (i.e., on 'yellow stickies', posted under keyboards or in books, left in desk drawers, programmed into function keys, part of batch, login scripts, setup files, or function keys, etc.).
- 4.6. Users will not share their password with anyone with the exception of their supervisor, commander, or any other authorized personnel. If password sharing is necessary for mission accomplishment make sure the password is changed immediately after shared access is no longer required.
- 4.7. The user will not permit anyone else to use his or her user ID. This is a violation of policy for any user to mask their identity or assume the identity of another user.
- 4.8. The system provides an automated password change every 90 days. Passwords are to be changed at least that often, when directed by the network security officer, or if suspicion that the password was compromised (report this to your system administrator).
- 4.9. Once a week the 305 RQS/SC personnel will run a program in an attempt to crack users' passwords. If a user password is cracked, he or she will be cutoff the Network. The 305 RQS/ CC must receive a letter from user's supervisor to get user back on the network. The second offense will call for complete termination of user account until further notified by the 305 RQS/CC.
- 4.10. For Users on Microsoft Windows NT operating system, one must keep the "Domain Administrators" in the "Local Administrators Group." This allows the System Administrator to retrieve a forgotten password and prevents system lockout.
- 4.11. Any changes of network settings on user's PC (i.e., IP address configuration settings, etc.) without permission of the 305 RQS/SC is prohibited.

5. Dormant User Policy:

- 5.1. If user is not going to be on station for an extended period of time because of temporary duty, leave, or any other reason, the 305 RQS/SC must be notified. The user will be removed from E-mail groups to ensure mail does not stack up and prevent problems with the Network.
- 5.2. All personnel leaving due to a permanent change of station or separation will out-process through the 305 RQS/SC office.

KENT D. CLARK, Col, USAFR
Commander