

**BY ORDER OF
THE COMMANDANT**

**AIR FORCE INSTITUTE OF TECHNOLOGY
INSTRUCTION 33-104**

1 APRIL 2002

Communication and Information

AFIT COMPUTING SECURITY POLICY



COMPLIANCE WITH THIS PUBLICATION IS MANADATORY

NOTICE: This publication is available digitally on the Air Force Institute of Technology, Information Management Branch, web site at: http://sc.afit.edu/support/SCBI/afit_publications.htm. If you lack access, contact your Publications Management office.

OPR: AFIT/SCB (Captain Lacey)
Supersedes AFITI 33-104, 10 Feb 98

Certified by: AFIT/SC (Lt Col Robert F. Mills)
Pages: 7
Distribution: F

SUMMARY OF REVISIONS:

This document has been substantially revised and must be completely reviewed.

1. Applicability. The AFITNET supports the Air Force Institute of Technology's (AFIT) desire to meet the ever-changing and challenging scientific, engineering, and technical management needs of the United States Air Force and the Department of Defense through its graduate and continuing education programs. The computing infrastructure of AFIT is essential to the education and research mission. The purpose of this regulation is to aid the network users of AFIT in better understanding the responsibilities of operating in the network environment. While AFIT has a .EDU domain to allow for flexibility in mission responsibility, the AFIT network is still a government network, and failure to comply with the requirements of this network security policy will be justification to deny access to AFIT's computing resources and/or other action as deemed appropriate by the Designated Approval Authority (DAA). If access is denied, it shall remain in effect until compliance is restored and approved by the DAA. The Base DAA is the final authority for all decisions affecting WPAFB network connections.

2. Responsibilities. This instruction is applicable to all personnel operating networked or stand-alone small computers, word processors, memory typewriters, laptop computers, microcomputers, and intelligent terminals used to process sensitive unclassified and/or classified information. Persons subject to the Uniform Code of Military Justice (UCMJ) who violate the responsibilities of this instruction are punishable under Article 92, UCMJ. The Air Force may take disciplinary action against civilian employees who violate their responsibilities under this

instruction. Applicable state and federal laws govern contractors that use government-furnished equipment.

3. References

- 3.1. AFI 33-112, *Computer Systems Management*
- 3.2. AFI 33-114, *Software Management*
- 3.3. AFI 33-119, *Electronic Mail (E-mail) Management and Use*
- 3.4. AFI 33-129, *Transmission of Information via the Internet*
- 3.5. AFI 33-202, *Computer Security*

4. Desktop Policy.

4.1. Operating Systems, Applications, and Associated Hardware.

4.1.1. The AFIT Network (AFITNET) consists of network file/print/application servers using Microsoft Windows 2000, LINUX, Sun Solaris, SUN OS, SGI IRIX, and Network Appliance Data operating systems. Desktop computers/laptops use Windows 2000, SUN Solaris, SUN OS, Digital UNIX, or LINUX as their operating systems. On occasion, Apple Macintosh workstations may be included using MacOS. The AFITNET also includes various network printers and CD-ROM servers. The CD-ROM servers are not used for sensitive information. AFIT/SC has taken steps to ensure all the applications used are either properly licensed Commercial Off The Shelf (COTS) or software specifically developed for government use. The only exceptions would be free software applications and "plug-in" accessory type software from recognized sources. An example of such software would be system support tools provided by Microsoft at no cost.

4.2. Telnet and File Transfer Protocol (FTP).

4.2.1. Telnet and FTP will only be used to connect to other computers from *within* AFIT. Inbound Telnet and FTP are not allowed through the Firewall. Telnet and FTP should always be accomplished with either an anonymous logon or with a different user-ID and password in order to prevent the unencrypted information from being stolen by a hacker.

4.3. Secure Shell.

4.3.1. Secure Shell encrypts user-IDs and passwords and is required for remote access into the AFIT network and file transfers from remote locations. Use of Secure Shell is in lieu of FTP and Telnet.

4.4. Software.

4.4.1. No AFITNET user may use a software product for which they do not have a license. Games are not allowed on the AFITNET unless approved by the DAA for official use. Installing non-standard software on the AFITNET requires submission of an AFIT Form 10. Installing personal software requires submission of a Personal Software Request Form. Random software

scans will be accomplished periodically to ensure only authorized software is installed on the AFITNET.

4.5. Remote Access.

4.5.1. No modems will be attached to the AFITNET. If a laptop with a modem is used on the AFITNET, the modem must be either removed from the laptop or disabled.

4.5.2. Remote access to the AFITNET from the Internet is only allowed through the Virtual Private Network (VPN) or WebMail. Remote users shall maintain security policies, use their account for official use only, and shall not allow anyone else access to their user-ID and password.

4.5.3. Computer Customer Support will grant Wright-Patterson Remote Access Server (WPRAS) accounts as mission needs dictate. Valid AFITNET users will fill out a WPRAS Account Application and return completed application to Computer Customer Support for processing.

4.5.4. Private Internet accounts and other public access methods are allowed provided that WebMail or VPN are used to access AFIT resources.

4.5.5. Home users are highly encouraged to use a personal firewall whenever accessing AFIT and other Government computing resources.

4.6. Antivirus Protection.

4.6.1. SC administrators will automatically push antivirus updates and patches to desktops. All AFIT-owned laptop computers which are used for checkout will have a DoD approved antivirus program running on them at all times. The antivirus program will be updated and latest signatures will be installed prior to checkout. All servers, including mail servers and the E-mail gateway, will have current virus protection software running on them when active on the network. Virus signatures will be updated at least once a week, based on mission requirements and real-world threats.

4.7. Password Protection.

4.7.1. All AFIT computers will have a password-protected screensaver and will set a time of no more than 8 minutes to automatically activate. Users should always lock their computers when leaving the area.

4.7.2. All shared harddrives/folders/files on desktop computers must be password protected to prevent unauthorized access to sensitive information.

4.7.3. Users are responsible for their AFITNET accounts. Users may not allow anyone else access to a computer in which they are logged in and may not give anyone their password at any time.

5. Network Policy.

5.1. Sensitivity.

5.1.1. The AFITNET provides connectivity and a means of transferring information for all AFIT personnel. These systems contain personnel data, administrative data, proprietary information, and nonsensitive data. The AFITNET may contain sensitive but unclassified data. Classified data will NOT be stored or processed on this system. The AFITNET will utilize access rights provided by the network operating system in order to restrict access to network resources.

5.2. Web Servers.

5.2.1. AFIT/SC will maintain control of all web servers. Personal web servers are prohibited on AFITNET.

5.3. Proxy Servers.

5.3.1. Proxy servers will be used to control access to military NIPRNET and public internet, as well as protect the AFIT network. MIL access will not be allowed to unauthorized users, to include foreign nationals and contractors not having a National Agency Check (NAC). An EDU proxy server will provide access for all users to web sites not restricted to MIL only.

6. User Policy.

6.1. System Users

6.1.1. The AFITNET has a diverse set of users that include military and civilian personnel, contractors, and foreign nationals.

6.1.2. No classified information is present on the AFITNET; therefore, no clearances are required to access the system. All users with access to MIL networks are required to have a favorable National Agency Check (NAC) before accessing them. Users are granted access to data based on their roles within AFIT. System administrators are authorized access to all data on the system pertinent to their role.

6.1.3 AFITNET users will use “strong” passwords per AF regs to maintain the security of their accounts, protect personal and sensitive AFIT information, and to protect access to the AFITNET.

6.1.4 Suspected computer security related incidents will be reported to the Compusec Manager or CSSO/ Information Systems Security Officer. E-mail the AFITNET Computer Security team by sending E-mail to afit.csso@afit.edu

6.2. Security Awareness Training and Education (SATE).

6.2.1. All potential AFITNET users will complete SATE training with a passing score before being given an AFIT account. In addition to initial training, all users are required to take annual refresher training. Failure to successfully accomplish the required training will result in the denial of access to the AFIT network.

6.3. Unauthorized Use of the AFITNET.

6.3.1. The AFITNET will not be used for the following activities: personal financial gain, financial trading, online auctions, or live chat (unless used for official business). There will be no viewing of hate, racist, sexually harrasing, or sexually explicit web sites in any form of transmittal or storage.

7. Computer Security.

7.1. Compusec Manager.

7.1.1 The Compusec Manager is responsible for formulating AFIT Computing Security Policy. He/she is responsible for making recommendations on new security policies and any changes needed in current policies.

7.1.2 Implements a unit COMPUSEC program to ensure compliance with the provisions of AFI 33-202, including any MAJCOM or base supplements.

7.2 Information Systems Security Officer (ISSO).

7.2.1 Will verify that all hard drive software images created for the AFITNET are compliant with Time Compliance Network Orders and that other security policy requirements are met.

7.2.2 Is the single liaison between the unit and the wing IA office for COMPUSEC matters.

7.2.3 Ensures all users and IA personnel receive security training

7.2.4 Provides Certification and Accreditation (C&A) information to the base IA office for appropriate tracking, according to DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

7.2.5 Is responsible for completing AFITNET certification and accreditation.

7.2.6 Ensures organizations do not use shareware or public domain software until approved for use by the DAA. The ISSO ensures the software is free of viruses, hidden defects, and obvious copyright infringements.

7.2.7. Monitors information system activities to ensure system integrity.

7.2.8. Identifies threats, deficiencies, and associated countermeasures.

7.2.9. Reports system security incidents, vulnerabilities, and virus attacks according to AFSSI 5021 (will convert to AFMAN 33-225, Volume 2).

8. SC Administrators.

8.1. User Accounts.

8.1.1. SC administrators will restrict AFITNET user accounts to the appropriate access level for users to perform their assigned mission. SC administrators will perform random checks to ensure all AFITNET users' passwords contain at least one uppercase letter, one numeral, and one special character. Passwords must be between 8 and 14 characters in total length.

8.2. Virus Protection.

8.2.1. SC Administrators will ensure that all online servers are running the current virus protection. SC administrators will check for and apply new virus signatures to all servers, including the e-mail gateway, at least once a day.

9. Functional System Administrators (FSA) and Workgroup Managers (WM).

9.1. Responsibilities.

9.1.1. Each two-letter organization will assign FSAs and WMs. The assigned personnel will take the required certification tests and will work with the SC Administrators, SC Computer Customer Support, and Computer Security Team. The FSAs and WMs will act as points of contact between SC and the AFITNET users.

10. Communications Personnel.

10.1.1. Communications personnel will ensure that communication devices are protected from tampering and accidental damage. These devices will be located behind locked doors whenever possible. Communications personnel will ensure IP addresses and network connections are only given to approved personnel and equipment. IP addresses will be uniquely assigned to individual machines.

11. Computer Customer Support.

11.1. Responsibilities.

11.1.1. Customer Support will establish AFITNET accounts upon completion of an AFIT Form 35, Request for Computer Resources.

11.1.2. Customer support will authorize access to MIL web sites only upon proof of

citizenship or “green card” and if the individual possesses an adequate security clearance and the sponsoring official signs that the individual has the need to access MIL web sites. Customer support will NOT allow foreign nationals access to MIL sites. The foreign national’s account information will reflect this status, and accounts will be set up to access the appropriate and applicable proxy server or servers.

11.1.3. Customer support will create images of hard drives that meet AFIT’s security policy requirements, compliance with all applicable TCNOs, removal of games, software license compliance, and removal of all remote control and chat programs (unless authorized). This image will be used to propagate compliant images on similar computers. The CSSO must approve the image before it is placed in operation.

MICHAEL L. HEIL, Colonel, USAF
Commandant
Air Force Institute of Technology