

**BY THE ORDER OF
THE INSTALLATION COMMANDER**

CHARLESTON AFB INSTRUCTION 33-501

3 JANUARY 2000

Computer Security

**COMPUTER SECURITY (COMPUSEC)
MANAGEMENT**



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO/PP WWW site at:
<http://afpubs.hq.af.mil>.

OPR: 437 CS/SCBS/WIAO (Mr. Jeffrey Morey)
Supersedes CAFBI 33-501, 31 March 97

Certified by: (Major Douglas J. Taylor)
Pages: 6
Distribution: F

SUMMARY OF REVISIONS

Removed information and added specific references to the relevant current Air Force and Air Mobility Command directives.

1. Purpose:

1.1. This base instruction provides guidelines to assist units in establishing and implementing an effective computer security program on Charleston AFB. This instruction provides reference to, and specific amplification of, the applicable Air Force and Headquarters Instructions.

2. Applicability:

2.1. This instruction covers all units or agencies utilizing Charleston AFB Automated Information Systems and/or network connections.

3. Responsible Entities:

3.1. A detailed listing of all required responsibilities for each entity below can be found in AFI 33-202 and AMCI 33-202 Vol. I.

3.2. Designated Approving Authority (DAA): The DAA for base systems classified up to Secret is the Wing Commander. The 437th Airlift Wing Commander has delegated this responsibility to the minimum position for the designee; squadron commanders or equivalents with operational jurisdiction over the AIS for which they are appointed. The DAA announces the decision to fully accredit an AIS, accredits on an interim basis, or disapproves AIS accreditation.

3.3. Wing Information Assurance Office (WIAO): The WIAO implements the COMPUSEC program for the base; provides security guidance to all base organizations on Command, Control, Communications, and Computer (C4) systems security programs; establishes and publishes base COMPUSEC policy; and assists all base organizations in the development of their COMPUSEC programs.

3.4. Unit COMPUSEC Manager (UCM): The UCM ensures users operate, maintain, and dispose of AISs according to security policies and practices. The UCM develops a system security policy for systems and networks, and manages a COMPUSEC training program for system users.

3.5. Computer Systems Manager (CSM): The CSM performs the same duties as a UCM, but for a network. The CSM reports required computer security information to the UCM. The CSM will ensure that all appropriate security patches are installed.

3.6. Computer System Security Officer (CSSO): The CSSO ensures that users follow the established security procedures and reports security problems, incidents, and vulnerabilities. The CSSO will establish and update a computer access listing for all AISs in their area.

3.7. Work Group Manager (WGM): WGMs are tasked with connecting AISs to servers and may be tasked with UCM/CSM/CSSO duties.

3.8. Users: Users must ensure AIS information is protected by understanding and following established security procedures. They must also report security problems, incidents, or vulnerabilities. Users will receive initial and periodic refresher training in COMPUSEC. Users will not be allowed to use an AIS before receiving training.

4. Applicable Publications:

4.1. Air Force Instructions

AFI 31-101, Vol. 1, The Physical Security Program

AFI 31-401, Information Security Program

AFI 33-114, Software Management

AFI 33-115, Networks Management

AFI 33-129, Transmission of Information Via The Internet

AFI 33-202, The Computer Security (COMPUSEC)

AFMAN 33-223, Identification and Authentication

AFMAN 33-323, Computer Records Management

AFSSI-5024, Volume I, The Certification And Accreditation (C&A) Process

AFSSI-5024, Volume II, The Certifying Official's Handbook

AFSSI-5024, Volume III, The Designated Accreditation Authorities Guide

AFSSI-5024, Volume IV, Type Accreditation

AFSSI-5102, Computer Security (COMPUSEC) for Operational Systems

4.2. Air Mobility Command Instructions

AMCI 33-202 Vol. 1, AMC Information Assurance

4.3. Base Publications

CAFBI 33-601, Base Area Network (BAN) Policy (DRAFT)

CAFBM 37-1, 437th Airlift Wing Networking Procedures

4.4. Operating Instructions (OI)

4.4.1. An OI is for unit or area specific procedures over and above those required in AFIs and may include information for protection of media, software, and hardware, maintenance, and security of hardware whether it is used for classified or unclassified processing.

Media -- i.e., keep away from magnets, keep current backups, proper storage, etc.

Software -- i.e., make backups, utilize backups to load software, store master software in secure area.

Hardware -- i.e., secure office area, position monitor so it cannot be seen by anyone else, lock keyboard/system, etc.

Maintenance -- i.e., establish procedures for obtaining government/commercial maintenance.

Security -- i.e., specify security requirements commensurate with the value of the AIS, authorize and control access as appropriate, etc.

4.4.2. OIs can be coordinated through the WIAO to prevent conflict with higher directives.

5. Certification and Accreditation (C&A) of AISs:

5.1. Detailed instructions for initial C&A of AISs can be found in AFSSI 5024, volumes 1-4.

5.2. UCMs are required to provide the WIAO an update to existing C&A packages monthly. Updates will be sent via e-mail to the WIAO. The body of the message must include the statement, "I certify that the AISs listed in the attached document meet all the requirements specified in my System Security Authorization Agreement and that their addition does not significantly impact the security posture as described in the original C&A effort."

6. Personnel Security:

6.1. The goal of the personnel security program is to protect against unauthorized (accidental or intentional) disclosure, modification, destruction of computer systems or data, or the denial of service to process data.

6.1.1. To assist in achieving these goals, the UCM should ensure the following measures are complied with:

A copy of all DAA and UCM/CSM/CSSO appointment letters must be provided to the WIAO.

All personnel, military and civilian, using or expected to have access to Air Force computer resources have computer security training. Initial and recurring training will be accomplished and documented.

Only authorized personnel are allowed to use computer resources.

7. Physical Security:

7.1. Physical security is recognized as the first line of defense in the protection of these valuable assets. Physical security techniques are used to control access to computer facilities, terminal areas, processing equipment, storage media, and information. Strict adherence to AFI 31-101, Vol. 1 will be followed.

7.1.1. Additional physical security measures are as follow:

All systems, including AISs, drops, devices, servers, cabling, network server rooms, computer hub rooms, telephone wiring closets, and software shall be secured when unattended.

Computer systems shall be included on end of day or end of shift security checklists.

Fire extinguisher (Type C) must be located within the system area, preferably within 50 feet.

All systems should have plastic sheeting available to protect the system in event of water accumulation, leaks, or activation of sprinkler system.

All systems should be equipped with surge suppresser to protect them from damage caused by power surges. These may be internal or external devices.

Privately owned computer hardware in the government workplace is **NOT** authorized and may be confiscated.

A periodic cleaning schedule will be followed.

8. Software Security:

8.1. It is critical that AFI 33-114 and AFI 33-202 software security measures be followed. Copyright infringement is a criminal offense and will not be tolerated.

8.1.1. Additional Software Security Measures:

A listing will be maintained by the UCM of all government-owned software in use by their unit, and spot checks will be performed to ensure no unlisted/unauthorized software is installed.

All game programs, to include games that were installed when the AIS was purchased, will be removed. Computer game playing is reportable as Fraud, Waste, and Abuse.

9. Information Security:

9.1. Information security procedures will ensure that all applicable guidance contained in AFI 33-401 is followed. Electronic documents will be treated the same way you would treat a paper document of the same classification or sensitivity.

Each user will ensure their data files are protected from unauthorized viewing, theft, or loss.

Personnel turn in all media to supervisory personnel when relieved from duties in their work center (PCS, PCA, etc.).

Need-to-know for classified, Privacy Act and other SBU information must be enforced. AFMAN 33-323 gives details on record management for computers.

9.1.1. Removable media will be labeled with proper classification labels IAW AFI 33-202:

SF-706, Top Secret

SF-707, Secret

SF-708, Confidential

SF-710, Unclassified

Standard Form (SF) 711, Data Descriptor, will be used and enforced. Include the name, organization, and telephone number of the owner of the media, and a brief description of the contents. Disks containing Privacy Act Information must be identified as to the contents of the data stored on them.

10. Malicious Logic:

10.1. AFI 33-202 gives specific guidance on actions required to protect against malicious logic.

10.2. Antiviral software will be run at a minimum of once a week, updated at least monthly, and never removed from the AIS. Norton Antiviral software has been designated as the standard for the 437 AW and is fully supported by the WIAO. Other COTS packages may be used, but will not be supported.

10.2.1. When Norton Antiviral software is installed on an AIS, at a minimum, the following configuration options will be set:

Manual scans set to scan master boot records, boot records, and within compressed files. The "all files" option will be selected.

Auto-protect enabled and loaded at startup. Set options to scan "all files" when opened, copied, moved, created, or downloaded.

11. Password Protection:

11.1. Passwords are a major computer security deterrent. Follow all guidance provided in AFMAN 33-223. Passwords will be changed every 90 days and **must** contain the following:

Minimum of eight characters

Alpha characters

Numeric characters

Special characters

Mixed case (at least one lower and one upper case alpha character)

12. Monitoring:

12.1. All AISs will display the current Electronic Consent to Monitoring Banner message. See AFI 33-219, Appendix 2, paragraph A2.3.5., for the minimum content of this message. This warning will be displayed electronically anytime a user logs on. In addition, a label must be affixed and visible on the monitor frame with the message: "This device is subject to monitoring at all times. Use of this device constitutes consent to monitoring."

13. Computer Security Incident Reporting and Containment Procedures:

13.1. Computer security incidents include, but are not limited to, discovering information classified higher than the approved AIS processing level (i.e., Secret on an Unclassified system) or attempts to gain access by an unauthorized user.

- 13.1.1. A user finding higher classification than authorized (including E-Mail) on an AIS will:
Contact Network Control Center Help Desk, 437 CS/SCBNH, at extension 3-3511 and report the incident.
Follow Network Control Center Help Desk instructions.
Disconnect the system from the network if applicable.
Guard the system until security personnel can respond to the situation.
- 13.1.2. An AIS that has been, or is suspected to have been, accessed by an unauthorized user will be reported to Network Control Center Help Desk at extension 3-3511.

14. Internet Access

- 14.1. Access to the Internet is limited to official and authorized purposes only. Refer to AFI 33-129, Section 6, for specific information.
- 14.1.1. Users should be aware that it is possible for a malicious webmaster to insert a code that could cause damage to AIS file systems or allow unauthorized access to the network through the user's system. Users will be held accountable for any loss or damage due to casual web browsing.

15. Electronic Mail (e-mail)

- 15.1. Refer to AFI 33-119 for specific guidance.

16. Hardware and Software Maintenance

- 16.1. Your first line of assistance is to contact your work group manager/administrator (WGM/A). If the WGM cannot provide relief, the WGM will contact your functional administrator (FA). If further assistance is necessary, call the Network Control Center Help Desk at 3-3511.
- 16.1.1. If you are working on a classified or sensitive AIS, you will have to take further security steps prior to allowing other individuals access. You must contact the WIAO before seeking outside maintenance on classified/sensitive AISs.

DENNIS M. KAAAN, Colonel, USAF
Commander, 437th Support Group