

23 JANUARY 2004



Communications and Information

927 ARW COMPUTER SECURITY POLICY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: 927 CF/SCBS (John Benzel)
Supersedes 927ARWI33-202,05 June 2003

Certified by: 927 CF/SCBN (Phillip D. May)
Pages: 33
Distribution: F

This instruction implements AFD 33-2, *Information Protection*. It establishes an operational system security policy for the 927 ARW Local Area Network (LAN) processing of unclassified and sensitive information and the processing of classified information (up to SECRET) on the Secret Internet Protocol Router Network (SIPRNET). It applies to all personnel in the 927th Air Refueling Wing utilizing computer assets.

SUMMARY OF REVISIONS

This revision deletes references to AFMAN 33-229 and AFSSI 5027. It changes the minimum time for a password change. It provides guidance for the frequency with which an Internet System Scan (ISS) is to be performed by the Network Control Center (NCC). It clarifies initial computer security training for network users. It establishes policy for the labeling of USB Portable Memory Devices. It deletes the term unit COMPUSEC Manager (UCM) and replaces it with Information System Security Officer (ISSO). A bar (|) indicates revision since the last edition.

1.	Roles and Responsibilities:	3
2.	System Information:	5
3.	System Security:	6
4.	Operational Services:	8
5.	Network Services:	23
6.	Marking and Labeling:	24
7.	Maintenance:	25
8.	Configuration Management:	26
9.	Declassification and Destruction:	27

10. Information Insecurity: 27

11. Communication Security (COMSEC): 28

12. Emission Security (EMSEC): 28

13. Incident Handling: 28

14. Certification and Accreditation (C&A): 29

15. Training and Awareness: 30

16. Specialized Security Training: 31

17. Documentation: 31

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 32

1. Roles and Responsibilities:

1.1. Designated Approval Authority (DAA). IAW AFI 33-202, *Computer Security*, the DAA for the LAN is the 927 ARW/CC. The DAA shall be responsible for reviewing the results of the risk analysis and certification documents presented by the certification official and determining whether the residual risk is sufficiently low to accredit the system/network for operational use. The DAA is responsible for the LAN infrastructure, including all workstations and network devices. The DAA ensures that the LAN meets Department of Defense (DoD), Air Force and HQ AFRC/SC security requirements. The DAA certifies that configuration and installed applications are in compliance with the network type accreditation and Certificates to Operate (CTO).

1.2. DAA Representative. The DAA representative is responsible for the day-to-day operations of the LAN. He/She should remain active in all Command, Control, Communications, and Computers (C4SP) process tasks and keep the DAA informed of major issues.

1.3. Certifying Official. The certifying official works on behalf of the DAA and develops the System-level Security Authorization Agreement (SSAA) or network system accreditation. The certification official shall provide the DAA with a recommendation for or against accreditation and operational limitations. The certification official shall document any security deficiencies in the SSAA submitted to the DAA.

1.4. Computer Systems Manager (CSM). The CSM is operationally and administratively responsible for the mission of the LAN. Normally, this is the senior communications officer of the network system. For the LAN, this is the 927 CF/CC. The CSM will plan and program budgetary, manpower, and training support for the operation and security of the system. The CSM will also develop administrative procedures (controls) to ensure the secure operation of the system.

1.5. Wing Information Assurance (IA) Office (WIAO). The Wing IA office personnel oversee the implementation of information assurance policy and guidance. They manage the 927 ARW Computer Security, Emissions Security, Telecommunications Monitoring and Assessment Program, Certification and Accreditation (C&A), and Information Awareness programs. They establish, review, and coordinate security requirements for the LAN. They also serve as the local expert and advisor to the DAA, DAA representative, CSM, certifying officials, Information System Security Officers (ISSOs), and others involved in the LAN system security policy formulation.

1.6. Information System Security Officer/Information Awareness (IA) Manager (ISSO). ISSOs administer the unit-level IA programs (COMPUSEC, EMSEC, TMAP, C&A, and IA). They serve as the liaison between the unit and the Wing IA office for COMPUSEC, EMSEC, TMAP, C&A, and IA related issues. The following are the specific responsibilities of the ISSO:

1.6.1. COMPUSEC. Establishes unit standardization and reporting controls as specified by the WIAO and implements a unit COMPUSEC program to ensure compliance with the provisions of this instruction, including any major command (MAJCOM) or base supplements. Additional duties can be found in AFI 33-202, *Computer Security*.

1.6.2. Emission Security (EMSEC). Ensures that all computers processing classified information comply with all EMSEC requirements IAW AFI 33-203, *Emission Security*.

1.6.3. Information Awareness (IA). Administers the unit's IA program IAW with AFI 33-204, *Information Assurance (IA) Awareness Program*, and accordingly must:

1.6.3.1. Ensure that network users receive IA training before granting access to the network.

1.6.3.2. Ensure that this requirement is added to the unit's in-processing checklist.

1.6.3.3. Maintain a hard copy record of IA completion for all users in the unit.

1.6.3.4. Forward via E-mail all IA customer education information sent by the Wing IA office.

1.6.4. Telecommunications Monitoring and Assessment Program (TMAP). This Ensures that all unit telecommunications systems comply with TMAP requirements IAW AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*.

1.7. Network Control Center (NCC). The LAN NCC provides responsive mission support by managing the local infrastructure that provides customers the communications and information resources needed to achieve their operational objectives. The LAN NCC serves as the single focal point for base network management and problem resolution. **(NOTE: For emergency situations during non-duty hours, contact the Command Post at ext. 4634. They will contact the appropriate NCC personnel).** The LAN NCC performs network and system administration to include security, fault, configuration, performance, and accounting management. They oversee network and system operations and manage the exchange of information.

1.7.1. Network Manager (NM). The Network Manager provides proactive and reactive network management by monitoring and controlling the network, available bandwidth, hardware, and distributed software resources. They terminate service and/or network connectivity of local systems, databases, and individual users that fail to maintain compliance with security directives, and this *Security Policy*. They respond to detected security incidents, network faults (errors), and user reported outages at the time of Helpdesk referral. They are responsible for all infrastructure devices on the network, to include switches and routers.

1.7.2. Network Security Manager (NSM). The Network Security Manager employs hardware and software tools to enhance the security of the LAN. NSM provides proactive security functions to assist users in deterring, detecting, isolating, containing, and recovering from information system and network security intrusions. The NSM installs, monitors, and is directly proactive and reactive with defensive measures to ensure the availability, integrity, confidentiality, and accountability of base networked information resources. He assists the Wing IA Office in developing local security policies, strategies, and plans to counter identified network security threats.

1.8. Functional System Administrator (FSA). FSAs are also commonly referred to as System Administrators (SAs). SAs ensure servers, workstations, peripherals, communication devices, and software are on-line and available to support customers. They install and configure software and hardware. They add, delete, or modify user accounts on their own functional network and maintain the network up to, but not including the first box in. They enforce password control, set permissions, perform security management functions, and coordinate maintenance call-out with the NCC. SAs must thoroughly understand the customer's mission, and be completely knowledgeable of the network capabilities/limitations and the network security policy. The SAs area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure components. The individual's unit or flight commander appoints SAs in writing and forwards the letter to the NCC.

1.9. Helpdesk Technician. Helpdesk technicians are assigned to the LAN NCC and troubleshoot the type of reported systems problems within defined response times, report the status of problem resolution to the affected customer, and maintain a historical database associated with problem resolution. They also use a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, and repair service support. Since they

work closely with users and workgroup managers, Helpdesk technicians must be familiar with the contents of this document for early detection of new vulnerabilities and incidents.

1.10. Subordinate Information Systems Security Officer (ISSO). The subordinate ISSO manages the COMPUSEC program for an information system. If a subordinate ISSO is not appointed within the unit, the ISSO assumes the duties of the subordinate ISSO. A complete list of duties can be found in AFI 33-202.

1.11. Work Group Manager (WM). WMs assist in directing the security program for terminal areas and remote terminals that are part of or access the LAN. Every WM will ensure established security procedures are followed; report security vulnerabilities, incidents, and problems to the ISSO; and ensure all users in their terminal area receive initial and recurring computer security training. WMs will also serve as the liaison on the following:

1.11.1. Between the NCC and the end users for technical assistance.

1.11.2. The ISSO and the end users on COMPUSEC, EMSEC, IA, and TMAP issues.

1.11.3. If possible, WMs duties and responsibilities should be assigned to a 3A AFSC.

1.12. Authorized Network User. Anyone who requires network access to conduct official Air Force business in the performance of their duties must have a completed National Agency Check (NAC) and have completed the required Information Awareness (see paragraph 16.) training. Additionally, they must be approved by their unit commander. All this information will be documented on the LAN access agreement. All users accessing the SIPRNET must have a minimum of a U.S. SECRET security clearance; waivers for exception to this policy will not be granted. All users shall comply with this *Computer Security Policy* and shall report security problems to their respective ISSO/WM. All users must complete a LAN access agreement prior to account creation.

2. System Information:

2.1. Security Mode of Operation.

2.1.1. Description. The LAN consists of an FastEthernet/GigE, multi/single mode fiber backbone that is interconnected via Switches and Hubs. The backbone is managed by the NCC and provides customers the information resources needed to achieve their operational objectives. Each building is provided 10baseT, FastEthernet, or GigE connection to the network. Through the use of network management systems, intrusion detection, and vulnerability assessment tools, the NCC performs network management and problem resolution for the backbone. Communications and information services entering and exiting the base or site fall under the operational control of the NCC. The NCC also provides MS Exchange & Defense Message System (DMS) E-mail, file, print, office automation, Internet access, and security services.

2.2. Accreditation Boundary. The accreditation boundary consists of all system components, resources, and connections on the proximal side of the Router. This includes all routers, network hubs, exchange servers, file servers, workstations, cabling, and all associated hardware (e.g. modems, and encryption devices).

2.2.1. Hardware that is temporarily installed on the LAN must be authorized by the DAA on a case-by-case basis. A separate accreditation or a letter of authorization will be required for temporary hardware installations.

2.2.2. The software boundary for this accreditation is defined to include the operating systems, common applications software, and utilities that remain installed on the LAN. Software and applications that are temporarily installed on LAN systems must be authorized by the DAA on a case-by-case basis. A separate accreditation or a letter of authorization will be required for these temporary software installations.

2.3. System Data Criticality. The LAN directly supports the U.S. Air Force war-fighting mission and should be considered like a "Weapon System." The LAN is a Group III (Mission Impaired) critical system. This means that loss of the system would have a direct effect on (but would not stop) direct mission support of wartime or contingency operations.

3. System Security:

3.1. Introduction. This system security policy is a hierarchy of the fundamental security objectives (computer, personnel, physical, communications, etc.) with supporting policy statements. The security objectives provide the framework for directing the design, implementation, and operation of system-related security services. The policy further refines the security objectives to state more specific rules for the LAN.

3.2. Security Requirements. The LAN shall ensure work can be accomplished in a timely manner with an acceptable degree of security assurance. The use of computer security technology shall not significantly detract from operational performance. Disabling required security functions is not an acceptable method to achieve operational performance. If the impact is assessed to be beyond acceptable limits, LAN users shall formally submit to the DAA those features they require disabled. The DAA shall be the approval authority for these requests.

3.2.1. Availability. The network and the information processed, stored, or transiting the system must be protected from loss or destruction and available whenever needed. The network will be available 24 hours a day 7 days a week, except during preventive or remedial maintenance.

3.2.2. Integrity. Integrity is concerned with ensuring that the data and information that we access is accurate and correct. There are two distinct aspects of integrity:

3.2.2.1. Data Integrity. The information itself must be accurate and complete. It must be plausible and users must trust the information as a true representation as it was entered, stored, or processed. Information has data integrity if there is assurance it has not been tampered with.

3.2.2.2. System Integrity. The network itself (hardware and software) must operate correctly and not corrupt the information within it. The integrity of the LAN shall be such as to prevent or deter any malicious action taken against the data, the software used to access the data, or the operating system environment.

3.2.3. Confidentiality. Confidentiality is preventing inadvertent disclosure of information. The information processed, stored, and transiting the LAN must have strict enforcement of confidentiality. The information will be at the sensitive and unclassified levels. Classified information must not be stored or processed on the LAN. Classified information above the U.S. SECRET level must not be stored or processed on the SIPRNET. No information can be made available to those without a valid need-to-know. Confidentiality will be supported by security services that are concerned with non-disclosure of information processed on the LAN. There shall be physical, administrative, and technical security measures, which can provide a sufficient measure of confidentiality.

3.2.4. Access Control.

3.2.4.1. A combination of physical, personnel, and system-enforced security mechanisms shall control access to the network. The Least Privilege Principle shall be implemented, which means that users will be given privileges, capabilities, and/or roles associated with their user-identifications (user-ids) that have the least amount of “power” or privilege that still enables them to do their jobs. As with functional users, explicit controls shall limit access capabilities associated with SA/WM, Database Administrator, or other Trusted Official privileged roles or functions.

3.2.4.2. The LAN will employ Discretionary Access Control (DAC), which provides the ability to control user’s access to information according to the authorization granted the user. It provides the data owner (individual or user group) a capability to specify permissions (read, write, delete, or execute) to information for each of their files and programs on the network. This implements the principle that a user should be given only those privileges or access that enables the individual to do his or her job. DAC guards against “need-to-know” violations. Files do not require an internal classification label unless they contain personal privacy act information. SAs/WMs and Helpdesk personnel will implement DAC by using the “rights and attributes” features of the operating system.

3.2.4.3. LAN system security features must include techniques that limit or otherwise restrict access to the system or its capabilities to specified users or user groups, including electronic interfaces to other systems. Specifically assigned user identification and password sequences shall be the basis to control access to the network, consistent with privileges and capabilities to be granted.

3.2.4.4. Administrative access to the LAN NT/Windows 2000 Domain and Exchange site will be limited to the NCC and authorized AFRC Network Operations and Security Center (NOSC) personnel that must have these rights to perform their official duties. NCC may authorize network access to network administrators with written approval of the DAA, DAA representative, and/or NCC Chief.

3.2.4.5. All users accessing the LAN shall be explicitly granted appropriate permissions and/or privileges according to their mission task requirements. All accesses, whether procedural and/or system-enforced, shall be adjudicated based on each person’s authorized “need-to-know” versus the requested data’s sensitivity level and its use restriction(s). Access approval for Foreign Nationals (FNs) will adhere to guidance as outlined in AFI 33-202.

3.2.5. Accountability. All security relevant actions on the LAN must be traceable to a single user who is accountable for those actions. Group accounts created on the LAN are prohibited. Accountability includes authentication and non-repudiation. It is the ability to validate, without a doubt, who is doing what on the LAN. The LAN shall create, maintain, and protect an audit trail of security relevant events. Access to audit information shall be limited to the ISSO/SA/WM and those authorized by the DAA. (Reference AFM 33-223, *Identification and Authentication*) for examples of additional security events to include as a minimum for auditing purposes.)

3.2.5.1. Authenticity. To the maximum extent possible, the LAN must ensure the originator of a file, message, or process can be proven and not “spoofed.” The use of audit trails, date-time stamps, and future digital signature technology assists in this goal.

3.2.5.2. Non-repudiation. The LAN will employ non-repudiation features. Non-repudiation is

undeniable proof of involvement (i.e., the recipient cannot deny receipt and the sender can prove delivery).

3.2.6. Security Management.

3.2.6.1. Security management is the development, implementation and maintenance of security policies, information, and information processing systems that support one or more security policies and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. Security management provides supporting services that contribute to the protection of information and resources in open systems in accordance with applicable information domain and information system security policies. Computer security is an integral system component that enhances the operational environment by allowing the system, rather than the individual user, to manage system security.

3.2.6.2. Access to the LAN backbone is based on the key concepts of “authorization” and “need-to-know.” Authorization is validated when a unit COMPUSEC manager notifies a SA or WM that an individual requires access to perform their official duties and that a personal account (logon ID) should be established. Notification may be by E-mail or letter contact. Need-to-know must be based on either an explicit written authorization or implicit authorization derived from the individual’s official duty assignment. Government contractors will not be given access to any information on the LAN unless first approved through proper channels. Foreign nationals employed by the U.S. government will be given access once all requirements specified in applicable security directives and this system security policy are met.

3.2.6.3. User Authorization Revalidation. LAN user authorization will be revalidated annually to ensure individuals who no longer require access are deleted from the database of authorized users. SA/WMs will revalidate user accounts under their control with the appropriate functional area manager and notify the NCC to remove any accounts that are no longer required. Validation will be conducted annually through the applicable ISSO

4. Operational Services:

4.1. Accountability

4.1.1. Events and Information to be audited. The following comprise audited events for the LAN and unit level servers:

4.1.1.1. Events audited shall include:

4.1.1.1.1. Successful and unsuccessful use of the authentication and non-repudiation mechanisms (login/logout).

4.1.1.1.2. Introduction of objects into a user’s allotted space.

4.1.1.1.3. Actions taken by the ISSO/SA/WM (e.g., adding a user, changing user rights).

4.1.1.1.4. System restarts.

4.1.1.1.5. Access or modification to audit logs.

4.1.1.1.6. Use of system commands which affect the audit mechanism (e.g., turn audit on or off).

4.1.1.1.7. Production of printed output.

4.1.1.2. System audit records shall include:

4.1.1.2.1. User identification.

4.1.1.2.2. Actions taken to create, modify, copy, execute, or delete programs, directives, or files.

4.1.1.2.3. Any event that attempts to change privileges or security profiles (e.g., change access controls, change security level of the subject, change user password).

4.1.1.2.4. Any event that attempts to violate the security policy of the LAN (e.g., too many attempts to log in, attempts to violate the access control limits of a file).

4.1.1.2.5. For each recorded event the audit trail shall record the date and time of event, the subject, the type of event, the success or failure of the event, the origin of the request, and the name of program/file introduced, accessed, or deleted).

4.1.1.2.6. Any actions to change the configuration of the network (e.g., a component leaving the network and rejoining).

4.1.1.3. Specific Audit Information:

4.1.1.3.1. Date and time of the event.

4.1.1.3.2. Unique identifier of the user or device generating the event.

4.1.1.3.3. Type of event.

4.1.1.3.4. Success or failure of the event.

4.1.1.3.5. Origin (terminal ID) of the request for identification and authentication events.

4.1.1.3.6. Name of the program or file introduced, addressed, or deleted.

4.1.1.3.7. Description of actions by the ISSO/SA/WM.

4.1.2. Automated or Manual Audit. Automated auditing techniques shall be applied. Security-relevant events that meet audit requirements shall be collected, processed, and stored by automated means. Analysis of collected audit data shall be performed using a combination of automated and manual techniques. Audited information shall not be required for real-time analysis.

4.1.3. Retention of Audit Records. Audit trails and other audit files and materials are retained for a minimum of 180 days after initial review. This includes both audit records generated by network servers and workstations. Disposal of audit files and materials shall be in accordance with the requirements of the highest classification of the information on the system. (Reference AFMAN 33-223, *Identification and Authentication* for more information).

4.1.4. Time-out Policy. Protect normal connections by a password protected screen saver when the workstation is left unattended. At the end of the duty day or shift, network users will log off of their systems.

4.1.5. Audit Review. The NCC will review LAN audit data daily. Local SA/WMs will review their audit logs each day. Discrepancies and violations noted during the review shall be acted upon immediately.

4.1.6. Protection of Audit Files. Access to audit information shall be limited. System segments shall protect audit files from unauthorized viewing, changes, or destruction. Protect audit files through file permissions. The ISSO/SA/WM will have read privileges to the audit file. Write and delete privileges to the audit file are restricted to the SA/WM. For all LAN NCC audit files, only the Chief or Superintendent of the NCC will be authorized to enable, disable, or direct configuration of the audit mechanism. Audit data files and products will be protected as sensitive but unclassified information, unless they disclose classified information, in which case they will be tracked at the level of information they disclose.

4.1.6.1. Permissible Audits. Permissible audits serve to minimize activities that degrade LAN performance or integrity in an unacceptable manner. They include detection and prevention of suspected LAN intrusion by non-authorized personnel. They also include prevention, detection, and maintenance of problems arising on the LAN during normal use by the LAN community. Law Enforcements audits are not permissible audits.

4.1.6.2. Law Enforcement Audits. A Law Enforcement Audit supports an investigative purpose where a violation of Air Force Instructions is suspected. A Permissible Audit becomes a Law Enforcement Audit at the time the auditor reasonably suspects one or more users have violated the Uniform Code of Military Justice (UCMJ). Do not conduct a law enforcement audit prior to obtaining a search authorization from the military magistrate. Consult the Legal Office for further guidance on law enforcement audits.

4.1.6.3. If a military computer is suspected to have been used to violate the UCMJ, immediately isolate the computer from the LAN and contact investigative authorities. Do not turn off the computer unless leaving it on would materially damage the computer, data stored on the computer, or the LAN.

4.1.7. Internet Security Scan. An Internet Security Scan (ISS) shall be performed at least quarterly by the NCC.

4.2. Password Management:

4.2.1. Password Composition. Passwords that allow access to the LAN must be at least eight (8) characters in length. Passwords shall include at least two alphabetic and one numeric or special character, be case-sensitive and shall not contain common names, foreign words, date of birth, or any information closely associated with the user. The NCC will initiate the use of Password Policy Enforcer (PPE) to ensure password composition. All passwords are checked against a dictionary consisting of approximately 3.5 million words at the time of password change.

4.2.2. Password Generation. Users shall generate their own personal passwords that conform to PPE restrictions. The system shall not allow a new password that duplicates the old password nor shall it allow the new password to be the same as or a variation of the USERID or the user's name. Variations are simple modifications to the USERID or user name such as reversing the order of characters or adding a one digit prefix or suffix. (OLDUSER becomes OLDUSER1, for example). Any standard system group or vendor-supplied default password shall be removed or changed at system installation time.

4.2.3. Password Displacement. The network logon shall be disabled or deleted within 3 workdays after the user leaves the organization or when the user no longer requires access for a period greater than 3 months. Users are required to notify the NCC to have their account locked during extended deployments. Passwords will be made invalid and destroyed by the system after they

have been inactive for a period of 7 months. Users are given seven months to cover the maximum TDY length, plus one month down-time afterwards. Additionally, passwords will be destroyed within one workday if a user's access is removed for reasons of pending or current punitive action or if the user's access is suspended. All displacement requests will be submitted via E-mail or memorandum by the ISSO/SA/WM.

4.2.4. Password Destruction. All default and initial passwords shall be removed / changed immediately from operating systems and applications. If they cannot be deleted, render them inactive.

4.2.5. Password Protection. The system shall protect password files so that an unauthorized user cannot access them. Users shall be responsible for actions attributed to the misuse of their password. Passwords shall not be stored in a human-readable form. Passwords shall not be written down or known by anyone other than the user. Only the SA/WM shall be afforded the responsibility to request password modification or deletion through the Helpdesk.

4.2.6. Changing Passwords. All passwords shall be changed every 90 days. The system shall prompt the user for a password change 14 (days) prior to expiration. The minimum time for a password change is 5 days. Simply stated, if a password is changed on a Monday, it cannot be changed again until Friday. A password history of the last 24 passwords will be set to ensure that users select a different password each time the password is changed.

4.2.7. NCC Requested Password Changes. SAs/WMs who have a letter on file at the NCC Helpdesk may request a password reset. As a last resort, if the SA/WM cannot be contacted, the user may come to the Helpdesk during normal duty hours to have their password reset. A valid form of identification is required when visiting the Helpdesk.

4.2.8. Password Lockouts. The system shall limit the number of consecutive incorrect access attempts by a USERID to no more than three (3) and shall automatically deactivate the USERID after the third unsuccessful log-on attempt. The system's action to deactivate a USERID shall affect only that USERID and shall not disable or otherwise affect the terminal or a different user who attempts to use the terminal. In recording the number of consecutive unsuccessful attempts for a specific USERID prior to reaching the lockout threshold, the system shall reset the number to zero (0) after a 24 hour period. For example, if a user has unsuccessfully tried to log-on two consecutive times, he or she can reset the counter by waiting 24 hours for their next log-on attempt or successfully logging on. SAs/WMs must not reinstate passwords without positive identification of the authorized user.

4.2.9. Password Classification. Passwords for the LAN will be protected by authorized users as "For Official Use Only (FOUO)." (Passwords for the SIPRNET will be protected and safeguarded as SECRET information). Although the password is FOUO, the obligation remains to protect the password so that only those with a need-to-know can access data.

4.2.10. Password Disclosure. Users shall not disclose their password to anyone and are responsible for actions attributed to the misuse of their password. Users must memorize their password. Do not place passwords on desks, walls, sides of terminals, or store them in a function key, login script, or the communications software. If documentation is necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a safe. If a user feels that his password has been disclosed to another individual, he shall change it immediately and notify their SA/WM or the ISSO.

4.2.11. Password Manager Requirements. The SA/WM or ISSO shall be the password manager and performs duties as outlined in AFMAN 33-223. Default passwords shall not be used and the password shall not be written down. Passwords changed by the password manager shall be invalidated at the first log-on after the change by the system so that the user is prompted for a new password immediately.

4.2.12. System Manager and User Privileges. At no time will SA/WM privileges be utilized to defeat security functions established within the LAN. Users with special permissions or privileges shall use them only for the requested or intended purpose. Those who abuse them shall have the permission or privilege removed by the SA/WM. Users shall only be reinstated upon determination by the ISSO. Only the SA/WM will be allowed to grant permissions or privileges upon written approval from the ISSO (if the ISSO is not the SA.)

4.2.13. Termination of Access to the Network. The ISSO/SA/WM will notify the Helpdesk within one duty day when an account requires deletion. All network accounts an individual has access to, will be terminated NLT the final out-processing appointment with the Military Personnel Flight (MPF) or civilian personnel. LAN management personnel will delete these user accounts when designated by the ISSO/SA/WM. The user ID accounts and passwords will be deleted from the system. ISSOs are also responsible for ensuring that procedures are in place to notify the SA/WM and the Helpdesk when an individual authorized access has expired.

4.2.14. Remote/Dial-up Access. The NCC will control and manage all dial-in access. Use of dial-in services must be logged and authenticated. The NCC will process all requests for dial-in access and brief users on the risks associated with dial-in access. The NCC will maintain a list of personnel having dial-in access. Dial-in software will disconnect sessions after 15 minutes of inactivity by the AFRC NOSC. The NCC will permit access only to those network services and data required by the remote users to perform mission essential tasks. Do not publicize modem telephone numbers to anyone other than those with a need-to-know and treat them as sensitive information. (Reference AFI 33-129, *Transmission of Information VIA the Internet*, for more information.)

4.2.15. Modems. Modems may not be purchased for servers without completion of a certification & accreditation package and approval of the DAA. Modems may not be purchased for computers and laptops without evaluation and approval of the NCC. Strict controls must be adhered to so that established security controls are not by-passed, which can result in a successful network intrusion by our adversaries. The AFRC NOSC provides a communications server cable for handling dial-in services.

4.2.16. Remote Login. Allow remote software diagnostics or maintenance only if the system audits such activities or if an appropriately cleared individual (capable of identifying unauthorized activity) observes such activities. The system being remotely maintained will authenticate the identity of the maintenance personnel. When maintenance activities are suspended or completed, disconnect or disable maintenance access to the system.

4.2.17. Workstation Screen Saver Passwords. To further prevent unauthorized access to workstations, all users must set a screensaver password on all workstations and servers. All screen savers activation timer will be set to no more than 10 minutes.

4.2.18. Running Crack on Passwords. The NCC will check password vulnerability by running an approved password-cracking program at least monthly.

4.3. Backup Copies of Original Network Software. SAs will make backup copies of all original network software that is installed as “standard” on all system file servers or “unique” software they maintain. Backup copies will be stored separately from the master copies whenever possible. Any duplication of commercially licensed software, except for backup purposes, is a violation of Federal copyright laws.

4.3.1. Server Backups. The NCC is responsible for ensuring validated backups are accomplished on LAN servers on a routine basis. SAs are accountable for ensuring all unit maintained servers have regular and reliable system backups of the data and the operating systems. Depending on a site’s hardware and software capabilities, on-line backups of Exchange and File Servers will be accomplished on a nightly basis. A full backup, which captures the data and operating system, will be accomplished on a weekly basis. Authorized outages will be scheduled by the SAs for all full off-line backups. The SA is responsible for validating that all backups are successfully accomplished within the prescribed time periods, and notifying the responsible commander when any anomaly exists. If a full off-line backup is postponed, due to mission requirements, the responsibility lies with the local SA to reschedule the backup as soon as the mission allows. At a minimum, there should be documentation showing who performed the backup; when it was performed; and how – performed and validated.

4.3.1.1. Storage of Server Backups. The NCC will utilize on-site and off-site storage. Tapes will not be overwritten for 30 days (limited by the software).

4.3.1.2. Archiving (Backup) of E-mail Systems. At a minimum, NCC personnel will make incremental and weekly full backups on all E-mail on the exchange servers. The backup copies retain the same classification as the original. Any copies made from equipment on the SIPR-NET must be protected as classified.

4.4. Policy on Exchange Server Accounts.

4.4.1. E-mail Account Storage Limitation. E-mail storage size will be limited to 50 megabytes. Special exceptions to this limitation up to 100 megabytes can be made for commanders, group accounts, and mission critical requirements. Individuals with the rank of O-6 and above are authorized 500 megabytes of E-mail storage. Waiver letters can be submitted and must be signed by unit commanders. When incoming E-mails of an account reaches the maximum size allowable, the NCC will deactivate the account. The ISSO will request reactivation. Personnel projected for TDY or deployment must coordinate with their SA/WM and the NCC prior to departure to avoid deactivation of account. All users will purge all files of a personal nature, i.e. saved E-mails and memorandums for record, prior to the computer being turned in for maintenance or PCS.

4.4.2. E-mail Message Size Limits. Single messages should not exceed 10 megabytes. Special exceptions to this limitation can be made for commanders, group accounts, and mission critical requirements with written approval of the CSM.

4.5. Permissible Internet and E-mail Actions. All government communication systems and equipment (including Government owned telephones, facsimile machines, E-mail, Internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only. Permissible uses are defined to include all uses not prohibited by law, regulation, instruction, command, or local policy. Internet and E-mail use must not adversely affect the performance of official duties, be of reasonable duration and frequency, serve a legitimate public interest,

create any additional expense to the Air Force, and not violate any security directives or this Computer Security Policy.

4.5.1. Authorized LAN users may use the government Internet and E-mail for:

4.5.1.1. Emergency communications and communications that are necessary in the interest of the Federal Government.

4.5.1.2. Morale and welfare, communications while deployed for extended periods away from home on official DoD business.

4.5.1.3. Brief communications while traveling on Government business to notify family members of official transportation or schedule changes.

4.5.1.4. Personal communications from the work center that are most reasonably made while at the work center (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief Internet searches; E-mailing directions to visiting relatives).

4.5.1.5. Educational work while pursuing collegiate degrees or self-improvement in the best interest of the DoD. Limited access is approved after duty hours when it does not conflict with organizational activities, and is coordinated with the commander.

4.5.1.6. Professional Military Education (i.e. Squadron Officer School, Senior NCO Academy), is approved after duty hours when it does not conflict with organizational activities. This does not include Weighted Airmen Promotion System (WAPS), which is not authorized.

4.5.2. Prohibited Internet and E-mail Actions. Use of Government information systems, including use of the E-mail and Internet, is subject to monitoring, interception, accessing and recording, and may be passed to Law Enforcement. Any violation of this policy can result in disciplinary or administrative action. The following list is NOT inclusive but provides guidance about prohibited E-mail and Internet actions. These actions are prohibited because they increase vulnerabilities or limit the network capability provided to the "war fighter". Abuse of network resources is categorized as intentional or unintentional (person did not understand consequences of their actions). NOTE: This list is not prioritized.

4.5.2.1. Creating/sending or "auto forwarding" official E-mails from a computer connected to the base network to a commercial Internet or Internet Service Provider (ISP) E-mail account.

4.5.2.2. Auto forwarding official E-mail messages to off base commercial accounts (non-DoD accounts) or another .mil E-mail address.

4.5.2.3. Forwarding unofficial E-mails to *.ALL extensions. This action usually results in a denial of service and limits the capability of personnel to accomplish the mission.

4.5.2.4. Sending E-mail to more than 249 addresses. Users who need to send to more than 249 addresses require NCC approval. Large E-mail distribution lists exist to facilitate the distribution of mission-related information. The NCC will determine which users on your base (Commanders, Directorate Chiefs, First Sergeants, etc.) have a mission requirement to send E-mail to the various distribution lists on the LAN. ".ALL" distribution lists will be restricted from general public use by configuring the distribution list to only those users with justified mission requirements.

- 4.5.2.5. Accessing or disseminating sensitive, For Official Use Only (FOUO), Freedom of Information Act (FOIA), or Privacy Act protected information in violation of established security and information release policies.
- 4.5.2.6. Accessing, storing, processing, displaying, distributing, transmitting, or viewing inappropriate material such as pornography, racist material, material promoting hate crimes, or material which may have adverse effect on good order and discipline.
- 4.5.2.7. Visiting, participating in, or downloading files from gaming, chat or hacker sites.
- 4.5.2.8. Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vender's patent, copyright, trade secret or license agreement.
- 4.5.2.9. Obtaining, installing, copying, posting, transferring or using software obtained through other than official means.
- 4.5.2.10. Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software code, to include viruses, logic bombs, worms and macro viruses.
- 4.5.2.11. Promoting partisan political activity.
- 4.5.2.12. Disseminating religious materials outside an established command religious program.
- 4.5.2.13. The use of commercial web-based E-mail (e.g. Hotmail, AOL, COMPUSERVE, YAHOO, etc ...) is not authorized for official correspondence. Deployed LAN users should utilize an approved government-controlled web E-mail service (e.g. Webmail or GI-MAIL, and Air Mobility Command (AMC) tool.).
- 4.5.2.14. Data streaming applications (e.g. RealPlayer audio/video, PointCast, etc.) will be used only for official business.
- 4.5.2.15. Accessing Internet data storage and/or transfer services for storage, backups, or to share data.
- 4.5.2.16. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission.
- 4.5.2.17. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.
- 4.5.2.18. Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.
- 4.5.2.19. Using someone else's identify (user id) and password.
- 4.5.2.20. Physical tampering of building communication closets or network equipment.
- 4.5.2.21. Installing and using a modem in a server, computer, or laptop that is also connected to the network.
- 4.5.2.22. Permitting any unauthorized individual access to the network.
- 4.5.2.23. Connecting or installing a non-approved system or software package to the network.
- 4.5.2.24. Any use of government-provided computer hardware or software for other than offi-

cial or authorized government use (i.e. morale use of E-mail where it does not impact work-center duties or network service).

4.5.2.25. Sending harassing, intimidating, abusive, or offensive material that violates AF standards of behavior.

4.5.2.26. Sending, receiving E-mail, or conducting an Internet transaction for commercial or personal financial gain (e.g. buying/trading stocks, advertising or soliciting services, sale of personal property.)

4.5.2.27. Gambling, wagering or placing of any bets.

4.5.2.28. Subscribing to mailing lists without commander approval.

4.5.2.29. Downloading freeware, shareware, or beta software programs without prior approval of the DAA, DAA representative or NCC Chief.

4.5.2.30. Excessive use of the data storage space on E-mail or file servers.

4.5.2.31. Violating remote access (dial-in) security procedures.

4.5.2.32. Writing, forwarding, or participating in further propagation of chain or hoax E-mails.

4.5.2.33. Posting personal home pages.

4.5.3. Suspension of Network Privileges. In the event a LAN user (identified by their user-id) is suspected of abusing network resources, the ISSO shall validate the user-id and provide support documentation to the Wing IA office. If a user is found more likely than not to have used computer or LAN equipment in violation of this Policy, Air Force Instructions, or the UCMJ, the user's access to the LAN will be suspended immediately. User rights will only be restored after the user's commander has requested and approved the reinstatement.

4.5.3.1. Furthermore, the NCC Chief is authorized to suspend network privileges and/or delete accounts as required to protect the performance and integrity of the LAN. Once a user's access is disabled, a letter/E-mail must be forwarded from the ISSO and coordinated by the unit commander outlining actions taken to prevent reoccurrence and stating that IA or applicable training has been re-accomplished. This letter/E-mail must be submitted to the Wing IA office to reestablish access.

4.5.3.2. Failure to comply with the above policies will result in the below listed sanctions. These are the minimum actions; the scope and maliciousness of the offense could result in more severe actions.

4.5.3.2.1. First Time Offender. The user's account should be locked for no less than 5 duty days.

4.5.3.2.2. Second Time Offender. The user's account should be locked for no less than 30 days.

4.5.3.2.3. Third Time Offender. The user's account should be locked/deleted for no less than 60 days. The DAA, in consultation with the unit commander, will determine if network access will be permanently revoked.

4.6. Software.

4.6.1. Malicious Software. Malicious software will not be installed on any LAN file server or workstation. Malicious software includes, but is not limited to, software that is specifically designed as packet analyzers for the purpose of capturing system passwords. The only exception to this policy is for Information Protection Operations personnel in the performance of their official duties.

4.6.2. Authorized Software. Only government approved software is authorized on the LAN. All other software, including games, music (MP3), pornographic, freeware, and shareware software, is unauthorized and will not be installed on LAN file servers or workstations.

4.6.2.1. Approval of Public Domain, Shareware, and Privately Owned Software. All such software will follow the certification process and have DAA approval prior to being installed on any workstation. To have the software certified and approved, the user will send a request (endorsed by the unit ISSO) with a detailed description of the software and the reason(s) for its use to the NCC, 927 CF/SCBN. User must state why the software must be used versus what is prescribed under the HQ AFRC Infrastructure Architecture. **Public domain/shareware software is not an acceptable substitute for Air Force purchased software.** Upon receipt of the request, the NCC, 927 CF/SCBN will test the software. If there are no problems, they will certify it and forward the request to the Wing DAA with a recommendation. The Wing DAA has final approval authority. Approved public domain/shareware will be added to the group, unit level, or staff section Automated Data Processing Equipment (ADPE) software inventory.

4.6.3. Use of Government Owned Software For Personal Reasons. The use of government owned software or hardware for personal projects (academic projects, professional military education (PME), Career Development Course (CDC), etc.) must be approved by a unit commander or designee. The use of commercial study materials developed for promotion testing, regardless of whether it is for Weighted Airman Promotion System (WAPS) or NONWAPS training is strictly prohibited.

4.6.4. Anti-Virus Software. ISSO/SA/WMs are responsible for ensuring networked servers, workstations, stand-alones and laptops are properly configured with the AF's approved anti-virus program(s). A continuous virus-scanning program is required on each system file server to check for known viruses.

4.6.4.1. Standard Anti-Virus Software (AVS). For the purpose of standardization, Norton AVS will be the standard for all workstations and servers on the LAN.

4.6.4.2. Norton AVS Signature File Auto Update. ISSOs are responsible for ensuring that all users are receiving their AVS signature file update via auto push method, except on areas where it is not technically possible. ISSOs will direct the responsible SA/WM to obtain the proper technical solution from the NCC. For areas where it is not possible to implement the auto update solution, the ISSO/SA/WM must contact the Wing IA office and obtain the AVS updates through other methods.

4.6.5. Scanning of Workstations. The user will run weekly virus detection to automatically scan user workstation local drives and random access memory locations for known viruses. Norton AVS software must be running in the background at all times.

4.6.6. Scanning Individual Workstation Storage Media. Users will perform a virus scan of floppy diskettes prior to initial use of diskettes on any workstation. This includes workstations remotely connected to the LAN.

4.7. Air Force Computer Emergency Response Team Advisories. The Network Security Manager, ISSOs, SAs, WMs, and Wing IA personnel must subscribe to the AFCERT Time Compliance Network Order (TCNO) and NOSC Notice to Airmen (NOTAM) distribution lists and implement patches as directed. AFCERT TCNOs and NOSC NOTAMs are sent from Wing IA throughout the month. UCMs are responsible for forwarding all AFCERT TCNOs and NOSC NOTAMs throughout the month to all SA/WMs within their unit. Compliance must be accomplished by the SA/WMs IAW the suspense date.

4.7.1. Compliance Reports. All ISSOs will report to the NCC upon AFCERT TCNO and/or NOSC NOTAM completion. The NCC will compile the information from the ISSOs and input this into the AFRC NOSC.

4.8. Hardware (Automatic Data Processing Equipment) Inventory. Organizational Equipment Custodians (ECs) will ensure that all LAN hardware assets (e.g., workstations, printers, personal digital assistants, etc.) under their span of control are listed in the ADPE Information Processing Management System (IPMS). NCC personnel will accomplish this task for their backbone assets. LAN users will only work on systems listed in IPMS. Any system without an IPMS label could be confiscated until the customer properly enters that system into IPMS.

4.9. Personally Owned Computers. Personal desktop or notebook computers owned by DoD members, government employees, or contractor personnel will not be used to process classified information. Personally owned computers (desktops or notebook) will not be physically connected to the LAN without DAA approval. The use of personal computers using an Air Force approved remote dial-in server can connect to the LAN for processing Sensitive but Unclassified (SBU) information.

4.10. Personal Digital Assistants (PDA). The interest in using PDAs/Handheld Terminals (HHTs) within the Air Force has increased significantly. This family of devices offers personal productivity enhancements, particularly by making certain features of your Microsoft Outlook portable, including contacts, notes, appointments, and E-mails. However, depending on the product and features, these devices introduce potential risks to our networks. A PDA is an automated information system (AIS) and therefore is subject to Air Force directives governing the security, connectivity, and use of a desktop or notebook computer.

4.10.1. *PDA Do's.*

4.10.1.1. Use to maintain schedules, contact information, notes, E-mail, and other items.

4.10.1.2. The user profile and password must be set and configured so the password must be entered when first powered on.

4.10.1.3. Use to take notes, save information, or write E-mails when away from your desktop workstation.

4.10.1.4. Synchronize information back into your desktop workstation using only direct-connect cables.

4.10.1.5. Must have an IPMS sticker, and consent to monitoring decal.

4.10.2. *PDA Don'ts.*

4.10.2.1. Do not process or maintain classified information. There are currently no approved methods for sanitizing/clearing classified from these devices. If contaminated, security personnel must protect, confiscate, and possibly destroy the affected PDA.

4.10.2.2. Do not connect to commercial Internet Service Provider (ISP). The use of commercial ISPs for official business is not allowed.

4.10.2.3. Do not synchronize the PDA across the LAN or remotely by direct dial-in access to desktops. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account.

4.10.2.4. Do not download or load Freeware or Shareware software enhancements for the PDA or for the desktop.

4.10.2.5. Afford the same physical protection as any laptop or device containing SBU and FOUO data.

4.10.2.6. PDAs purchased with unit funds must remain the property of the unit when the member departs and must be accounted for by the unit ADPE custodian. Use AF Form 1257 to document issue to members.

4.10.2.7. Do not use wireless (infrared capable) PDAs within controlled areas.

4.10.3. PDA Modem Use. The only authorized connection through a PDA modem is to an official Air Force RAS account protected by an authorized NCC firewall. Desktops will not be configured to permit dial-in access for the purpose of synchronizing the PDA remotely.

4.10.4. Personally Owned PDA. Users using personally owned PDAs on government owned computers will adhere to all the policies outlined in this system security policy regarding the use of PDAs and require DAA approval.

4.11. Digital Copiers / Printers. These devices are considered AISs with associated processors, memory, and hard-drives that subject them to network and computer security policy. At a minimum the following procedures apply:

4.11.1. An AF Form 3215, C4 Systems Requirements Document (CSRD), is required to purchase a Digital copier/printer.

4.11.2. Maintenance. Digital copiers/printers maintenance is limited to authorized maintainers with close supervision to prevent inadvertent disclosure of sensitive information. Any memory modules, disk drives, or other components with the ability to retain data that is removed from the machine must remain with the unit and be disposed of according to the highest classification.

4.11.3. Maintenance on devices that have been cleared for processing classified material, even once, must be performed only by a maintainer with a US Citizenship and security clearance to the appropriate level.

4.11.4. Devices connected to the network must be disconnected prior to maintenance.

4.11.5. Devices are not approved for networking and facsimile operation at the same time. It can be one or the other, but not both.

4.11.6. Devices must be included in a units OAR package.

4.12. Workstation Configuration Requirement. All workstations will be configured, standardized, and quality checked by the NCC. No user will install programs without approval from the NCC. All workstations added to the LAN must comply with the AFRC workstation standard naming convention. The ISSO/SA/WM is responsible for making sure each computer within their area of responsibility is configured properly.

4.13. Configuring a Workstation as a Web Server. LAN workstations will not be converted into Web Servers. Web Servers must follow the base and Air Force guidelines for web sites and web servers, and must be approved by the DAA and the base Public Affairs (PA) office. Workstations configured as Web Servers may create additional vulnerabilities to a user's personal data and the LAN.

4.14. Web Servers. Web servers connected to the LAN must follow the Air Force web server/site approval process prior to activating their unit web site. Contact the Wing IA office for details. All web sites must have unit commander, OPSEC, and PA (for public Internet sites only) approval before being released. Web servers must have an approved Certification and Accreditation (C&A). Web servers may only be hosted by the AFRC NOSC, not on the 927 ARW LAN.

4.15. Encryption. In the event that the DAA approves a technical solution that requires classified information (encrypted) to traverse over the unclassified network, use only National Security Agency Type I or II endorsed products, or National Institutes of Standards and Technology Federal Information Processing Standard 140-1 validated products.

4.16. Information Protection (IP) Tools. Use only AF/SC approved IP tools. These tools perform numerous security functions including boundary protection, viral detection, configuration inspection, network mapping, remote patching, vulnerability testing, etc. They are used to protect information systems and to measure the security posture of information systems.

4.16.1. Use. Because of the intrusiveness of some IP tools and the sensitivity of the information that may be observed during IP operations, only properly trained NCC personnel are authorized to use "intrusive" IP tools.

4.16.2. Intrusion Detection Agent (ITA). In order to provide the wing a real-time intrusion detection capability, the NCC and functional LAN servers will be configured with an ITA. This provides instantaneous feedback to the NCC of detected intrusion attempts and ensures proper actions can be initiated to combat the threat.

4.16.3. Training on IP Tools. The NCC personnel required to use IP tools will be trained on the use of the tools and the rules of engagement; either through Air Force approved courses, or through on-the-job training conducted by personnel who have received their training from Air Force approved courses. Personnel will utilize IP tools for continued monitoring of systems for health and security.

4.17. Personnel Security.

4.17.1. Security Clearances. Unit Security Managers (USMs),/SAs/WMs will comply with the personnel security program for the network. All persons accessing the LAN must, at minimum, have completed a National Agency Check (NAC, ENTNAC, or equivalent) verified through the JCAVS program, government orders, or a valid visit request. The USMs are responsible for verifying the user's clearance status. Access to the SIPRNET requires a minimum of a US SECRET security clearance. The SIPRNET administrator must validate an individual's clearance before a SIPRNET account is created. If, for any reason, a user's security clearance is removed, the user's access to the SIPRNET must be immediately terminated. SAs/WMs are responsible for reporting this type of action to the SIPRNET administrator so the account can be disabled. No foreign nationals are allowed access to the SIPRNET.

4.17.2. Need-to-Know. All users have clearance and access approval for all information within the system but not all users have a need-to-know all of the information within the network. The

ISSO will brief users on protection requirements for the various categories (e.g., Privacy Act, FOUO, proprietary) within the network. An individual's supervisor shall make the need-to-know determination and an access request will be submitted to the USM and forwarded to the ISSO or SA/WM.

4.17.3. Authorization for Categories. The LAN will operate in a System High Security mode.

4.18. Physical Security. Physical Security is used to prevent unauthorized access to equipment, facilities, materials, and information. It includes the application of physical barriers and control procedures as countermeasures against threats to LAN resources (hardware, software, network media) and information. The LAN shall be protected from natural threats (e.g., heat, weather); physical disasters (e.g., fire, building collapse), human threats (intentional and unintentional), and any other identified physical threats. Additional physical security mechanisms to prevent or limit damage shall be proposed, evaluated, and implemented where deemed feasible and cost effective.

4.18.1. Entry Controls to LAN Computer Facilities. Entry to the NCC resources shall be controlled. All SAs shall be responsible for positive identification (by personal recognition) of persons attempting to gain access to LAN assets. Personnel shall challenge any individual they cannot positively identify. If in doubt, they shall verify the status of the unknown individual. Status implies not only the appropriate clearance and need to access LAN resources, but that the individual is authorized to perform the function for which access is requested and the function constitutes official business.

4.18.2. Entry Controls to Remote Terminals. Only authorized personnel will be allowed access to user workstations. ISSOs/SAs/WMs shall ensure that these devices are secure from any unauthorized access and challenge any unknown individual attempting access. Unclassified workstation areas shall be monitored during duty hours and kept in locked areas during non-duty hours. Classified workstation areas shall be secured in accordance with (IAW) procedures defined for classified Controlled Areas. When the ISSO is unavailable, users must maintain security over classified workstations and controlled areas. Users are at all times responsible for maintaining area and workstation security until the ISSO can be notified of a problem affecting the security posture.

4.18.3. Resource Protection. LAN resources will be implemented to maintain a C2 level of operations. The first line of defense for protecting valuable assets is resource protection. The LAN is made up of high value items (both physically and logically), which are subject to pilferage. Physical resources are the network equipment, physical storage media, and the physical environment (site). Logical resources encompass data and software.

4.18.4. Physical Resource Protection. System assets shall be installed in areas that afford maximum physical protection or continuous observation. System installation plans must consider the potential for physical damage, information exposure, malicious tampering, and theft.

4.18.5. Logical Resource Protection. The LAN shall be protected from logical threats such as hacking, virus infections, and malicious attacks on resources perpetrated by authorized and unauthorized personnel.

4.18.6. NT Domains. The domain model used for the LAN is the Single Master domain model in which AFRC acts as the master domain and contains all user accounts as well as base resources such as the Exchange site. All other domains on base will be local resource domains that contain resource accounts specific to that unit such as unit file and print servers and computer workstation accounts. The only exceptions to this policy will be the AFRC NOSC with which a two-way trust

is maintained to facilitate their requirements to monitor all base domains and the AFRC FM which maintains a server within the NCC boundaries and also has a one-way trust relationship for financial transactions.

4.18.7. Policy for Protection of Support Systems. Support systems such as power distribution, air conditioning, and effective lighting shall be protected by physical and administrative mechanisms. Mechanisms employed for protection of support systems shall be documented in the System Security Architecture. Redundancy of support systems should be implemented when practical. A contingency plan shall address procedures for network system operations and recovery when services of a support system are lost. Surge protection or some form of electrical power conditioning shall be installed on all electrical power sources serving LAN resources.

4.18.7.1. Uninterrupted Power Supplies (UPS). All primary LAN resources should be installed with a UPS. Primary resources are those that are necessary for the network to continue operation such as servers and network equipment. This requirement should be applied to connected stand-alone systems or terminals, which do not impact the network's operation on an as needed basis, according to criticality, if the benefit is justified by the cost.

4.18.7.2. Fire Extinguishers. As a preventive measure, fire extinguishers shall be readily accessible in all areas where LAN resources are located.

4.19. Hardware/Software. The ISSO shall ensure hardware security controls are in place, documented, and implemented for LAN resources. The following requirements apply equally to firmware. The use of the term software in this policy shall include operating system and applications software, including database, spreadsheet, and word processing applications.

4.19.1. Volatility of Electronic Memory Components. The DAA shall be notified of all types of LAN hardware elements that contain nonvolatile storage in the risk analysis and/or certification documentation. DOD 8510.1M, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, states that removal of power is sufficient to sanitize classified information from volatile memory. Powering down the computer for 30 seconds can securely erase all volatile memory on the LAN.

4.19.2. Non-removable Magnetic Media. All non-volatile storage media (tapes, disks, battery powered RAM, etc.) used on LAN components will be controlled to insure personnel privacy act and FOUO information is not disclosed to unauthorized personnel. No storage media will be released to outside agencies (e.g. DRMO, other bases) until the media has been purged.

4.19.2.1. Local procedures shall be established for purging, storage, the handling of storage media during maintenance, and/or the destruction of such storage media. For the SIPRNET, AFI 31-401, *Information Security Program Management*, provides policy and guidance for the marking and storage of classified information/devices and requires compliance by all activities/users. The ISSO shall ensure that magnetic media, when not in use, is physically stored and protected commensurate with the sensitivity of the information contained therein.

4.19.3. System Architecture. The system architecture is defined in the applicable network backbone's System Security Architecture document. Using organizations may not at any time alter any of the system architecture of the LAN backbone without the knowledge and concurrence of the ISSO and DAA. The ISSO shall coordinate any requests for change to the proper authorities, at a minimum, the NCC, network architecture office.

4.19.4. Office Automation Workstation Operating System. All office automation workstations connected to the LAN must use Microsoft Windows NT, Windows 2000, or Windows XP operating system with the latest service pack authorized by the Wing IA office. This is due to the inadequate security features of the Windows 9x and older operating systems. Any waiver requests must have written DAA approval. HQ AFRC has directed that the wing migrate to the NT / Windows 2000 file system. No purchase of Novell products or enhancements are authorized.

4.19.5. DoD Goal Security Architecture (DGSA) Compliance. The LAN network communication pathways will comply with the DGSA.

4.19.6. Security Testing. All new software, including new shrink-wrapped products, will be verified as "virus free" using one or more (preferably more) virus checkers prior to initial use. Contamination discovered on new software shall be reported under AFSSI 5021, *Time Compliance Network Order (TCNO) Management & Vulnerability & Incident Reporting*.

4.19.6.1. A Security Test and Evaluation (ST&E) Plan shall establish testing procedures to ensure compliance with this system security policy and to guard against obvious ways for an unauthorized user to bypass or otherwise defeat the security measures of the system. This includes testing for obvious flaws that could allow the violation of resource isolation and that could permit unauthorized access to the audit or authentication data. Security testing shall become a part of the LAN life cycle.

5. Network Services: Network services will be configured and controlled IAW AFI 33-202. This section defines common infrastructure services and policies. For the purposes of this document, inbound is defined as coming from outside the base network boundary (i.e., from the Internet). Outbound is defined as originating within the base network and leaving the base network boundary (to the Internet).

5.1. Contingency Planning. The LAN is essential to the 927 operation. Continuity of operations plans or emergency action plans to enhance system survivability will be developed. These plans must be consistent and integrated with disaster recovery plans maintained by the base and organization. Test contingency plans periodically to ensure currency. AFMAN 10-401, Vol 1 *Operation Plan and Concept Plan Development and Implementation* provides further guidelines in contingency planning.

5.2. Contingency Plans. A contingency plan shall be developed to reduce the impact caused by unanticipated interruption of LAN operations. The contingency plan shall establish procedures to follow if a catastrophic event happens, how to reduce the impact from such events, and how to resume operations after the event. The plan shall address natural and system events. Such events or failures include: weather damage, heat damage, battle damage, terrorist damage, loss of all or part of the LAN capabilities, inoperative components, defective storage media, maintenance problems, disruption to LAN operations due to building evacuation, and complete or partial failure of LAN security measures.

5.2.1. Backup and Recovery.

5.2.1.1. At least weekly, a "save all" shall be backed up to tape and the tape shall be stored off-site in a secure location. Sufficient software, backup media, and instructions shall be developed and retained at an off-site storage location to fully recover daily and/or weekly backups.

5.2.1.2. Incremental system backups or "save" actions will be made daily. These backups may be retained on mass storage media for up to one week. The SA shall ensure that daily and weekly backups are made with a "save all" of the entire system made to tape at least weekly or

when new software is installed and configured. The SA or WM shall ensure sufficient software, backup media, and instructions are at an off-site storage location to fully recover daily and/or weekly backups.

5.2.1.3. At a minimum, NCC personnel will make daily incremental and weekly full backups of all E-mail on the exchange user and public folder servers.

5.2.1.4. A vendor or contracted maintainer of unique or proprietary operating systems shall be required to have and make available on demand software or procedures for system/data recovery, viral protection, detection, and eradication (if appropriate) and system clearing/purging.

5.2.2. Emergency Response. A roster of key personnel to be contacted during emergency operations shall be maintained and immediately available to LAN users and maintainers.

5.2.3. Exercising and Testing. The contingency plan shall be reviewed and selectively tested at least annually by the ISSO/SA/WM. Documented results shall be maintained with contingency plans.

5.2.4. User Data. Backup and restore of user maintained and developed data (i.e. E-mail (.pst), and data files, is the responsibility of the individual user. LAN NCC backups of the Exchange server are made only for disaster recovery of the entire server. Requests for restoration of E-mail accounts must be made via memorandum signed by the unit commander and state the impact to the mission if not restored. If the NCC inadvertently deleted an account, then all efforts will be made to restore the account and a memorandum will not be necessary.

6. Marking and Labeling:

6.1. All classified products and media shall be marked according to DOD 5200.1-R and AFI 31-401. Sensitive unclassified materials, which require special marking and handling, such as FOUO, FOIA (mandated by the Freedom of Information Act (FOIA)) and Privacy Act, shall be marked according to applicable regulations. Appropriate marking/labeling applies to printed listings, display terminals, monitors, CPU's, printers, diskettes/jackets, and storage devices. Appropriate, pre-printed, Air Force labels shall be used whenever possible for standardization.

6.2. Automated Marking. Automated page markings shall not be implemented at the system level. Users shall have the capability of turning on or off page marking via application formatting options. The user is responsible for ensuring all output products are properly marked and handled in accordance with established policy for manually marking output products. The ISSO shall ensure users receive continual training and reminders that they, not the computer system, are ultimately responsible for the accuracy of these markings.

6.3. Manual Marking. All users are ultimately responsible for ensuring that the output generated by all network systems, printers, and other devices are properly marked. Users will ensure that all output, and removable media is properly and adequately (i.e. conspicuously) marked IAW AFI 31-401, to prevent inadvertent disclosure of sensitive or classified information in situations where the system does not automatically perform such function.

6.4. Marking Storage Media. Storage media shall be marked at the highest level for which it was ever used. Air Force approved pressure sensitive labels shall be used. Floppy disks, tapes, and removable hard disks shall be labeled according to DOD 5200.1-R and AFI 31-401. Labels will be applied to all removable storage media (floppy diskettes, tapes, and hard drives). The labels will indicate the storage

media's owner, use, and description of contents. Standard Form 711, Data Description, or a commercial equivalent label will be used for this purpose. Additionally, removable magnetic storage media must contain the appropriate classification label (SF 707 for Secret, SF 708 for confidential, and SF 710 for unclassified). Disk packs shall be labeled on the casing in a conspicuous location. Compact disks (CDs) or other media that cannot be labeled directly shall be placed in a case marked with the appropriate label.

6.4.1. Universal Serial Bus (USB) Portable Memory Devices such as flash cards, memory sticks and thumbnail drives pose special difficulties because of their extremely small size. Because the usual classified labels are too large for most of these devices, the user must devise other methods for marking. Recommend using a tag or plastic tape or any other type of label, as long as the label is conspicuous, colorful and firmly attached to the device. Special caution should be exercised because these small devices may be easily overlooked in a physical security check of classified areas. **(NOTE: Because of the potential security problems associated with these very small devices which can hold large amounts of information, it is recommended that more traditional storage devices such as floppy diskettes and CDs be utilized).**

6.5. Marking Output Products. To preclude a compromise of personal privacy act data, users will review data after printing to insure personal privacy act output is marked appropriately. All output containing personal privacy act data would be marked with "Personal Privacy Act Information" if required. AF Form 3227, *Privacy Act Cover Sheet*, will be kept on hand and available for use with Privacy Act material in areas that routinely produce output containing privacy act data. Reference AFI 33-332, *Air Force Privacy Act Program*, for more information. All other output products such as Source Selection Sensitive Information or classified, will be marked / labeled IAW appropriate policy directives.

6.6. Internal Files Marking. Internal files shall be properly marked with the appropriate markings for FOUO or Personal Privacy Act Data within electronically stored documents if required.

6.7. Marking Peripheral Devices. Peripheral devices, such as external hard drives, that store sensitive information shall be marked with the designation of FOUO or Personal Privacy Act Data by using Air Force approved pressure sensitive labels. Manually generated labels may be used if Air Force approved pressure sensitive labels are not available. Devices connected to the SIPRNET will be appropriately marked and protected as classified.

7. Maintenance:

7.1. Maintenance on Hardware Devices. Only authorized maintenance personnel (i.e. LAN NCC personnel, ISSOs, SAs, WMs or government-approved vendors) will perform hardware maintenance on LAN resources. Initial troubleshooting, maintenance activities, and component replacement will be conducted by the ISSO/SA/WM. Individuals performing maintenance on network resources shall be cleared at the SECRET level. Security clearance must be validated prior to allowing maintenance of SIPRNET equipment. Maintainers in training shall be supervised by an appropriately cleared and trained maintainer. If releasing equipment for maintenance, equipment must be purged and all sensitive information removed unless the maintenance facility and personnel are cleared. Approved clearing procedures for unclassified equipment shall be performed before releasing the equipment for maintenance. The ISSO/SA/WM conducts, verifies, and documents sanitization of any media (hard drive or memory) that requires vendor/contract maintenance or replacement. The SA/WM or ISSO must establish procedures for handling diagnostic and maintenance equipment used on LAN segments

to preclude the compromise of sensitive information. Dial-up diagnostic and maintenance technology shall not be used on any network resource. Individual users will not perform hardware maintenance or modifications without approval of the NCC Chief.

7.2. Software Maintenance. All original copies of software shall be write-protected, inventoried, and kept in a secure location designated by the ISSO, SA, and/or WM.

7.2.1. A Software Maintenance Plan shall be developed and approved by the DAA to govern the development and maintenance of locally written software. The plan shall address such factors as: ensuring that a three-step development, test, and production sequence is adhered to; that development and test versions are not available for operational use; that production versions cannot be modified by any user; and that a thorough software design review and documentation process is implemented. Development and test programs shall not use "live" operational data, databases, or files. Software maintainers shall be cleared at a secret level.

7.2.2. The ISSO/SA/WM shall maintain DAA-approved software for wipe disk, fix sectors, data recovery, and viral protection, detection, and eradication. This software shall be available to all ISSO/SA/WM and authorized LAN users when requested. Personnel shall be trained in its use. In the case of unique or proprietary operating systems where such software is unavailable, the vendor or contracted maintainer shall be required to have and make available on demand software or procedures for system/data recovery, viral protection, detection, and eradication (if appropriate) and system clearing/purging.

7.2.3. Remote diagnostics must be restricted (i.e. length of remote session, authorized personnel) and approved by the DAA. The SA conducts software maintenance and installs vendor patches. Users must follow the guidelines for software security as dictated in AFI 33-112, and AFI 33-114. In addition, access to diagnostic programs and security-critical software shall be restricted to use by SAs/WMs, and NCC personnel. If Shareware or public domain software is required for mission accomplishment it must be authorized by the DAA on a case-by-case basis, in order to be placed on an operational system.

7.3. Software Patches and New Release. A software patch is a correction to a problem or "bug" within the software. A new release is a complete new application with a higher version number than the existing application. A new release may correct a "bug" or "bugs" and may contain additional functionality. All patches will be evaluated to assess the impact of applicable patches. Evaluated software patches, vendor patches, and new releases will be installed on their respective platforms in the following manner:

7.3.1. Server Software Patches and New Releases. The SA/WM is responsible for the proper installation, operational testing, and notification to the respective ISSO for all authorized software patches and new releases that he or she installs. The ISSO will notify the Wing IA office who in-turn reports to AFRC NOSC when upgrades have been completed.

7.3.2. Client Workstation Software Patches and New Releases. ISSOs are responsible for managing unit implementation of patches, new releases, and will notify the Wing IA office who in-turn reports to AFRC NOSC when upgrades have been completed.

8. Configuration Management: The NCC conducts configuration management for the local backbone to include the first box in. Significant changes (i.e., additional servers, new operating system) to the net-

work configuration must be coordinated with the NCC and the DAA, and subsequently documented in the system architecture section of the network's accreditation package.

8.1. The SA/WM or ISSO shall maintain documentation describing the software, hardware, firmware, and physical and logical connections of the LAN. All modifications to systems hardware, software, and firmware shall be coordinated between the ISSO/SA/WM, and the equipment management office. IPMS will be updated to reflect the modification if applicable. Configuration changes that affect the network's security mechanisms shall also be coordinated with and approved by the DAA.

9. Declassification and Destruction: SBU and classified data must be protected from unauthorized recovery of previously deleted data. This is accomplished by using either the Remanence security process of clearing or purging. By definition, clearing removes sensitive information from computer storage devices (hard disks and floppy disks) in a manner that renders that data unrecoverable by normal system utilities or non-technical means. Additionally, routines that only remove pointers and leave data intact are not acceptable methods of either clearing or purging of storage devices. There are three authorized methods of clearing magnetic computer storage media. The first data clearing method is to overwrite all locations with any single character. The Air Force APL identifies several commercial products (such as PC Tools and Norton Utilities) that are available to overwrite all locations on MS-DOS formatted magnetic storage media (e.g. local hard drives and floppy diskettes). The second data clearing method is to use a Type I degausser. The third method is to destroy the magnetic storage media. Either method two or three must be used whenever the use of method one is not possible, such as when a hard drive is not operational. In contrast to clearing, purging is defined as the removal of sensitive information from computer storage devices in a manner that gives assurance, proportional to the sensitivity of the data, that the information is unrecoverable by technical means. Purging is associated with classified data and will only be required when classified data is inadvertently entered into the LAN. Destruction will also be accomplished with approved devices in accordance with AFSSI 5020 for magnetic media and AFI 31-401 for paper. The user and/or ISSO is responsible to ensure these actions take place. Media and equipment will be purged of sensitive data prior to being transferred to non-DoD organizations (e.g. DRMO, schools, charitable institutions.)

10. Information Insecurity: When classified or higher than approved classified E-mail or documents are discovered on the LAN, Wing IA and the LAN NCC take immediate measures to identify and remove classified information from servers and individual workstations. Wing IA will direct all required actions and reporting. It is imperative that full cooperation be given by the affected organization(s) so classified information is not inadvertently forwarded throughout the local network, to another military base, or to personnel connected through a commercial network. In the event that an organization cannot be contacted or is not co-operative, the Network Manager takes action to remove classified information remotely from servers and workstations. If it cannot be accomplished remotely, disconnect the devices from the network.

10.1. Purging and Clearing of Storage Media. The determination of whether to purge or clear the media shall depend on the media's contents and destination. If media containing sensitive data is to be destroyed and released to uncleared personnel or environments, it shall be purged. Purging media shall be performed by degaussing (magnetically erasing) it or by overwriting every storage location at least three times with a binary 0, at least three times with a binary 1, and once with a random character. If media used on a classified system is to be used in an unclassified system it shall be purged. If media containing no higher than sensitive unclassified is to be released outside of government control, it shall be purged. Clearing media shall be performed by overwriting the media once with a binary 0 or

a binary 1. Clearing shall not be sufficient for declassifying media, releasing sensitive media to uncleared personnel, or placing it in an environment not suitable for protecting the media at its previous classification. Only products approved by the government for clearing and purging shall be used. AFSSI 5020, *Remanence Security*, shall be consulted for specific instructions dealing with purging and clearing. The procedures used to purge or clear media must be approved by the DAA and used only under the direct supervision of the ISSO/SA/WM.

10.2. **Declassification and Destruction of Hardware Devices.** Removing power for at least 60 seconds shall declassify hardware devices which are not capable of retaining data or which have volatile storage devices. Hardware devices that contain imbedded Programmable Read-only Memory (PROM) devices, Erasable Programmable Read-only Memory (EPROM) devices, or other types of non-volatile storage will be cleared or declassified by removing the memory or storage device. Destroy only the minimum necessary hardware to prevent a possible compromise of sensitive or classified information and recycle or reuse the remaining hardware.

10.3. **Declassification and Destruction of Storage Media.** The ISSO shall approve any media purge prior to purging the media. All sensitive, privacy act, and classification labels shall be removed from purged media prior to release. Media containing classified information will be destroyed by pulverizing, incinerating, disintegrating, or other physical destruction mechanism if purging is not available. (NOTE: Storage media containing classified may also be sent to NSA for destruction. Contact the Wing IA office for further information).

10.4. **Declassification and Destruction of Output Products.** If classified or sensitive output is produced, it shall be declassified or destroyed by pulverizing, incinerating, disintegrating, or other physical destruction mechanism. Use a DAA approved method under the ISSO's supervision.

11. Communication Security (COMSEC): Transmission of certain sensitive data and classified information requires using secured communications systems (SIPRNET, for example), registered mail, secure telephone and facsimile equipment, manual crypto systems, call signs, or authentication. These rules can be found in AFI 33-201, *Communications Security (COMSEC)*.

12. Emission Security (EMSEC): All SIPRNET connections must prevent the compromise of classified information due to the leakage of electromagnetic radiation. The SIPRNET components must provide appropriate shielding and/or an appropriate control zone. The Wing EMSEC manager (WIAO office) must be contacted during the planning and installation of any peripheral devices, such as workstations, printers, file servers, etc that process classified information. AFMAN 33-214, V2, *Emission Security Countermeasures Reviews*, provides guidance and information for EMSEC protection measures.

12.1. Cellular phones, two-way radios, two-way beepers and any other electronic equipment that can receive and transmit a signal are prohibited in all staff offices or areas where classified information may be processed.

13. Incident Handling: Suspected security incidents will be processed IAW the following procedures AFSSI 5021. The first person to contact in the event of an incident is your ISSO or SA/WM.

13.1. **Response.** Upon determination by the user or ISSO that the LAN may have been compromised, the ISSO or SA shall physically disconnect all external communications access with the LAN. All users shall immediately upon notification terminate all access to the LAN. The ISSO will notify the Wing IA and prepares all the necessary reports. LAN users will immediately report vulnerabilities,

security incidents, or unauthorized entry of the computer system to their ISSO/SA/WM, and WIAO. NOTE: During non-duty hours, the 927 Command Post will be notified. The CP shall in-turn contact the NCC Chief. SA/WMs will perform an initial evaluation of each security problem or incident, document the circumstances, begin corrective or protective measures, and accomplish follow-on reporting as required. In the case of an in-progress intrusion or suspicious activity, the SA/WM will immediately contact the NCC Chief who will immediately contact the AFCERT. Suspicious activities include browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics without the owner's knowledge.

13.2. Reporting. Proper reporting of newly discovered vulnerabilities and incidents ensures containment of impact, recovery of network availability, identification of breach and perpetrator, and countermeasure implementation. ISSOs train users on vulnerability and incident reporting procedures. ISSO/SA/WMs, and the Network Manager must comply with the reporting procedures found in AFSSI 5021.

13.3. System Sanitization. Sanitize the system and components according to AFSSI 5020.

14. Certification and Accreditation (C&A): IAW *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)* all systems connected to the LAN will be certified and accredited prior to operation. The accreditation will be updated to reflect physical, logical, configuration, and procedural changes to the network.

14.1. DAA Accreditation Requirements. The LAN must be accredited IAW AFD 33-2. Accreditation is the formal written declaration by the DAA that a particular system is approved to operate in a given mode, against stated residual risks, and with stated countermeasures. The DAA formally accepts responsibility for the operation of the system and personal liability and accountability. Use DITSCAP and AFI 33-202 to complete an accreditation package.

14.2. Systems Certification. Each unit will perform certification on the systems they own and operate. HQ AFCA/SC is the single accreditation authority for all DoD, AF and AFRC command and control, business, common-user, and intelligence applications on the LAN. Certification of all applications on the LAN will utilize the CTO process, the single authorization and direction for wings and units to certify and accredit applications. There is no further requirement for the wing or units to certify and accredit applications.

14.2.1. Once certified, the AFRC NOSC, program management office (PMO), and other agencies will coordinate application installation through Wing IA.

14.2.2. If a security risk or other problem concerning an application that is not identified in the CTO package is discovered, the DAA or DAA representative will immediately notify the MAJ-COM DAA representative. Additionally, notify the AFRC NOSC of immediate security or operational impact.

14.3. Systems Accreditation. Accreditation is the DAAs approval to operate a system. A system cannot be approved to operate by anyone other than the DAA who is delegated as the responsible party for the system.

14.4. Accreditation Documentation. Documentation will consist of a completed System Security Authorization Agreement (SSAA) and meet all requirements found in the DITSCAP. The NCC maintains its approved accreditation package and provides a copy to the Wing IA office. Functional LANs'

approved accreditation packages will be maintained by their ISSO and the SSAA will stay with the identified system. The Wing IA office maintains the original copy of the functional LAN accreditation packages. The receiving organization is responsible for completing the required C&A package 40 days prior to an installation or contractor team's arrival. Organizations will submit the C&A package to the Wing IA office and comply with this Computer Security Policy to ensure the security of the entire network. The NCC is not authorized to connect any system to the network without being provided an accreditation number from Wing IA and approval of the DAA.

14.5. Reaccreditation. Reaccredit systems every three years or upon significant changes to hardware, software, or environment. The SSAA is a living document where changes and updates are constantly occurring. An accreditation package is not to be left in a file and completely re-accomplished every three years. Most changes to the system will only require an update of a page within the SSAA. Should a major change occur, the bulk of the agreement is reusable in a reaccreditation.

15. Training and Awareness: Training shall promote the proper and consistent application of security features and procedures to provide adequate protection for information. Personnel shall be trained on procedures to report incidents and vulnerabilities under AFSSI 5021. Personnel with administrative access to the network shall receive intensive training on the correct implementation of information security practices. All personnel shall receive training on the proper response to compromise or possible compromise of system data or secured operations.

15.1. Network (LAN) users must obtain a network user license prior to receiving full network privileges. The training required to obtain a network user license is standardized in the "Network User Licensing" Computer-Based Training (CBT) course. The user shall provide documentation for having successfully completed the course to their ISSO and the NCC. The ISSO shall maintain the training documentation. Specialized training shall be provided for key network personnel. At least two key system/network individuals shall attend each specialized training session.

15.2. LAN users will be provided information awareness training IAW AFI 33-204, *Information Assurance (IA) Awareness Program*. User-level training will include all network security related features from a client perspective. The SA/WM will provide training to new users, prior to them being granted access. As a minimum, training shall consist of:

15.2.1. Common LAN and local threats and vulnerabilities within the unit, and how they may impact the LAN operation.

15.2.2. LAN system security policies and procedures for protection of the areas in which the LAN components are located, protective measures against viruses, worms, etc. Backup of data files, protection of magnetic storage media containing sensitive unclassified data, classified data (as appropriate), and reporting security violations, COMPUSEC incidents, and system vulnerabilities.

15.2.3. The user's role in maintaining LAN system security policy.

15.2.4. The basic concept of risk management and the importance and effectiveness of the controls established for the LAN.

15.2.5. The established administrative procedures for the protection of sensitive data. This includes designation of sensitive data, classified data, marking, reproduction, transmission, destruction and disclosure of sensitive (or classified) data; accountability for sensitive (or classified) data; reporting computer abuse and proper housekeeping procedures.

15.2.6. The established procedures for physical security measures employed to protect LAN components and information at their appropriate levels includes: access, control, fire prevention and, protection measures.

16. Specialized Security Training: All ISSOs, SAs, and WMs will receive initial training that covers, as a minimum, the requirements addressed in this system security policy. The availability of specialized training is constantly changing. The ISSO will document all specialized training by name, assigned position, training subject, and date received. In addition, all network professionals (ISSO/SA/WMs) must complete the required IA CBT course provided by AFCA or equivalent approved training. IAW 33-115, Volume 1, all SA/WMs will be trained by the NCC prior to being given privileges/rights to perform their assigned duties and responsibilities. Any previous training received must be supported with documentation and provided to the NCC.

17. Documentation: Documentation required by this system security policy shall be reviewed and updated by Wing IA at least annually. The use of previously produced and still current documentation that supports the accreditation process and security operations shall be encouraged.

17.1. Test Documentation. When required, test documentation shall include a ST&E plan and report. DITSCAP shall be used for guidance in producing the ST&E plan and report. This documentation shall be included as part of the SSAA.

17.2. Design Documentation. Network engineering manuals and installation drawings that illustrate network connections and physical layout, when available, shall suffice for design documentation.

KENNETH D. SUGGS, COLONEL, USAFR
COMMANDER

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFPD 10-11, *Operations Security*

AFI 10-1101, *Operations Security*

AFPD 31-1, *Physical Security*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 31-701, *Program Protection Planning*

AFI 31-702, *Systems Security Engineering*

AFI 31-703, *Product Security*

AFPD 33-2, *Information Protection*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115v1, *Network Management*

AFI 33-115v2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-117, *Visual Information (VI) 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 Program*

AFI 33-202, *Network and Computer Security*

AFI 33-203, *Emission Security*

AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*

AFI 33-205, *The Information Protection Metrics & Measurements Program*

AFI 33-206, *Air Force Specialized Information Protection Publications*

AFI 33-207, *Computer Security Assessment Program*

AFI 33-219, *Telecommunications Monitoring & Assessment Program (TMAP)*

AFMAN 33-223, *Identification and Authentication*

AFI 33-230, *Information Assurance Assessment and Assistance Program*

AFMAN 33-270, *Command, Control, Communications, and Computers (C4) Systems Security Glossary*

AFM 33-274, *On-Hook Telephone Security Guidelines*

AFI 33-332, *Air Force Privacy Act Program*

AFSSI 5009, *Information Protection Interim Toolset*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Time Compliance Network Order (TCNO) Management & Vulnerability & Incident Reporting*