

Communications and Information

COMPUTER SECURITY (COMPUSEC)

----**Compliance with this publication is mandatory**----

This instruction provides policy and guidance for managing and operating Automated Information Systems (AIS) and software as outlined in AFI 33-202. It applies to all personnel assigned to the 372d Recruiting Group and to all persons who are authorized use of AIS's within the 372d Recruiting Group.

SUMMARY OF REVISIONS

This revision clarified physical and information security guidelines.

General Requirements and Definitions

1. Overview. AIS's have become a major part of the Air Force work environment; this publication has been written to outline responsibilities for these systems. This publication combines information from several COMPUSEC Instructions and consolidates it into a single document.

2. Responsibilities. Within the group, the individuals with overall responsibility for AIS's are the System Administrators (SA) and Workgroup Managers (WM). The SA's are appointed Information Systems Security Officer (ISSO) for their respective units.

2.1. ISSO will ensure compliance with all information systems directives, regulations, and instructions.

2.1.1. Units collocated with DOD installations must also comply with host directives, regulations, and instructions to maintain connectivity and utilization of host information systems infrastructure.

2.1.2. Review all computer security and information assurance self inspections at least annually to ensure compliance with workstation/network security policies and software security guidance.

2.1.3. Notify all personnel of malicious logic reports received from AFRS or host base.

2.2. Terminal Area Security Officers (TASO) will be used for geographically separated offices.

TASO will ensure compliance with governing regulations.

2.2.1. TASO's, normally flight chiefs or their alternates, are appointed by the Commander. Each office will maintain TASO appointment letters in a Systems Administrators appointment letter book. A copy will be given to each appointed individual.

2.2.2. The current TASO will ensure that a new TASO is assigned prior to departing PCS, separating or retiring. This will be accomplished by contacting the SA *no less than* 10 days prior to the desired departure date.

2.2.3. The TASO is responsible for all AIS's assigned within the TASO's area of responsibility (office, flight, branch, etc.).

2.2.3.1. Ensure all equipment is protected from potential theft.

2.2.3.1.1. Do not place AIS in a position where they're visible from the exterior of the office and when possible restrict visibility from initial entry into the office.

2.2.3.1.2. Ensure the office is locked (windows and doors) each time you leave and at the end of the duty day.

2.2.3.1.3. Identify any high-risk or potential theft problems to SA/WM.

2.2.3.1.4. Property mark all equipment as per ADPE Custodian (EC) guidelines. Instructions can be found at <http://afrecruiting.com/eco/>

2.2.3.2. Apply all security patches and fixes to all AIS equipment as directed by SA/WM. All systems should be updated within 72 hours.

2.2.3.3. Ensure all systems have current antivirus software loaded and apply updated virus definition files within 24 hours.

2.2.3.4. Ensure all equipment is maintained in good, clean, operating condition. Report any discrepancies to the ADPE Custodian, especially inoperable or degraded power supply fans.

2.2.3.5. Train all users to scan all disks, downloaded files, and email attachments before running

3. Access. No individual may be allowed to use a computer assigned to the 372 RCG unless they meet the following criteria.

3.1. Their name is listed on the unit's computer access letter or have a signed letter from the SA, which identifies the individual and shows the inclusive dates of authorization (commonly used for Air Force personnel TDY to our squadron).

3.2. A current security clearance or national agency check has been validated

3.3. They have completed INFOCON and Network user Licensing computer based training (https://www.smartforce.com/learning_community/Custom/USAF).

4. Passwords. Passwords are required on all systems and must be changed every 90 days. Use passwords with at least eight alphanumeric characters (upper and lower case) with at least one special character (@&+, etc). NO WORDS, English or foreign, are allowed within the context of the password.

4.1 Screen saver passwords are required on all systems. Screen saver settings will be set to activate password protection within 5 minutes of inactivity.

4.2 Memorize the password. Do not place password on desk, under keyboards, on walls, or on sides of terminals. Do not store them in a

function key, log-in script, communications software, or internet software.

4.3. An individual is required to log out of the system if leaving the terminal for any length of time otherwise it's unsecure.

4.3.1. An account must be deleted or moved by the SA/WM prior to an individual's departure, not only for PCS, separation and retirement but for intersquadron moves as well. Contact the SA/WM *no less than* 10 days prior to the desired departure date to arrange for account retirement.

5. Official Usage. The computers used at work are government property.

5.1. The hardware and software used on these systems is obtained for exclusive use on the government AIS.

5.2. Only hardware/software provided by the SA can be loaded on an AIS.

5.3 No Freeware, public domain software, shareware, or privately owned software may be used on government AIS's without DAA Approval.

5.4 Games will be removed from all computers prior to being placed in service.

6. Internet. Accessing the Internet through a government computer or network uses a government resource. Government-provided hardware and software are for conducting official and authorized government business.

6.1. Using the Internet for other than authorized purposes may result in adverse administrative or disciplinary action. Activities listed in AFI 33-129 paragraphs 6.1.1 through 6.1.12 are prohibited. This does not prohibit commanders from authorizing personnel to use government resources to further their professional and military knowledge if they determine it is in the best interest of the government and authorization is documented by letter, local operating instruction, or explicit policy.

7. E-Mail. E-mail is used to supplement or replace traditional mail, facsimile, telephone, and other messaging systems. Refer to AFI 33-119,

and AFI 33-129 for prohibited activities while using government E-Mail resources.

7.1. Air Force employees will use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

7.2. E-mail is official communication. E-mail may be used to transmit both formal and informal correspondence. E-mail account users bear sole responsibility for material they access and send.

7.3. The basic standards for using e-mail are common sense, common decency, and civility applied to the electronic communications environment. This includes following traditional military protocols and courtesies.

8. Personal Use. The following paragraph describes what *is/is not* allowed to be done on a government computer with regard to personal information/correspondence.

8.1. The commander may grant approval authority to supervisors for allowing subordinates to use government computers for personal information /correspondence as long as it doesn't interfere with the performance of government business and conforms to all items outlined in this publication.

8.2. Supervisors may allow the following type of personal information or correspondence.

8.2.1. Projects considered beneficial to the Air Force.

8.2.2. Professional Military Education studies and other military education courses.

8.2.3. Off-duty education (exceptions below)

8.3. Individuals may not use government computers for the following types of personal use (supervisors do not have authorization authority).

8.3.1. Although the AIS may be used for educational purposes, school diskettes may not be introduced into the AIS. School diskettes are

another main source by which viruses are introduced into systems.

8.3.2. Government AISs are not allowed to be used for producing, printing or storing personal resumes (non-military use).

8.3.3. Any type of gambling pool, betting, sports lottery, online lottery, online trading, or any other file whose purpose is to make or manage money from an illegal operation or an illegal manner is prohibited.

8.3.4. Any purpose which would result in financial benefit to the individual or in support of off-duty employment or self-employment is prohibited. **NOTE:** The term "load" refers to placing the diskette into the AIS, even if the contents of the program are not placed on the hard drive.

9. Physical Security. The following precautions will be exercised to protect computer equipment from theft and damage.

9.1. Make sure proper markings are on output products and storage media as required by current AFSSI's and AFI's. Use AFRS supplied warnings and banners. Verify that sensitivity markings on products are correct. SF711 labels, Privacy Act labels, AF 992 ADPE labels and engraving are the most commonly used marking tools.

9.2. Portable computer systems (Laptops) and accessories must be secured out of sight when left unattended for any period of time. Items must not be stored or left where visible from the exterior of the building or room/office. Users are responsible for keeping up to date (knowledgeable) on AFRS policy revisions.

9.3. When unattended, or at the end of the duty day, terminals will be logged off, magnetic media secured, and all printers and monitors turned off. Shared workstations may remain on for access to files by authorized users working after duty hours as long as proper safeguards have been implemented against unauthorized access.

9.4. Systems must be equipped with surge suppression devices. Do not plug coffeepots, electric pencil sharpeners, etc. into surge

suppressors which are in use by computer system(s).

9.5. Do not eat or drink near computer system or peripherals.

10. Shareware. Shareware, freeware, and public domain software programs will not be introduced into any system unless provided through the SA with DAA and Recruiting Service approval.

10.1. Shareware and freeware programs are different by design. These types of programs are both primary targets for viruses.

10.1.1. Shareware programs are written for the purpose of being sold. These programs are distributed freely and the user is required to evaluate the program and then purchase or remove the program.

10.1.2. Freeware programs are written in order to provide a program without requiring a fee.

10.2. Public domain software is any software available to the general public, regardless of source, that has not been approved for use by the DAA.

10.3. If an individual wants to have a shareware or freeware program approved for use, he/she must do the following:

10.3.1. Submit a complete, documented copy of the program to the SA.

10.3.2. Provide a brief description of what the program does.

10.3.3. Provide a statement as to what benefit the unit would gain by using the program.

10.3.4. Indicate what mission impact would exist if a request is disapproved.

10.4. Do *not* use either shareware or freeware programs while awaiting approval. NOTE: The first thing the SA/WM will do with a program that has been submitted is test it for viruses.

11. Viruses. Viruses have become a major concern within the computer industry. Viruses are introduced by placing an infected diskette

into the disk drive of a computer, browsing unofficial internet sites, and e-mail attachments. There is no way of knowing that the disk, internet site, or attachment is infected until it's too late.

11.1. The following are the most common ways viruses are introduced into computer systems.

11.1.1. "School" disks. Any diskette that is obtained from a learning institution. Typically, this occurs when an individual takes a college course and the college requires a program to be operated from a diskette (regardless of who provides the disk).

11.1.2. Games. Any diskette which contains a game other than an original game disk purchased from reputable company.

11.1.3. Downloading files from electronic bulletin boards or internet sites.

11.1.4. Browsing unofficial internet sites for downloads, auctions, day trading, and commercial e-mail.

11.1.5. Running e-mail attachments.

11.2. The following guidelines are provided in order to reduce the possibility of a virus entering our computer network.

11.2.1. A Virus protection program is required to be loaded and running at all times (AFRS approved virus protection program is Norton Anti-Virus). Signature files will be updated within 24 hours of release.

11.2.2. No diskette shall be introduced into our computers from any learning institution (i.e., school disks).

11.2.3. No games shall be played on or loaded into any government AIS.

11.2.4. An individual desiring to put personal information/correspondence onto a diskette must virus scan the diskette *prior* to use.

What to do if a virus is suspected on a computer.

11.3. Do **NOT** shut the system off!

11.3.2. Do **NOT** do a tape backup! This is so a virus is not transferred to backup tapes!

11.3.3. Contact the SA/WM immediately. If no one is available, contact the base CSSO, base ISSO or AFRS help desk at DNS 487-2335/5097 or commercial (210-652-2335/5097).

12. Personal Computers. By order of the 372d Recruiting Group Commander, under no circumstances will personally owned computers be allowed to be used for government business.

12.1. Personally owned accessories may be used when approved by squadron commander and the items are properly labeled and documented by the squadron SA.

13. Diskette. The following guidance is provided regarding diskettes.

13.1. Government provided diskettes are to be used for government use only.

13.2. All diskettes will be labeled. Labels should indicate the classification of data stored on the disk; the name, unit/office symbol, and telephone number of the owner; and a brief description of the contents of the disk. Use either Standard Form 711 or labels provided by the manufacturer.

13.3. Diskettes must be marked with a Privacy Act label (AFVA 205-15), if applicable.

13.4. Any diskette that is taken out of the office must be virus scanned by the SA/WM prior to placing it back in any of our computers.

14. Points of Contact. Remember that this publication is only designed to provide the **basic** information that is needed as it relates to the use and maintenance of government owned AIS's within the 372d Recruiting Group.

14.1. Group and squadron SA/WM's are the focal point for all AIS issues and should be contacted if there are any questions or problems relating to AIS's.

14.2. If the SA/WM is not available, the Recruiting Service trouble desk can be reached by calling DSN 487-2335 or commercial (210) 652-2335. The trouble desk should be called for emergency computer hardware or software problems only – all other problems should be handled by the SA/WM.

15. Report of Survey. A report of survey must be conducted when an ADPE item is lost or stolen. To initiate the report of survey, notify the ADPE Custodian who will then notify the ROS Administrator in the squadron or group RSRL branch.

GAIL M. GILBERT, Colonel, USAF
Commander