

**19 DECEMBER 2001**



**Communications and Information**

**COMPUTER SECURITY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 911 AW/SC (Robert A Langhurst)

Certified by: 911 AW/CC (Col Baxter Lane)

Pages: 10

Distribution: F

---

This instruction implements AFD 33-2, *Information Protection*, AFI 33-202, *Computer Security*. It establishes, prescribes responsibilities and procedures and implements the 911 AW Air Force Reserve Station Pittsburgh (911AW) Computer Security Program. It deals with procedures for the protection of all government-owned computer systems, including all associated hardware and software, and implements applicable portions of the Air Force System Security Memorandums (AFSSMs) and Air Force System Security Instructions (AFSSIs).

**1. Scope.** This instruction is directive in nature and applies to all assigned personnel. Failure to observe its provisions may result in administrative or judicial sanctions to include punishment under the Uniform Code of Military Justice (UCMJ) and Federal Law.

**2. General.** This instruction covers all computers in or belonging to the 911<sup>th</sup> Airlift Wing.

2.1. Security responsibilities for these systems are assigned to:

2.1.1. Designated Approval Authority (DAA)

2.1.2. COMPUSEC Manager (CM)

2.1.3. Computer Systems Manager (CSM)

2.1.4. System Administrator (SA)

2.1.5. Information Systems Security Officer (ISSO)

2.1.6. Small Computer User

2.1.7. Security Awareness, Training, and Education Manager (SATE Manager)

2.2. Systems will not be used for processing information until the ISSO and Unit COMPUSEC Manager has completed all administrative requirements and the DAA has granted approval. All computers connected to the LAN are covered under the LAN Certification and Accreditation. All functional area servers and systems will be certified and accredited with a Certificate of Networkiness (CTO) and a Certificate to Operate (CTO) approved thru MAJCOM. Subsequent certification will be completed

per AFI 33-202, Chapter 4; and must follow the new Department of Defense (DOD) 8510.1-M, *DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*.

2.3. Computer systems connected to the 911AW local area network (LAN) NIPRNET are **NOT** authorized to process classified information.

2.4. Computer systems connected to the SIPRNET or designated stand-alone computers are authorized to process classified information.

2.5. On all small computers used to process classified data, dedicate at least one set of removable storage media for classified processing only. This set of media will include, but is not limited to, system and word processing system disks, work disks, and dictionary disks, and will be handled and stored per AFI 31-401, *Managing the Information Security Program*. One set of removable storage media will also be dedicated for unclassified use.

2.6. Users processing classified data must have their computer monitors, display terminals, and printers positioned so that unauthorized personnel cannot observe them through doors, windows, or by casual observation. The monitor should be positioned so the user can observe personnel entering the work area.

2.7. Systems processing classified data will be marked with the highest classification label (i.e. SF 707- SECRET) of information authorized for processing.

### 3. Roles and Responsibilities.

3.1. **COMPUSEC Manager.** The COMPUSEC Manager establishes standardization and reporting controls as specified by the DAA and implements the COMPUSEC program to ensure compliance with AFI 33-202, including any major command (MAJCOM) or wing supplements. The objectives of COMPUSEC are to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle.

3.2. **Computer Systems Manager (CSM).** The CSM is the office manager or section chief who is responsible for the overall operations of LAN and computer support in the facility. The CSM responsibilities are outlined in AFI 33-202, para 2.11.2. In addition the CSM will:

3.2.1. Establish security procedures and measures for the unit work area.

3.2.2. Appoint ISSOs to assist system administrators and users in the security aspects associated with network operations under CSM control. These individuals must be knowledgeable of computer security principles.

3.2.3. Will approve local computer security procedures for the workstations and remote terminal areas.

3.3. **Designated Approval Authority (DAA).** The DAA, for all information systems at 911AW, is the Wing Commander.

3.4. **Unit COMPUSEC Manager.** The Unit COMPUSEC Managers administer the Computer Security Program for their organization. These responsibilities are outlined in AFI 33-202, para 2.11.1. In addition, the Unit COMPUSEC Managers will:

3.4.1. Ensure all computer systems in the organization have been submitted for accreditation DAA approval before operational use.

3.4.2. Develop procedures to ensure staff agencies, and ISSO's are informed of significant changes in COMPUSEC policies and procedures.

3.4.3. Forward all accreditation packages to the Wing Information Assurance office. Interim or type accreditations are due once a year and full accreditations (i.e. LAN or other servers are due every three years or after major changes). All certification & accreditation packages are reviewed every year to identify or make note of any changes to the system. Type Accreditations are processed from the System or Program developer office and only certain areas of the accreditation need to be changed to make it unique to Pittsburgh.

3.4.4. Report computer viruses, using the 911AW Incident Reporting Procedures found under Virus Reporting on the Pittsburgh Communications INTRANET page.

3.5. **System Administrator (SA).** The SA is responsible for the overall operation of their unique system server. The Unit Commander will appoint a primary and alternate SA assigned in writing. A copy of the appointment letter will be sent to the 911 AW/SC office for their files. The SA will:

3.5.1. Maintain a system status file through REMEDY which will include system maintenance the date, time, who performed the maintenance, and what maintenance was performed.

3.5.2. Ensure the system is available to perform day-to-day operations as required.

3.5.3. Develop and periodically review backup strategy. Ensure the backup strategy is followed and back-ups are performed on a rotational basis. (The LAN server backups are being maintained off site at Bldg 128, SCBA.)

3.5.4. Review audit trails daily and perform system maintenance.

3.5.5. Inform the CSM, ISSO, and Automated Data Processing Equipment (ADPE) custodian of any potential problems that may affect the performance of the system.

3.5.6. Assist in the installation of new software.

3.5.7. Approve all system configuration changes. This includes installation and removal of hardware/software and relocation of computer equipment.

3.6. **Information Systems Security Officer** . ISSO will assist system administrators and users in the security aspects associated with network operation. ISSO must be knowledgeable of computer security principles. In addition ISSO will:

3.6.1. Ensure antivirus software is loaded on all PCs. (The Norton Anti-virus software is being pushed down to all PCs by the Network Control Center). If you're PCs are not up dating properly report to your Workgroup Manager or the Communications "Help Desk".

3.6.2. Report any COMPUSEC incidents or vulnerabilities per AFSSI 5021, *Computer Security Reporting Programs Procedures and Formats*.

3.6.3. All Wing computers will be configured to perform automatic virus scans of fixed media on a daily basis.

3.6.4. Maintain a log of all Air Force Computer Emergency Response Team (AFCERT) advisories and notices, which contains the advisory number, date, initials, and actions taken. All advisories need to be acted upon.

3.6.5. Ensure the audit trail log is checked daily for any anomalies and report findings per AFSSI 5021. Audit trail logs will be included in the backups and kept for 90 days in electronic form.

### 3.7. **Small Computer User.**

3.7.1. Understand and apply approved guidelines and procedures when using the systems and equipment.

3.7.2. Inform the ISSO, UCM, and CSM of incidents or circumstances that may impact the security posture of the system or other data resources.

3.7.3. Safeguard classified sensitive and critical computer resources in their custody.

3.7.4. If connected to the LAN, ensure they are logged off prior to leaving his/her workstation.

3.7.5. Ensure system configuration files (autoexec.bat, config.sys, etc.) are not modified without SA approval. Changing the configuration of these files can cause LAN workstation failure.

3.7.6. All stand-alone computers will have an anti virus program loaded and updates will be perform when directed by the ISSO or SA.

3.8. **Security Awareness & Education Training Manager.** The Unit SATE Manager is responsible for their unit Computer Security Training, both initial and annually. The SATE Manager will provide training through the SATE Internet Computer Base Training (IBT). Training will be documented on 911 AW Form 5, SATE Training Card, per 911 AW Supplement/AFI 33-204.

## 4. **911AW LAN.**

4.1. **System Description.** The 911AW LAN consists of approximately 800 user accounts. Individual workstations are configured differently. Differences include the size of the internal hard drives, monitors, keyboards, central processing unit model and the software installed on them. Specialized equipment used by individual workstations includes scanners, and laser printers. System data storage is provided by individual workstations via on-line internal hard drive, personal/workgroup/shared folders on the file server, and off-line devices. Off-line devices include 3.5- inch floppy disk drives, CD/RW drives, and zip drives.

4.2. **Access Controls.** Automated access controls help limit access to the 911AW LAN to authorized users only. These controls include user passwords and restricted file access.

4.2.1. All users will have their clearances verified through the Unit Security Manager and will receive their Security Awareness, Training, and Education (SATE) training prior to receiving their LAN password. This ensures all users will have the required need-to-know and clearance to use the 911AW LAN and personal computers.

4.2.2. Each LAN user must use a personal password (i.e., screen saver, basic input and output system (BIOS) and LAN). When leaving the workstation, or turning over control to another person, users must log off the LAN. LAN passwords are maintained in an encrypted format on the file server.

4.3. The SA restricts access to files on the file server. Working groups are allowed access to only those files and storage devices needed to accomplish their tasks. This prevents an intruder from gaining access to all parts of the system. Individual users may also protect files within their particular user directory. The SA can provide assistance in protecting these files.

4.4. **Audit Requirements.** As a minimum, on sensitive systems, the audit mechanism must provide for recording any event that attempts to change the security profile. As a minimum, provide a mechanism for recording:

- 4.4.1. Login and logout.
- 4.4.2. User actions to open, close, create, execute, modify, or delete programs or files.
- 4.4.3. Date and time of the event.
- 4.4.4. Type of event.
- 4.4.5. Success or failure of the event.
- 4.4.6. Name of program or file introduced, accessed, modified, or deleted.

4.5. **Password Management for LAN Workstations.** While assigned to 911AW all users will require a valid User ID and password. All user IDs and passwords are unclassified, but should be protected as "For Official Use Only." Screensaver passwords will be placed on all computers assigned to 911AW.

4.5.1. User IDs will not change while the individual is assigned. However, all passwords will change every 90 days. The domain controller will force LAN passwords to change when logging in on the 90th day. Users will follow the instructions when notified by the network to change their password.

4.5.2. Passwords must be at least eight characters long and must have one of each of the following-alpha-numeric, upper and lower case, and special characters (no family name, SSAN, etc.). Passwords will not be written down or released to another individual.

4.5.3. Suspected compromises will be reported to the CSM, ISSO, or SA within 24 hours. The old password will be deleted and a new password issued.

4.5.4. Personnel assigned to the installation will in-process through the Communications Help Desk Branch to receive their User ID and password. Also, they will out-process through the Help Desk to have their user account deactivated. Upon supervisors' notifications of personnel actions the SA will suspend passwords within one duty day when:

- 4.5.4.1. There is pending or current punitive action.
- 4.5.4.2. The Wing Commander has suspended the user access to the system.
- 4.5.4.3. Personnel are on extended TDY (more than 3 months).

4.6. **Physical Protection.** Physical protection is the easiest part of computer security to control, but it is also the easiest to circumvent. Failure to follow established procedures subjects our resources to unnecessary risks.

- 4.6.1. Lock all offices that are capable of being locked during nonduty hours.

4.6.2. During duty hours, all personnel will lock their workstation (Ctrl, Alt, & Del) or use a screensaver password when leaving their work area. This will prevent unauthorized users from gaining access through unattended workstations. Due to the wear and tear caused by repeated electrical surges, all workstations will be turned off only at the end of the duty day.

4.6.3. Whenever possible, electrical surge protectors will be used for computer equipment. This provides protections from harmful electrical surges to delicate internal components. Do not plug other electrical equipment (coffee pots, microwave ovens, etc.) into sockets used by computer equipment. These can cause power surges that can damage computer power supplies and integrated circuits.

4.6.4. Upon notification from proper authority, sometimes computer systems will be powered down when lightning is in the local area. (With the surge protectors this doesn't occur all the time now).

**4.7. Daily Operating Procedures** . The file server's operations/applications are available at all times. The SA may take the file server down for maintenance and other unforeseen events; however, all attempts will be made to provide users with enough prior notification to prevent lost work. The file server will be brought down when environmental concerns occur (lightning hazards, excessive heat, unstable power, etc.). All users will be given three minutes notice, whenever possible, prior to system shutdown. A message will display on the computer screen. When this occurs, save all work and log off the LAN.

4.7.1. Access to the LAN is through user workstations using valid User IDs and personal passwords. Access will be restricted to directories, applications, and files to which the user is authorized access. When leaving workstations or transferring control to another user, log off the LAN.

4.7.2. All users should backup their mission-critical files regularly. This habit will preclude loss of data due to computer/hard drive failures. A complete system backup may be necessary. The SA will backup the file server daily; however, users are responsible for backing up their workstation hard drives.

**4.8. Software Security.** Virus protection software is available from the Unit COMPUSEC Manager. This software must be loaded on all PCs and servers, including standalone computers.

4.8.1. Virus protection software will scan the memory and hard drive daily. Additionally, all floppy diskettes will be scanned before use; this includes commercial software purchased for installation. Software not owned by the government will not be used on government systems.

4.8.2. Personally owned applications will not be brought in for use. Data disks containing work accomplished at home or on TDY may be brought in, but must be scanned for viruses prior to use. **Games and entertainment packages are prohibited.**

4.8.3. All diskettes, and/or CDs in an environment running both non-classified and classified will be labeled with level of classification, (unclassified- green label SF710, classified- red label SF707).

**4.9. Portable Computer Security** . While being used in an office environment, the security and environmental requirements for a portable computer are the same as a stationary system (remember this computer can be easily stolen).

4.9.1. Portable systems may be loaned to unit members, on an as-needed basis, when performing TDYs, formal schools, etc. However, when on loan, members must not directly or indirectly use, or allow the use of, government property or resources for other than approved activities.

4.9.2. Users must conform to the security provisions established in this instruction. Each user must implement procedures to prevent unauthorized or illegal use of portable computers. Neither equipment nor software will be used for personal projects unless specifically authorized, in writing, by the commander or designated authority.

4.9.3. Liability for loaned equipment is transferred to the supervisor, who certifies the loan is for an approved purpose, and the borrower, who assumes responsibility for loss/damage while the equipment is away from the work area.

4.9.4. Before authorizing the loan of computer equipment to work on approved projects outside the work area, the supervisor must first determine if the work could be completed in the work area (either before, during, or after duty hours).

4.9.5. **ABSOLUTELY NO CLASSIFIED PROCESSING IS ALLOWED ON LOANED PORTABLE COMPUTERS.** The user must be aware that all information is of a sensitive nature. Take appropriate steps to safeguard the equipment, the data it contains, and the media used on the system.

4.9.6. Physical security must be a prime concern when equipment is on loan. Due to the small size and portability of laptop computers, there is a significant danger of theft if the equipment is left or stored in an uncontrolled area. The laptop should be secured for protection when left unattended. (i.e., a locked cabinet, or locked room.)

4.9.7. An AF Form 1297, **Hand Receipt**, will be generated by the Equipment Custodian (EC), and the borrower will sign the hand receipt. A copy of the hand receipt will be provided to the ADPE Custodian. The borrower will keep one copy and be prepared to present it, if necessary, to show authorized use of the equipment. The borrower will return the equipment to the appropriate office for certifying the equipment is undamaged and functioning properly. If undamaged, the borrower will be given the original receipt. If damaged, notify the ADPE custodian for processing actions for replacement or repair of the equipment.

4.9.8. Guidance on the use of Personal Digital Assistants (PDA): A PDA is an automate information system and therefore is subject to Air Force policy and guidance governing the security and use of a desktop or notebook computer. Individuals may use PDAs to process unclassified information from desktop workstations; take notes, save information, or write emails when away from desktop workstations and synchronize information with desktop workstations. **DO NOT PROCESS OR MAINTAIN CLASSIFIED INFORMATION.** Do not connect or subscribe to commercial Internet Service Providers (ISP) for official E-mail services. The use of commercial ISPs for official business is not allowed due to the high operational risk posed by the possible collection of sensitive information. Do not synchronize information across a network using a wireless connection. All users are required to sign a PDA agreement stating they are aware of all terms pertaining to PDAs. All PDAs are tracked in the Inventory Processing Management Inventory for accountability. If a PDA is lost, a report of survey must be accomplished in accordance with Air Force Manual 23-220, *Reports of Survey for AF Property*.

4.10. **Virus Prevention.** A virus is a penetration technique to gain access, or collect, falsify, or destroy data in a computer system. It is a software attack that works the same way on a computer as a

biological attack works on people. It searches the computer for a program that is germ free. It then copies itself and attaches to that program and continues looking for other uninfected programs to infect. It can cause corruption or erasure of data, and can even lead to unauthorized access or transmission of data. Personal computers are highly susceptible to viruses through downloaded bulletin board files, disks from unknown sources, hostile web sites, etc. To help prevent penetration of a virus on computer system, follow these rules:

- 4.10.1. Frequently back-up files.
- 4.10.2. Limit access to PCs.
- 4.10.3. Use Antivirus software to scan all floppies, hard drives, and E-mail messages.
- 4.10.4. Scan hard drives after systems return from repair centers.
- 4.10.5. Don't use illegal copies of software or disks brought from home.
- 4.10.6. Beware of borrowed software or unsolicited software.
- 4.10.7. Scan all commercially procured software before installing; software out of the wrapper has been found with viruses.
- 4.10.8. If you use one set of disks to install multiple copies on different computers ensure that all the disks are write-protected to avoid possible virus spreading.
- 4.10.9. If a computer is identified as being infected, it will be isolated immediately (no exceptions).

4.11. **Virus Reporting.** Use the chain of command to report suspected viruses on computer systems. **DO NOT ATTEMPT TO USE A COMPUTER SYSTEM SUSPECTED OF CONTAINING A VIRUS! Immediate supervisors, ISSO, and Unit COMPUSEC Manager** should be notified as a minimum. There are three types of incidents, which are closely related to viruses:

- 4.11.1. ROUTINE: Hacker activity or malicious logic is suspected or threatened.
- 4.11.2. PRIORITY: Hacker activity or malicious logic has been confirmed.
- 4.11.3. IMMEDIATE: Hacker activity or malicious logic, like a virus, is confirmed and in progress.

4.12. **Maintenance Procedures.** Periodic maintenance on computer systems is vital to the extended life of computer workstations. The proper upkeep and preventive procedures will help prevent the premature loss of valuable center assets. Only authorized personnel should complete maintenance on a computer or on the LAN.

- 4.12.1. Preventive Maintenance. External components should be cleaned with a mild soap and water solution--**DO NOT USE AMMONIA PRODUCTS.** Please consult with the System Operations Branch before you begin cleaning your system. In addition to physical cleaning, the hard drive should be examined (using software) for proper configurations and optimized regularly.
- 4.12.2. System Failures. Users will report system failures or problems to their Workgroup Manager (WM) or the Help Desk at Ext. 8444. Network management personnel assigned to 911AW will examine the workstation or other component and attempt to resolve the problem. They will always be utilized first when repairs are required. They will troubleshoot problems and determine the repairs to be made. If available, the repairs can be made using on-hand stock. If parts are not

available, they will provide a source and price for the needed item. The user will procure the part or purchase with their Government IMPAC card, if less than five hundred dollars. If the cost is over five hundred dollars the money will be transferred to SC to purchase with the special IT IMPAC card. The IMPAC purchase will be approved through the division chief and budget office. They will decide to replace or repair the component based on cost estimates and replacement costs. Authorized service centers will repair all unresolved problems and out of warranty items.

4.12.3. Workstation Failures. Should a workstation fail and need extensive repairs, the CSM will develop a plan to work around the station's loss. Proper data backup procedures will prevent catastrophic losses.

4.12.4. LAN File Server Failure. The SA will select a replacement workstation for the file server should it fail. Due to the size of the LAN's hard drives, all applications that reside on the server may not be able to be restored to the smaller workstation. Fixes may include restricting the size of user directories, preventing storage of E-mail on the server, etc. Such actions will limit on-line storage and will require improved planning by system users.

4.12.5. LAN Connectivity Failures. LAN connectivity failures are normally related to software problems. To prevent this type of failure, do not change system files without consulting a Workgroup Manager or the Help Desk. Non-software connectivity failures usually occur when components are physically disconnected from the LAN cabling. Do not disconnect any component from the LAN cabling. Only network management personnel are authorized to disconnect and connect components to the LAN.

## **5. Transmission of Classified Information on an Unclassified System.**

5.1. Notify the ISSO and the Unit COMPUSEC Manager of any E-mail message (or any other type electronic correspondence) containing classified information that was transmitted over one or more unclassified LANs. The Unit COMPUSEC Manager will then contact the SA and the Wing COMPUSEC Manager. AFSSI 5020, *Communication-Computer System Security Publication*, provides clearing, purging, and declassification guidance, and lists references for Air Force- and DoD-evaluated products approved for declassifying magnetic media.

5.2. The Wing COMPUSEC Manager will contact the E-mail originator. The Manager will find out all addressees of the E-mail, including their organizations. In addition, request the following information from the E-mail recipients:

5.2.1. Was a hard page copy of the information made? If yes, secure the hard-page copy and sanitize the printer per AFSSI 5020.

5.2.2. Was the information saved to a system's hard drive or removable magnetic storage media such as a floppy disk? If yes, purge the data from the hard drive or removable storage device. If the storage device is not to be purged immediately, secure it accordingly. Again, identify variances. For example, if the addressee saved the information to a hard drive or floppy disk and then later deleted the file, the information is still available. Recover and then purge the information.

5.2.3. Was the E-mail or information sent to anyone else? If yes, contact the new addressees and SA and restart the cycle. Maintain documentation on all purging (i.e., declassification) actions.

5.3. The SA must purge the E-mail from the LAN. The method used to purge the E-mail will vary depending on specific LAN hardware and software configurations. The SA is the system expert and is

expected to know how to locate all copies of the information on his/her particular system. Use an AF approved purging method (AFSSI 5020). Identify variances such as when a user deletes an E-mail message. Normally this action only deletes systems pointers to the information, not the data itself. The SA must first retrieve the information and then purge the data rendering it unrecoverable. If the incident occurs over a time frame in which system back-ups were performed, secure and purge the back-up media.

5.4. Recovery action should be a team effort. As a minimum, team members should include information assurance officer; help desk technician, system administrator, and network control center personnel. Each of these members has expertise and skills to answer questions and provide assistance to system administrators or individual users responsible for purging their systems. The transmission of classified information over an unclassified LAN is a security incident reportable under AFI 31-401. Information Assurance personnel are responsible for ensuring the information is purged from computer systems. The Unit Security Manager (USM) is responsible for other actions associated with security incidents. When an incident occurs, ensure someone in the affected unit notifies the USM.

## **6. Remenace Security.**

6.1. Nonvolatile storage media containing classified and/or sensitive material (sensitive includes, but is not limited to, Privacy Act and FOUO material) must be cleared per AFSSI 5020 prior to turning in or before uncleared maintenance personnel begin working on the system.. Remember deleting is not acceptable, as information may still be recovered. Only use an Air Force approved product to sanitize the hard drives if turning into another DOD agency. If computer will be issued outside Department of Defense channels the hard drive is removed.

F. BAXTER LANE, Colonel, USAFR  
Commander