

**BY ORDER OF THE COMMANDER
913TH AIRLIFT WING**

**913 AW INSTRUCTION 33-201
1 August 2000**

Communication and Information

NETWORK SYSTEM SECURITY PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: 913 CF/SCBN (Mr. Larry Antonio)

Certified by: 913 SPTG/CC
(Col Dana S. Marsh)

Pages: 25

Distribution: F; X; HQ AFRC/SCSI

This instruction implements Air Force Policy Directive 33-2. It establishes the Information Security Policy for the 913 AW Local Area Network (LAN). The Sensitive But Unclassified LAN is the Non-secured Internet Protocol Routing Network (NIPRNET). The classified LAN is the Secured Internet Protocol Routing Network (SIPRNET). This instruction establishes the minimum-security requirements needed to protect the sensitive unclassified and classified information on the networks. The Security requirements identified are intended to prevent or minimize the unauthorized modification, removal or destruction of the information processed and to control access to the information on a need-to-know basis. The objective of these security services is to ensure the confidentiality and integrity of data processed, handled, and stored by the system, as well as to ensure the availability of the system for mission accomplishment. It is the responsibility of commanders and supervisors at all levels to ensure compliance with this instruction. This instruction applies to all military members and civilian employees assigned to the 913th Airlift Wing, Willow Grove Air Reserve Station, Pennsylvania and the assigned Geographically Separated Units (GSUs). Violations of these provisions by civilian employees may result in adverse administrative action. Violations of these provisions by military personnel may result in prosecution under the Uniform Code of Military Justice (UCMJ).

Table of Content

| Title | Paragraph |
|---|--------------|
| Purpose | 1 |
| Applicability and Scope | 2.1 |
| Terms | 3 |
| Mission | 4 |
| Concept of Operations | 5 |
| Basic Facts | 6 |
| Security Policy | 7 |
| Operational Security | 7.2 |
| Access Control Policy | 7.3 |
| Configuration Management | 7.4 |
| System Security | 7.5 |
| Personnel Security Policy | 7.5.2 |
| Physical Security | 7.6 |
| Hardware Security | 7.7 |
| Security Testing | 7.8 |
| Software Security | 7.9 |
| Marking and Labeling | 7.10 |
| Maintenance Policy | 7.11 |
| Electronic Mail | 7.12 |
| Contingency Planning | 8 |
| COMSEC | 9 |
| Emission Security (EMSEC) | 10 |
| Designated Approval Authority..... | 11 |
| Certification and Accreditation of Networks | 12 |
| Certification and Accreditation Policy | 12.2 |
| Interim Accreditation | 12.2.3 |
| Certification Documentation Requirements | 12.2.4 |
| Reaccreditation Policy | 12.3 |
| Security Awareness, Education and Training | 13 |
| PC Security Policy | 14 |
| References | Attachment 1 |
| Acronyms | Attachment 2 |
| Glossary | Attachment 3 |
| Sample of WGARS FORM 3 | Attachment 4 |

1. Network System Management Procedures. This identifies the security requirements, and rules that regulate how information is stored, managed, protected, and distributed by the Willow Grove Air Reserve Station Network and Personal Computers (PCs) under the jurisdiction of the 913 Airlift Wing Commander who is the Designated Approval Authority (DAA) as delegated by the AFRC/CC.

1.1. While the ultimate responsibility for the Local Area Network (LAN) rest with the 913 AW/CC, the base LAN Administrator, in coordination with the Information Assurance office , is responsible for applying the most effective methods of protecting all information (data) transferred or stored on the LAN servers and the user's Personal Computer (PC).

1.1.1. Requirements for new hardware (PCs and/or peripheral components) or software (Operating Systems and Applications) is determined by the unit Automated Data Processing Equipment Monitor (ADPE), also known as the Unit Equipment Custodian (UEC). Once requirements have been determined at the unit level, the request is submitted to 913th Communication Flight, using AF Form 3215, "C4 SYSTEMS REQUIREMENTS DOCUMENT".

1.1.1.1. The 913 CF/SCB in coordination with the base LAN Administrator ensures that requested hardware or software meet the minimum requirements set by Department of Defense (DoD), Headquarters Air Force (AF) and Headquarters Air Force Reserve Command (AFRC). An accreditation package for all hardware and software, regardless of source, is submitted to the base Certifying Official (913 CF/SCB) before being placed into service. The Certifying Official evaluates the package and passes it on to the DAA for final approval. If the DAA determines the system fails to meet the stated security requirements, the system owner is responsible for ensuring the necessary changes occur to ensure DAA approval.

2. Applicability and Scope.

2.1. Procedures stated in this instruction are mandatory for all network servers, stand-alone systems and Personal Computers (PCs). The goal is to achieve the Air Force computer security objectives of availability, integrity, and confidentiality. This procedure implements AFRD 33-2, *C4 Systems Security*, and establishes guidance for all computer systems on Willow Grove Air Reserve Station, Pennsylvania.

3. Terms and Acronyms. Terms and acronyms used in this document are defined in AFI 33-270, *C4 Systems Security Glossary*, and Attachment 3 of this document.

4. Mission. The primary function of the 913AW LAN is to supply decentralized processing capability for the 913AW, its' tenants or assigned units. It provides a reliable Internet access through the network backbone to servers whether they exist locally on the Willow Grove Air Reserve Station, or at some other remote location. This includes all forms of data transmissions to include electronic mail (e-mail), file transfer, and electronic distributions of print products. The network assets must ensure the availability, integrity and confidentiality of information processed on the network.

5. Concept of Operations. The 913th Airlift Wing LAN is the collection of various components designed to transfer data to and from users. The network is capable of data transfer on a 24 hours a day, seven days a week operation with a ninety eight percent (98%) availability rate, including scheduled/unscheduled maintenance and/or repair. The infrastructure is under constant change due to new technology, which ensures users have fast and secure access to a host of resources. The network is designed to be robust and reliable to ensure minimal impact on the users' mission in the event of network fault.

6. Basic Facts. The procedure stated in this instruction applies to all hardware, software and equipment supporting or connected to the 913AW Network, and to everyone using, designing, maintaining, or administering the system. This document blends the security requirements in AFPD 33-2, C4 Systems Security, Air Force Systems Security Instructions and Manuals (AFSSI/AFSSMs) and DoD Directive 5200.28.

6.1. Classification of information. The highest classification for the SIPRNET is Secret. The highest classification of information processed on any PC connected to the NIPRNET will be Sensitive But Unclassified (SBU). Stand-alone PCs may process SBU or classified. However, any PC processing classified must be appropriately labeled and meet EMSEC requirements.

6.2. Assurance of information. All users will ensure appropriate safeguards are implemented to protect the confidentiality and integrity of the information as described in AFI 33-119, *Electronic Mail Management and Use*, and AFI 33-129, *Transmission of Information via the Internet*.

6.3. Minimum and maximum user clearances. DoD military, civilian, consultants, and contractor personnel using unclassified PCs must have, at a minimum, a National Agency Check/Entrance National Agency Check in accordance with DoD 5200.2-R, Personnel Security Program. Users processing classified must have a "need-to-know" and a clearance equal to or higher than the classification of the information they are processing

7. Security Policy.

7.1. The security policy for each of the categories described below is stated in accordance with security policy statements obtained from DoD documents, Air Force Instructions (AFIs), Air Force Systems Security Instructions (AFSSIs), and Air Force System Security Manuals (AFSSMs).

7.2. Operational Security.

7.2.1. The LAN Administrator establishes an audit record capable of tracing network activity to individual users.

7.2.2. Automated auditing techniques are employed on Willow Grove LANs. Audit trails and the events and information they contain are directed in AFSSI 5102. Audit reports are provided to the IA Office and/or the LAN Administrator for review.

7.2.3. Audit trail data are reviewed daily for any suspicion activities or security deviations. The audit records are reviewed weekly, at a minimum, for security trends (violations and alarms) and discrepancies. Discrepancies and violations noted during reviews must be acted upon immediately in coordination with the legal office. Close coordination with the Information Assurance office will be maintained until discrepancy is resolved.

7.2.4. Only authorized personnel (representatives of the IA Office, LAN Administrator, Security personnel or the Legal Office) are authorized direct access to the audit information. Audit information is protected in accordance with evidence assurance procedures, to preclude modification or destruction. Audit trail data is retained for a minimum period of 30 days for the purposes of analysis and investigation.

7.2.5. As a minimum, for each recorded event, the audit mechanism records:

7.2.5.1. Date and time of the event

7.2.5.2. Network identifiers (e.g., Internet address)

7.2.5.3. Type of event (e.g., logon attempt, telnet, ftp, etc.)

7.2.5.4. Success or failure (e.g., logon, program/file access)

7.2.5.5. Any attempt to change privileges or security profiles

7.2.5.6. Any actions taken or attempts to change configuration

7.2.5.7. Origin of request

7.2.5.8. Name of program/file introduced, accessed, modified, or deleted

7.2.5.9. User actions to create, modify, or delete programs and/or files

NOTE 1: Actions taken by network operators, administrators, and security personnel are annotated by some method such as a memorandum for record.

NOTE 2: Identification of each attempted or completed connection with a host, and its principal parameters (host/user identifiers) is part of the audit record. Network identifiers (e.g., IP address) may be used as identifiers of individual users, however, it must be possible to positively identify the individual(s) represented by the network identifier.

7.2.6. For Dial-in connection, a time out option of 30 minutes is installed to force users off the system in such a case as inactivity. Dial-in connections are only used for access to the local Willow Grove NIPRNET components. Dial-in connection is not normally used to provide any off-base connections, including Internet access.

7.2.7. The installed "Firewall" will not restrict Internet access both incoming and out going to authorized sites. The restrictions placed on the "Firewall" are at the discretion of the HQAFRC, LOCAL DAA, and/or AFCERT.

7.3. Access Control Policy.

7.3.1. Access to the Willow Grove Network is only authorized when individual users meet the criteria of AFI 33-204 para. 6.1. This is accomplished by the user submitting a properly completed 913AW Form 1, Request for Local Area Network and System Access. (See Attachment 4)

7.3.2. All PCs and Servers must have a warning banner to inform the user they are using a U. S. Government asset and they are responsible for proper use of it. Also the users are warned of consequences of misuse and must submit to monitoring. If the user is logging onto a LAN, once access has been achieved, via proper User ID and Password, a warning banner is again displayed to inform each user of their responsibility and consequences when using the Willow Grove LAN.

7.3.3. The length of a password adds improved security of the system. The selected password length provides a level of assurance commensurate to the value or sensitivity of the resources or data it protects. Passwords contain at least eight (8) alpha-numeric characters containing at least one (1) special character (characters above the numbers on the top row of the keyboard), as determined by the DAA or higher HQ. Passwords cannot be plain text, such as words found in a dictionary or encyclopedia. Also, they cannot be anything that may be associated with the user, i.e., name of user or family member or birthday.

7.3.4. Users generate their own passwords after the initial assignment by the Network Control Center (NCC). Mandatory passwords are installed on each Advanced Intrusion System (AIS) to include CMOS, Network and Screensaver. Administrative passwords have already been installed before AISs are released to each unit equipment manager.

7.3.5. Keep personal user-ids unique and assign them to only one person throughout the life cycle of the system. Passwords are set to expire every 90 days. The same password cannot be reused until at least 10 other passwords have been used.

7.3.6. Passwords are not shared or given to anyone except the authorized user to which initially assigned or a person who has been delegated, in writing, to act for the user. (i.e., Staff secretary) Sharing of passwords means all persons involved will be directly responsible and/or held liable for any loss, modification, or destruction of software or information belonging to the United States Government.

7.3.7. Passwords will not be programmed into functions keys, and will not be part of login scripts or batch files.

7.3.6. User IDs can only be changed by a member of the NCC. Locked out users can be reset by the NCC.

7.3.7. On PCs that process classified, User-IDs and passwords are classified at a level commensurate with the highest classification of the information to be accessed.

7.3.8. User privileges are limited to the least amount of power or privilege that enables the user to do his or her job.

7.4. Configuration Management.

7.4.1. Configuration changes and change notification is accomplished as deemed necessary by the LAN Administrator, AFRC or AF. In no case will a user add or update any program or application without written notice from the NCC. User PCs contain a standardized Operation System (OS), Windows 95 or NT and applications, such as MS Office or FormFlow.

7.4.2. Additional applications are at the direction of the LAN Administrator, AFRC or AF. Applications or programs directed by an organizations higher headquarters must be noted to the LAN Administrator. (This needs to be done in the event there is a conflict with existing programs). Administration or trouble shooting will be the responsibility of the headquarters that downward directed the application. If the higher headquarters remotely administers the application and a root login is required, they are not authorized to login directly using the root User ID/Password. They are to login as a lower privileged user, then switch to the higher-powered Administrative user.

7.5. System Security.

7.5.1. The primary elements used to protect the Base LAN (NIPRNET) will be the Air Force Internet Network Control Centers (AFINCC) router and the "Firewall" installed in support of the "Barrier Reef/CITS" programs. These systems offer a very high degree of assurance against intrusion from unauthorized sources. The SIPRNET network is protected by its' AFINCC router and the military encryption devices used to decode all data before entering the Internet system.

7.5.2. Personnel Security Policy. All users must have a security clearance equal to or higher than the highest category information contained on the PC the user has. Even if the user has the required security clearance, a higher priority is the "need-to-know". If the user does not have a "need-to-know", then the access will be denied.

7.5.3. DoD military, civilian, consultants, and contractor personnel using unclassified information systems must have, at a minimum, a National Agency Check/Entrance National Agency Check in accordance with DoD 5200.2-R, Personnel Security Program. Those personnel requiring access to classified systems are subject to the appropriate investigative scope.

7.6 Physical Security.

7.6.1 Where the hardware allows; some PCs/Servers are required to have a "CMOS" password. (This password is recorded with the users USERID/Password as mentioned in section 8.2.7). Each PC or Server must display to each user attempting access, a warning notice about unauthorized use of the PC/Server and a consent to monitoring statement. The warning banner is implemented on all system in accordance with AFI 33-219, *The Telecommunications Monitoring and Assessment Program*.

7.6.2. Resource assurance must be implemented in accordance with AFI 31-101, *Air Force Physical Security Program*.

7.6.3. The network control facilities which house key network devices (i.e., NCC) must be secured behind locked doors and/or monitored by authorized users to prevent unauthorized access. NCC personnel are responsible for the positive identification (e.g., personal recognition) of persons attempting to enter the facility

7.6.4. Network assets are installed in areas that afford maximum physical assurance or continuous observation

7.6.5. Persons leaving their workspace will logout before departing to prevent unauthorized entry. PCs are monitored during normal duty hours and secured in locked areas during non-duty hours. They will have screen savers that require a password entry before access can be obtained.

7.6.6. PCs/servers that do not require 24-hour operation, are turned off when not in use, or when the user leaves at the end of their work schedule. PCs/Servers that require 24-hour operation, the user will logout of the PC/Server before leaving.

7.7. Hardware Security.

7.7.1. Do not use PCs/Servers containing nonvolatile, non-removable storage media to process classified information unless one of the following conditions are met:

7.7.2. The PC is certified and accredited to process classified information.

7.7.3. HQ Air Force Communications Agency (AFCA) is the source for certification.

7.7.4. The PC is protected and stored according to AFI 31-101. The PC is in constant visual observation in a place certified for "open storage".

7.7.5. Provide the appropriate level of Emission Security (EMSEC) Assurance when using PCs and peripheral devices to process classified information or to coexist with PCs that do not process classified information (AFI 33-203).

7.7.6. No PC processing classified is connected to the Base NIPRNET without certified encryption devices between it and the network.

7.7.7. Security Testing. The objective of security testing is to uncover vulnerabilities, weaknesses, or flaws through which an unauthorized user (intruder) could access (gain entry to) the network. It also denies permissions to read, change, or delete data to which access is normally denied via discretionary access controls. This testing can only be done by a member of the NCC or IA section who has attended the appropriate Information Assurance schools and is certified to do the testing. AFCERT also has the authority to test our base. A piece of equipment is installed on our base that has the ability to monitor and log all traffic into and out of the base. This system can also be used to provide evidence of infractions of this Security Policy, which can be used in the process of disciplinary action related to the infraction.

7.9. Software Security. Software security ensures proper handling, dissemination, use, and storage of system software.

7.9.1. Use only software that was originally supplied with your PC, or provided by a Headquarters function. Software obtained by other means is not loaded to any PC or LAN Server without the approval of the LAN Administrator or the DAA.

7.9.2. Except for rare cases, all software is licensed for use on the PC where it is installed. Except for backup/working copies, **NO software will be copied, loaned or networked** (Use of back-up copies of Masters for re-installing damaged software instead of the Master copies will assist in not damaging costly or un-replaceable Software.)

7.9.3. Upgrading of existing software is not assumed to be automatically allowed. Unless written authority is provided by the NCC or LAN Administrator, upgrading is not allowed. This is particularly true in the case of WEB browsers. They are not designed to run under restricted governmental use.

7.9.4. Shareware is not free and is not to be used. This is HQ AFRC policy.

7.9.5. Protect applications and files from unauthorized access to provide program/file assurance from modification or deletion.

7.9.6. Personal, bulletin board, WEB software is not used without the written approval of the LAN Administrator.

7.9.7. Network/system software must complement and support hardware-based security features. Once implemented, computer-based security allows the system to abort or suspend unauthorized activity and record the incident in the audit log.

7.9.8. All software data/files are scanned for viruses, and malicious program (code) prior to being loaded to network or system(s).

7.9.9. It is mandatory that all PCs have an automated anti-virus program installed and functional.

7.9.10. It is suggested, at a minimum, that all users do some kind of back-up of their data files. (I.E. Word, Power Point, etc.). Where possible, the entire contents of their hard drive should be backed-up. All back-up copies are retained in a locked container, NCC backups must be retained in a locked container, in a separate facility.

7.10. Marking and Labeling. At a minimum, ALL removable media and output products that contain sensitive unclassified or classified information are marked as required by prescribing directives (AFI 37-131 for FOUO and AFI 37-132 for Privacy Act). Hardware that processes classified documents are labeled as to the highest class of classified that can be processed or produced. Securing and destruction of the hardware and products is done in accordance with their appropriate directives

7.11. Maintenance Policy. Maintenance of PCs and network components are restricted to authorized maintenance personnel with the appropriate clearances. Any maintenance on PCs must be done under the supervision of the NCC. Maintenance of the network fiber backbone is done by assigned HQ AFRC or higher command contractor.

7.12. Electronic Mail.

7.12.1. Most e-mail is downloaded to the user's PC. It is the user's responsibility to guard and backup their own e-mail.

7.12.2. Having military account e-mail forwarded, either manually or automatically, to private (civilian) e-mail accounts on commercial or educational networks is prohibited IAW AFI 33-129.

Sensitive information is not disseminated on the Willow Grove public folders.

8. Contingency Planning.

8.1. Contingency plans describe the actions necessary to ensure continuity of operations in the event of disaster, or to restore operations in the event of network failure. Plans should also include actions and procedures to protect data as a result of loss or interruption of commercial and environmental services (e.g., electrical power, air conditioning, commercial telephone services, etc).

8.2. All Systems within the NCC are connected to an Uninterrupted Power Supply (UPS) to preclude network interruption due to power surge or loss.

8.3. The NCC maintains adequate system backup tapes. A daily incremental backup and one complete weekly backup is created. Copies are kept one week for daily backups and one month for weekly backups. The dailies are stored on site in the NCC and the weeklies are stored in a secure location off-site.

8.4. If an emergency occurs after hours, the Command Post contacts 913CF/SCB, Chief Information Systems, who begins immediate notification of NCC personnel.

8.5. In the event of evacuation, all network servers within the NCC must be shut down and wrapped in a protective barrier to protect them from water and debris intrusion. Other functional servers are the responsibility of the organization. Primary HUBS (Tins) receive the same assurance as the NCC servers.

8.5.1. Priority for the servers are: NXXNT01, NXXNT02, NXXNT03, NXXCD02, FSZAWA01 + 03 AND NXXCD01. Priority for the ITN's ARE: Bldg. 202, Bldg. 201, Bldg. 235, and Bldg. 219. Every effort is made to disconnect and seal all fiber connections between the fiber boxes and the hubs in all Communication closets. Fiber connections are the weakest link of recovery. Fiber connections are stored in weatherproof containers and placed in a secured place.

8.6. Restoration priorities are NXXNT01, NXXNT02 ,NXXNT03, FSZAWA01, + 03, NXXCD02 and NXXCD01. ITN restoration is the same order as assurance. Recovered backup tapes are used to restore the servers, if required.

9. COMSEC.

9.1. Classified systems (PCs) are protected in accordance with AFSSI 4001, *Controlled Cryptographic Items (CCI)*, and AFSSI 3030, *Protected Distribution Systems*.

9.2. Declassification and destruction of hardware devices including clearing and sanitizing media (disk, tape and paper) is accomplished in accordance with AFSSI 5020.

10. Emission Security (EMSEC).

10.1. See AFI 33-203, *The Air Force Emission Security Program*, and AFSSM 7011, *The Air Force Emission Security Program*.

10.2. The Willow Grove EMSEC Program OPR is 913CF/SCBS.

11. DAA.

11.1. All PCs/Servers on Willow Grove must have DAA accreditation prior to placing the system into operation. The DAA has the overall responsibility for the secure operation of the Willow Grove Network (and systems connected to them), makes appropriate decisions to balance security requirements, mission, and resources against a defined threat.

11.2. DoD places the authority and responsibility of the DAA with the component commander. Within the Air Force, the Major Command (MAJCOM-AFRC) commander is the DAA. The DAA responsibility has been extended to the 913AW commander who is the final approval authority for Willow Grove Air Reserve Station.

11.3. DAA primary responsibilities are outlined in Air Force Security Systems Instruction (AFSSI) 5024. This person has the largest effect on the scope of work in the Certification and Accreditation program (C&A) of any PC/Server. The DAA ensures a security policy (this document), is developed and certification goals are clearly defined. He/she is the final authority on what is included in the C&A plan

11.4. To ease the burden of dealing with the day-to-day issues of accrediting, the DAA may appoint a representative to perform many of the duties; usually assigned the title of Certifying Official. The DAA representative should remain actively involved in certification activities and keep the DAA informed of major issues. **The DAA**, not the representative, decides the accreditation decision and signs the C&A. AFSSI 5024, Vol I & II is the guiding directive for Certification and Accreditation.

11.5. The System Security Authorization Agreement (certification package) must be submitted to the DAA for accreditation (approval to operate) of PCs/Servers and networks under the DAA's jurisdiction and control. The certification package must include a copy of the EMSEC Assessment or a memorandum stating the prescribed plan for corrective actions to be implemented to ensure compliance with EMSEC requirements. EMSEC accreditations must include the AFCOMSEC Form 7001, (Classified when filled in).

12. Certification and Accreditation of Networks and Personal Computers. A certification plan must be accomplished for all PCs operating on Willow Grove Air Reserve Station, whether connected to a LAN or as a stand-alone workstation. For systems managed by a different DAA that resides on Willow Grove Air Reserve Station, a Memorandum of Agreement (MOA) must be established between the applicable DAAs. As a minimum the MOA must include:

12.1. Classification range of data to be transmitted between systems

12.1.2. Clearance level(s) of users

12.1.3. Intended use of network

12.1.4. Countermeasures to be implemented prior to connection to the network

12.1.5. Statements of accreditation of the interconnecting system

12.1.6. Procedures for notification of changes in the system e.g., hardware, software, or configuration

12.1.7. Procedures for notification of proper parties in the event of security violations

12.1.8. Accreditation criteria

12.1.9. Rectification / reaccreditation requirements and responsibilities

12.1.10. Emission Security (EMSEC) Assessment letter.

12.2. Certification and Accreditation Policy.

12.2.1. AFPD 33-2 mandates that all Air Force PCs/Servers and networks be certified and accredited. This accreditation is valid for three (3) years. The certification process will be accomplished in accordance with AFSSI 5024, Vol I and II. AFSSI 5024, Vol. I, identifies variables that may necessitate reaccreditation sooner.

12.2.2. Willow Grove networks are certified and accredited as a whole. Any subnet not covered in the C&A of the network must be certified and accredited separately. The Certifying Official, designated by the DAA, will ensure that all certification tasks are completed. Upon completion the Certifying Official submits the appropriate recommendation (full, interim, or denial) in a formal recommendation letter to the DAA.

12.2.3. An Interim Accreditation (temporary approval to operate) should only be granted when mission criticality mandates the system be operational. Interim accreditation may be granted for no more than a one-year period.

12.2. Certification Documentation Requirements. Certification documentation must be completed in accordance with AFSSI 5024, Vol. I.

12.2.1. Metric reports for Security, Awareness, Training and Education (SATE), system accreditations, uncontrolled PC intrusions, and malicious logic incidents must be completed in accordance with AFI 33-205, *Information Assurance Metrics and Measurements Program*. The Wing IA Office forwards metric reports to HQ AFRC/SCMD no later than the first duty week of the new calendar year.

12.2.2. Certification documentation must include an EMSEC Assessment letter signed by the host base EMSEC manager. The EMSEC assessment must be accomplished as prescribed in AFI 33-203, and AFSSM 7011, *The Air Force Emission Security Program*.

12.3. Reaccreditation Policy.

12.3.1. Re-certification and re-accreditation is accomplished at a maximum of every three (3) years.

12.3.2. Re-certification and re-accreditation must be accomplished sooner should changes occur in configuration, software, hardware, operating parameters (i.e., new operating system, change in security environment, or change in classification of data processed), affecting overall security of the network.

13. Information Protection, Security Awareness, Training and Education (SATE) Program.

13.1. Ensure all personnel receive appropriate training in accordance with AFI 33-204, *The Information Protection, Security Awareness, Training and Education (SATE) program* annually.

13.2. Training consists of a series of Air Force Information Assurance Internet Based Training (AF-IAIBT) modules and comprehensive exams informing the user of his/her responsibilities and liabilities when using government owned computers assigned to Willow Grove Air Reserve Station.

13.3. Due to the requirement of obtaining a user account, password, and e-mail account prior to the accomplishment of this training, a temporary User ID and password will be issued for a period of 90 days for the sole purpose of allowing civilians/reservists to log onto the training website to accomplish their training. The PC will not be utilized for any other duties, until the required training has been completed. If after 60 days, this AF-IAIBT is not completed, the account and mailbox will be disabled and will only be enabled upon DAA approval.

13.4. The user will print and forward the completed AF-IABT certificate(s) to their unit SATE manager who is responsible for monitoring the training progress within the unit. On a monthly basis, the unit SATE manager will report non-completion of required training to the Network Control Center (NCC), 913CF/SCBN. IBT certificates will be issued upon successful completion of training which enables users to perform their job related duties, as well as, acknowledge that the individual is aware of their responsibilities and liabilities associated with using government computers assigned to Willow Grove Air Reserve Station.

13.5. The user must also complete and sign the 913th Wing Local Area Network (LAN) User Agreement (913AW Form 1) which is located on P: drive under 913 Forms folder. This test form is used as a checklist and kept on file in the NCC while assigned at Willow Grove.

14. PC Security Policy.

14.1. PC/Server must include as a minimum:

14.1.1. Labeling human-readable output

14.1.2. Mandatory access control

14.1.3. Device labels

14.1.4. Audit methods and procedures

14.2. The system security policy for each system is reviewed by the LAN Administrator, IA office and the Certifying Official prior to forwarding to the DAA for approval.

14.3. Local risk analysis is reviewed frequently to keep abreast of changes in vulnerabilities and risk associated with the system.

FREDDIE M. HEGLER, Colonel, USAFR
Commander

Attachment 1

A1. References

A1.1. Department of Defense Publications:

DoD 5200.28-M, ADP Security Manual (C31)

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (C31) (commonly referred to as the Orange Book)

DoD Directive 5200.28, Security Requirements for Automated Information Systems (AIS's)

DoD 5200.1R, Information Security Program Regulation

CSC-STD-002-85, Department of Defense Password Management Guideline

NCSC-TG-004, Version 1, Glossary of Computer Security Terms

A1.2. Air Force Publications.

AFPD 33-2, Information Assurance

AFI 31-101 Air Force Physical Security Program (formerly AFR 207-1)

AFI 31-401 Information Security Program Management (DoD 5200.1-R) (formerly AFR 205-1)

AFI 31-501 Personnel Security Program

AFI 31-209 Resource Assurance Program

AFI 33-112 Automated Data Processing Equipment (ADPE) Management

AFI 33-114 Software Management

AFI 33-115 Networks Management

AFI 33-119 Electronic Mail (E-Mail) Management and Use

AFI 33-129 Transmission of Information via the Internet

AFI 33-201 The Communications Security (COMSEC) Program (formerly AFSSI 4100)

AFI 33-202 Computer Security

AFI 33-203 The Air Force Emission Security Program (formerly AFSSI 7000)

AFI 33-204 Information Assurance Security Awareness, Training, and Education (SATE) Program

AFI 33-205 Information Assurance Metrics and Measurements Program

AFI 33-270 The C4 Systems Security Glossary

AFI 37-131 Freedom of Information Act Program

AFI 37-132 Air Force Privacy Act Program

A1.3. Air Force Systems Security Instructions (AFSSIs):

AFSSI 5001 Computer Security Policy Generation (Future AFMAN 33-222)

AFSSI 5002 Controlled Access Assurance (Future AFMAN 33-229)

AFSSI 5013 Identification & Authentication (Future AFMAN 33-223)

AFSSI 5024 Volume 1, The Certification and Accreditation (C&A) Process

AFSSI 5024 Volume 2, The Certifying Official's Handbook

AFSSI 5020 Remanence Security (Future AFMAN 33-224)

AFSSI 5021 Vulnerability and Incident Reporting (Future 33-225)

AFSSI 5101 Computer Security in the Air Force Acquisition Life Cycle (Future AFMAN 33-226)

AFSSI 5102 The Computer Security (COMPUSEC) Program (Future AFI 33-202)

A1.4. Air Force Systems Security Memorandum (AFSSMs):

AFSSM 5023 Viruses and Other Forms of Malicious Logic

AFSSM 7011 The Air Force Emission Security Program

A1.5. Other Publications and Documents:

Public Law 93-579, Privacy Act of 1974

Public Law 99-474, Computer Fraud and Abuse Act

Public Law 100-235, Computer Security Act of 1987

Public Law 104-294, National Information Infrastructure (NII) Assurance Act of 1996

Attachment 2**A2. Abbreviations and Acronyms and Definition**

| | |
|----------|---|
| ADP | Automatic Data Processing |
| ADPE | Automatic Data Processing Equipment |
| ADP EC | Automatic Data Processing Equipment Custodian |
| AFCERT | Air Force Computer Emergency Response Team |
| AFIWC | Air Force Information Warfare Center |
| AFRC | Air Force Reserve Command |
| AFNCC | Air Force Network Control Center |
| ASIM | Automated Security Intrusion Measurement |
| C4 | Command, Control, Communications and Computer |
| COMPUSEC | Computer Security |
| COMSEC | Communication Security |
| CSO | C4 Systems Officer |
| CSM | Computer Systems Manager |
| CSRD | C4 Systems Requirements Document |
| DAA | Designated Approval Authority |
| ECO | Equipment Control Officer |
| EMSEC | Emission Security |
| FW | Firewall |
| IA | Information Assurance |
| IS | Information System |
| IT | Information Technology |
| MAJCOM | Major Command |
| NIPRNET | Non-secured Internet Protocol Routing |
| NCC | Network Control Center |
| SA | System Administrator |
| SATE | Security Awareness, Training, and Education |
| SCMD | Information Assurance Branch |
| SIPRNET | Secured Internet Protocol Routing |
| SSAA | System Security Authorization Agreement |

Attachment 3

A3. Glossary

A3.1. Terms used in this document are defined in AFI 33-270, C4 Systems Security Glossary.

Accreditation - Formal declaration by a DAA (DAA) that a PC is approved to operate in a particular security mode using a prescribed set of safeguards.

Approval to Operate - Concurrence by the DAA that minimum security requirements are met and there is an acceptable level of risk. Accreditation authorizes the operation of a computer system or network at a specific site.

Assurance - Measure of confidence that the security features and architecture of a PC accurately mediate and enforce the security policy.

Authentication - A security measure designed to protect a communication system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.

Availability of Data - Data that is in the place, at the time, and in the form needed by the user.

Access - A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Accreditation - A formal declaration by the DAA that the PC is approved to operate in a particular security mode using a prescribed set of safeguards.

Information System (IS) - An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Commonly referred to as PS's or Servers.

Availability - Assurance of service applies to resources and to users. Resources must be available and reliable. Users must always be able to access that subset of resources to which they have been granted authorized access. Denial of service has a positive and negative aspect. Negative aspect is interruption of service with mission impact. Positive aspect is denying service to unauthorized users.

Certification - Comprehensive evaluation of the technical and non-technical security features of a PC and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Class C2, Controlled Access Assurance - Systems in this class enforce a more finely grained discretionary access control than C1 systems, making users accountable for their action through login procedures, auditing of security relevant events, and resource isolation.

Confidentiality - Assurance that information is not disclosed to unauthorized individuals, entities, or processes.

Configuration Control - Process of controlling modifications to PC hardware, firmware, software, and documentation to make sure the system is protected against improper modifications before, during, and after system implementation.

Connection - A network connection is any logical or physical path from one host to another that makes possible the transmission of information from one host to the other.

Contingency Plan's - Plan's maintained for emergency response, backup operations, and post-disaster recovery for a PC, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency.

Criticality - COMPUSEC characteristic that measures how important the correct and uninterrupted functioning of the PC is to national security, human life or safety, or the mission of the using organization.

Computer Security (COMPUSEC) - Measures and controls that protect computers against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of computers and data. Computer security includes consideration of all hardware and/or software functions.

Confidentiality - Protect classified data from unauthorized access by individuals that do not have the proper clearance and need-to-know. Protect sensitive, but unclassified data from individuals that do not have a need-to-know.

Data Integrity - Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Discretionary Access Control - Means of restricting access to objects based on the identity and need-to-know of users and, or groups to which the object belongs.

DoD Trusted Computer System Evaluation Criteria (TCSEC) - Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and

software security controls built into a PC. Note: This document, DoD 5200.28-STD, is frequently referred to as “The Orange Book”.

Firewall – A software package that restricts access to a network or the Internet by authorized users only.

Information System (IS) - Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

Integrity - System integrity is the ability to function unimpaired, free from deliberate / inadvertent unauthorized Manipulation. Data integrity is data that correctly represents information: authorized users and processors handle data properly.

Malicious Logic - Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose (Computer Virus, Trojan horse and Network Worm).

Network – A localized or wide area grouping of components, usually PC’s and Servers that are linked together to process or pass information between components or users.

Network Control Center – A centralized command and control function to administrator and regulate all network activities.

Network Security Policy - The set of laws, rules, and practices that regulate how an organization Manages, protects, and distributes sensitive unclassified information on and PC.

Network Worm - Use network connections to spread form system to system. They can behave as a computer virus; it could implant Trojan Horse programs or perform any number of disruptive or destructive actions.

Non-secured Internet Protocol Routing – A DISA provided unclassified entrance into the Internet.

Password - A protected/private character string used to authenticate an identity.

Penetration - The successful act of bypassing the security mechanisms of a system.

Permissions - Description of the type of authorized interactions a subject can have with an object. Examples include, read, write, execute, add, modify, and delete.

Personnel Security- Procedures established to ensure that all personnel who have access to sensitive unclassified information have the required authority, as well as appropriate clearances, and the need to know the information.

Public Domain Software - Software distributed without charge. Such software commonly does not have security Assurance features and is more susceptible to viruses.

Risk Management - Process concerned with the identification, measurement, control, and minimization of security risks in information systems.

Secured Internet Protocol Routing – A DISA provided classified entrance into the Internet.

Sensitive Unclassified Information - Any information that, as determined by competent authority (e.g., information owner) has relative sensitivity and requires mandatory Assurance because of statutory or regulatory restrictions (e.g., for Official Use Only, and Privacy Act Information) or requires a degree of discretionary assurance because the loss, misuse, unauthorized access to, or modification could adversely affect US national interest, the conduct of DoD programs or the privacy of DoD personnel.

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Note: Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235) (NSTISSI 4009)

Trojan Horse - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

User - Person or process accessing a PC either by direct connections or indirect connections.

Virus - A self-propagating program or file, composed of a mission component, a trigger component, and a self-propagating component. (See Malicious Logic)

Vulnerability - A weakness in system security procedures, system design, implementation, internal control, etc., that could be exploited to violate system security policy.

Attachment 4

A4- 913th Airlift Wing Local Area Network ((LAN) User Agreement

FC: 3320

| 913th AIRLIFT WING LOCAL AREA NETWORK (LAN) USER AGREEMENT | | | | |
|---|---------------------------------|------------------------------------|---|--------------------|
| I. IDENTIFICATION | | | | |
| NAME (Last, First, MI) | | GRADE/RANK | FUNCTION/POSITION | |
| SMITH, SUSAN A. | | TSgt | Information Management | |
| BASE/LOCATION | ORGANIZATION | OFFICE SYMBOL | PHONE (DSN) | PHONE (Comm) |
| Willow Grove ARS | 913 CF | SBCG | 991-XXXX | 443-XXXX |
| E-MAIL ADDRESS | | FAX (DSN) | FAX (Comm) | SECURITY CLEARANCE |
| | | | | SECRET |
| II. USERID | | | | |
| INDIVIDUAL <input checked="" type="checkbox"/> | ADD <input type="checkbox"/> | DELETE <input type="checkbox"/> | CHANGE ACCESS <input type="checkbox"/> | |
| JUSTIFICATION FOR ACCESS: | | | | |
| III. USER AGREEMENT | | | | |
| AS AN AUTHORIZED USER OF AIR FORCE INFORMATION ASSETS, I AM RESPONSIBLE FOR: | | | | INITIALS |
| 1. User ID and Password are For Official Use Only (FOUO) and will be protected as such. I will NOT compromise my User-ID and Password to other individuals or sources. I accept full responsibility for all actions taken within the system under my assigned User-ID. | | | | SSA |
| 2. I understand that "boot-up" and Windows screen saver passwords will be used on all systems and are not to be removed. | | | | |
| 3. I understand that all passwords that I create will be comprised of 8 characters in length and will be comprised of one each of the following: upper and lower case letters, numbers and/or special characters. Words found in any dictionary, in any language, will not be used. I further understand that the life cycle of network level passwords will not exceed 90 days. | | | | SSA |
| 4. I understand use for other than OFFICIAL US Government business including use of E-Mail and Internet access for non-approved/non-Government purpose is not allowed and is a violation of federal law unless specifically approved in writing by the Designated Approval Authority (DAA). | | | | SSA |
| 5. I understand that no games will be used on Government systems, this includes all Windows/DOS games supplied with those applications. I will remove any games found. | | | | SSA |
| 6. I understand that the initiation of, transmission of, or forwarding of such things as chain letters or other inappropriate broadcasts via E-Mail is prohibited IAW AFI 33-119, Electronic Mail (E-MAIL) Management and Use. I further understand that I will immediately report the receipt of these types of E-Mails to my Unit COMPUSEC Manager and/or system administrator. | | | | SSA |
| 7. I understand that I am not allowed to maintain adult material or visit sites that maintain and/or distribute adult material while using this account and DOD/Air Force-owned hardware and software. | | | | SSA |
| 8. I understand that storing, processing, or displaying offensive or obscene material, such as pornography, hate literature, etc., is prohibited. | | | | SSA |
| 9. I understand any illegal, fraudulent, or malicious activities are prohibited. These activities include but are not limited to: partisan political activity and political or religious lobbying or activities on behalf of organizations having no affiliation with the United States Air Force. | | | | SSA |
| 10. I understand that activities for the purpose of personal or commercial financial gain are prohibited. This includes but is not limited to: chain letters, solicitation of business or services, sales of personal property. | | | | SSA |
| 11. I understand I am not allowed to annoy or harass another person, e.g., by sending uninvited E-Mail of a personal nature or by using lewd or offensive language. | | | | SSA |

913AW FORM 1, APR 00 (Test Version Expires: APR 2001)

(Continued on Reverse)

| | | |
|---|-----------|--------|
| 12. I understand that storing or processing classified information on any system not explicitly approved for classified processing is prohibited. All systems that create or use Privacy Act Data must be marked on the outside of the system. | | SSA |
| 13. I will not allow or permit any unauthorized individuals to access a Government-owned system. This includes, but, is not limited to: allowing unauthorized individuals to add software/hardware or do any maintenance on a system. | | SSA |
| 14. I understand connecting to the WGARS LAN is subject to having all activities monitored and recorded without further notice. Any individual who uses this system expressly consents to such monitoring and is advised that if this monitoring reveals possible evidence of unauthorized or criminal activity, this evidence may be provided to federal law enforcement officials for possible punishment/prosecution. | | SSA |
| 15. I understand that no "Freeware" or "Shareware" software, including trial versions offered by vendors, will be installed on any Government-owned computer without written authorization and approval from the DAA. I further understand that all request to install "Freeware" or "Shareware" software, including trial versions, must be coordinated through the Commander, Information Systems Flight (913 CF/SCB) using an AF Form 3215, C4 Systems Requirements Documents. | | SSA |
| 16. I understand that I must have the most current DISA procured anti-virus software installed and running at all times. | | SSA |
| 17. I understand that all removable storage media will be labeled indicating at a minimum the classification of the media, the owner and phone number of the media, the contents, and a description of the media. | | SSA |
| IV. USER'S SIGNATURE | | |
| I fully understand and comply with the User Agreement. | | |
| NAME/GRADE/TITLE | SIGNATURE | DATE |
| SUSAN A SMITH, TSgt INFORMANTION | | 070900 |
| V. SUPERVISOR'S SIGNATURE | | |
| I verify the individual above requires access for the completion of his/her assigned official duties. | | |
| NAME/GRADE/TITLE | SIGNATURE | DATE |
| | | |
| VI. SECURITY MANAGER'S VERIFICATION | | |
| Individual's security clearance has been verified and National Disclosure Act (NDA) is on file. | | |
| NAME/GRADE/TITLE | SIGNATURE | DATE |
| | | |
| VII. SECURITY AWARENESS TRAINING AND EDUCATION (SATE) MONITOR'S VERIFICATION | | |
| I verify SATE training is completed. | | |
| NAME/GRADE/TITLE | SIGNATURE | DATE |
| | | |

