



DEPARTMENT OF THE NAVY

TRAINING SQUADRON THIRTY-ONE (VT-31)
501 BATAAN STREET SUITE B
CORPUS CHRISTI TEXAS 78419-5249

VT31INST 5230.1

ADMIN

14 JUN 2004

TRARON THIRTY-ONE INSTRUCTION 5230.1

Subj: MANAGEMENT INFORMATION SYSTEM SECURITY

1. Purpose. To establish security policy and procedural guidance on the use of command information systems (IS).
2. Discussion. Command information systems, including related hardware, network devices and Internet access, are provided for authorized U.S. Government use only. IS may be monitored at any time to ensure proper equipment utilization, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes internal and external inquiries by authorized DOD entities to test or verify the security of the systems. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over the systems may be monitored. Use of these DoD computer systems constitutes consent to monitoring. Unauthorized or improper use may lead to administrative, criminal or adverse action.
3. Policy. Command personnel are provided IS to improve the efficiency of respective departments. All personnel shall be thoroughly familiar with the policy and guidance set forth in this instruction and operate IS accordingly. Personnel are required to report unauthorized access, physical damage, contamination (virus) or improper use of IS to the Management Information System Officer (MISO).
4. Guidance
 - a. Classified information may not be saved onto any of the squadron's computers or discs, printed on printers, or copied with the photocopiers. Sensitive information shall be protected with a password if stored on a computer system and secured in a locked container if stored on a disk.
 - b. Personnel must log off of the system if leaving their workstation unattended for an extended period or at the end of the day. Use of password protected screensavers is authorized however, strict control and protection of passwords must be established and adhered to within the department.

VT31INST 5230.1

c. Initiate a virus scan on any information downloaded from the Internet or from a disc brought into the squadron from an outside source.

d. Passwords are an extremely important tool used to protect IS and sensitive information. Passwords should be changed periodically or when departmental personnel with access detach from the command. Use a combination of letters and numbers and avoid easily guessed passwords such as spouse's, children's, or pet's names and call signs. Never share or write down passwords.

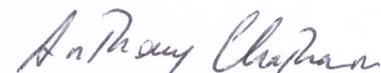
e. Hardware/Software. Computer hardware is sensitive and valuable. Squadron Duty Officer shall secure all command spaces in accordance with standing physical security practices. Department Heads shall conduct periodic inventories of hardware assigned and report any equipment that has been damaged or stolen. IS users shall avoid eating or drinking food in close proximity of IS to prevent damage. Personal IS equipment is unauthorized in squadron spaces.

f. Software installed on squadron's computers is for official government use only. Permission from respective Department Head is required if using IS for any educational purposes. Its use is authorized outside normal working hours. Copying or removing software is strictly prohibited. Users must request software additions to their workstations through the MISO. This ensures compatibility and proper installation and licensing of authorized programs.

g. Internet access is for official use only. Access to web sites not related to or supporting departmental responsibilities is strictly prohibited. MISO will conduct periodic monitoring of IS with Internet access and report any violations to the Department Head.

h. Every squadron member will have a CC-Mail account. This capability is provided to improve the flow of information between personnel. Communicating outside squadron domain via CC-Mail is authorized. CC-Mail shall never be used for personal gain or profit.

i. Playing games on command informational systems is prohibited.


A. P. CHATHAM

Distribution:
List I