BY ORDER OF THE COMMANDER
AIR FORCE RECRUITING SERVICE

AFRS INSTRUCTION 33-201

21 MARCH 2003

Communications and Information

COMPUTER SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AETC Publishing WWW site at http://www.aetc.randolph.af.mil/im. If you lack access, contact your base publishing manager.

OPR: HQ AFRS/RSIAP (MSgt Larry Gonzales) Certified by: HQ AFRS/RSI (Major Lannie Allen)
Pages: 29
Distribution: F

This instruction implements AFPD 33-2, *Information Protection*. It establishes and implements information protection and computer security (COMPUSEC) policy for Air Force Recruiting Service (AFRS). It applies to all AFRS personnel.

This publication does not apply to Air National Guard (ANG) and Air Force Reserve Command (AFRC) units. Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, *Records Disposition Schedule*. See Attachment 1 for a glossary of references and supporting information.

1. General Requirements:

1.1. The information in this instruction pertains to all AFRS information systems.

1.2. Security responsibilities for these systems are assigned to:

1.2.1. Designated approval authority (DAA) (AETC/SC).

1.2.2. DAA representative (HQ AFRS Commander, AFRS/RSI and group or squadron commanders).

1.2.3. Unit COMPUSEC manager (UCM).

1.2.4. Communication and information systems officer (CSO).

1.2.5. Information systems security officer (ISSO).

1.2.6. Information assurance awareness program (IAAP) manager.

1.2.7. System administrator (SA) (in most cases the SA will be the ISSO, UCM, and IAAP manager). Workgroup managers (WM) may also be tasked to perform these roles as directed by their local commander.

1.2.8. Small computer user.

1.3. Systems will not be used for processing information until the ISSO and UCM have completed all administrative requirements, and the DAA has granted approval. The UCM will perform accreditations on all small computers and send the results to HQ AFRS/RSIAP for validation. Once validated, submit

the accreditation packages to the DAA for approval. Complete subsequent certification in accordance with AFI 33-202, *Computer Security* and DoD 8510.1-M, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*.

1.4. The CSO and ISSO may perform spot checks at any time to ensure compliance with computer security policies. If a random check uncovers any violation, the ISSO will report the violation to the CSO who will recheck the system after correction. The CSO will again check the system at least once more within 60 days to verify continued compliance. If violations recur, the CSO will report them to the commander.

1.5. Information systems are not authorized to process classified information when connected to any local area network (LAN). On designated information systems approved to process classified data, the CSO will dedicate at least one set of removable storage media for classified processing only. This set of media will include, but is not limited to, system and word processing system disks, work disks, and dictionary disks, and will be handled and stored in accordance with AFI 31-401, *Information Security Program Management*. Also, dedicate one set of removable storage for unclassified use.

1.5.1. Users should position monitors, display terminals, and printers so unauthorized personnel cannot observe them through doors, windows, or by casual observation. In addition, the user should position the monitor so personnel entering the work area can be observed.

1.5.2. The ISSO will mark systems processing classified data with the highest classification of information authorized for processing.

2. Responsibilities:

2.1. Designated Approval Authority (DAA). The AETC/SC is the DAA for all information systems that process up to and including secret information.

2.2. DAA Representatives. DAA representatives will identify, address, and coordinate security accreditation issues with AFRSI/RSI (who in turn will coordinate with AETC/SC) and deal with the day-to-day issues of accrediting systems in accordance with AFI 33-202. In addition, they will assist in accomplishing the following DAA responsibilities:

2.2.1. Allocate funding and manpower resources to achieve and maintain an appropriate level of protection, and to remedy security deficiencies.

2.2.2. Identify the ISSO for all information systems under the DAA jurisdiction.

2.2.3. Ensure IA personnel review all information system requirements documents to ensure IA requirements are appropriately addressed.

2.2.4. Appoint a certifier to accomplish information system certification. Ensure individual possesses the technical expertise on the information system being certified, and on the security mechanisms in use.

2.2.5. Make appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat.

2.2.6. Ensure resources are available to support certification and security countermeasures.

2.2.7. Formally assume responsibility for the secure operation of the information system to operate in a specific environment.

2.2.8. Ensure security policy is developed, and certification goals are clearly defined.

2.2.9. Approve security requirements documents, memorandums of agreement, and deviations from security policy.

2.2.10. Accredit all information systems and applications under their authority prior to operation.

2.2.11. Appoint a UCM and IAAP manager (primary and alternates) in writing (Attachments 2 and 3).

2.3. Group or Squadron Unit COMPUSEC Manager (UCM). The group or squadron UCM (normally the systems administrator) and the alternate group squadron UCM will administer the computer security program for the group or squadron. These responsibilities are outlined in AFI 33-202. In addition, the group or squadron UCM will:

2.3.1. Maintain a COMPUSEC continuity folder.

2.3.2. Provide guidance to unit ISSOs as required.

2.3.3. Develop and conduct COMPUSEC self-inspections using the AETC inspection guidance as a reference (Attachment 4).

2.3.4. Ensure all group or squadron computer systems are submitted to DAA for approval.

2.3.5. Conduct semiannual meetings for all applicable group or squadron ISSOs.

2.3.6. Develop procedures to ensure staff agencies are informed of significant changes in COMPUSEC policies and procedures.

2.3.7. Prepare a letter certifying all computer systems within the group or squadron have a completed risk analysis or accreditation, and have received DAA approval to operate. Prepare this letter in July of each year.

2.3.8. Report computer viruses, using AETC incident reporting procedures established (AFSSI 5021, time compliance network orders [TCNO] and vulnerability and incident reporting).

2.4. Communication and Information Systems Officer. The CSO is the office manager or section chief (normally the support flight commander [RSS]) responsible for the overall operations of LAN and computer support in the facility. The CSO responsibilities are outlined in AFI 33-202. In addition the CSO will:

2.4.1. Establish security procedures and measures for their work areas.

2.4.2. Appoint ISSO for terminals and work areas under CSO control. ISSOs are responsible for the computer security program in their functional areas. The intent is to have a local representative available who is knowledgeable of computer security principles and the computer systems in their area.

2.4.3. Approve local computer security procedures for the workstations and remote terminal areas.

2.5. System Administrator. The SA is responsible for the overall operation of computer systems and any LANs under their control in accordance with AFI 33-202. The SA will:

2.5.1. Ensure the system is available to perform the daily operations as required.

2.5.2. Develop and periodically review a backup strategy for all systems. Ensure users and technicians follow the backup strategy, and perform backups on a rotational basis with a minimum of two sets of backup media. The SA should maintain one set off-site and document its location.

2.5.3. Review audit trail daily and perform system maintenance.

2.5.4. Inform the CSO or network manager (NM), ISSO, network security officer (NSO), and information technology (IT) equipment custodian of any potential problems that may effect the performance of the system.

2.5.5. Assist in installation of new software.

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

2.5.7. Ensure compliance with Air Force wireless LAN and personal digital assistant (PDA) policies.

2.5.8. Ensure the consent to monitoring statement is on all information systems.

2.6. Information Systems Security Officer. ISSOs are responsible for the computer security program in their functional area. The intent is to have a local representative available who is knowledgeable of the computer systems in their area and computer security principles. In addition the ISSO will:

2.6.1. Ensure antivirus software is loaded on all information systems.

2.6.2. Report any COMPUSEC incidents or vulnerabilities IAW AFSSI 5021.

2.6.3. Make sure audit trails are reviewed periodically (for example, daily, weekly, etc.).

2.6.4. Establish and manage a COMPUSEC training program for information system users specific to their work center.

2.6.5. Maintain a log of all TCNOs which contains the TCNO number, date, initials, and actions taken. This log may be electronic or paper-based. All applicable TCNOs will be acted upon. A list of TCNOs may be found at https://afcertmil.lackland.af.mil/advisories/advisory_list.html, or within e-mail (go to Public Folders, select All Public Folders, select AFRS HQ, select Information Assurance, select TCNOs, and select 2002/2003 [applicable year]).

2.7. Network Control Center ISSO. The NCC ISSO will:

2.7.1. Load and properly configure antivirus software on the server.

2.7.2. Ensure audit trail logs are checked for any anomalies, and report any found in accordance with AFSSI 5021. Maintain audit trail logs for one week either in electronic or printed form.

2.8. Small Computer User. The user will:

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

2.8.2. Inform the ISSO, CSO, or the NM of incidents or circumstances that may impact the security posture of the system or other data resources.

2.8.3. Safeguard classified, sensitive, and critical computer resources in their custody.

2.8.4. Lock the system or activate the screen saver when away from the workstation for 10 minutes or less (if supported by a base, set the screen saver to the more stringent requirement). Log-off, if away for more than 10 minutes.

2.8.5. With SA approval, temporarily disable the screen saver to accomplish the mission during official functions such as AF presentations. SAs will ensure applicable users are briefed in accordance with AFI 33-202 to reapply the screen saver after completion of the presentation.

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

2.8.7. Comply with proper password management as outlined in paragraph 4.3.

2.9. IAAP Manager. The IAAP manager is responsible for initial COMPUSEC training. The IAAP manager will provide training through computer-based training (CBT) (Attachment 5). Users must first in process through the USM and IAAP prior to logging onto the LAN or getting an e-mail account.

3. Air Force Recruiting Service Local Area Network:

3.1. System Description. The AFRS LAN consists of over 4000 user accounts. Individual workstations are configured differently. Differences include the size of the internal hard drives, monitors, keyboards, and the software installed. Specialized equipment used by individual workstations include modems, scanners, and laser printers. Individual workstations consist of on-line internal hard drives, user directories on the file server, and off-line devices for system data storage. Off-line devices include removable media such as compact discs (CD), digital video discs (DVD), floppy, ZIP, jazz disks, and backup tapes, etc.

4. Policies and Procedures:

4.1. Access Controls. Automated access controls help limit access to the AFRS systems to authorized users only. These controls include user passwords (basic input output system [BIOS] or boot-up and network) and restricted file access.

4.1.1. Prior to obtaining an account, all AFRS systems users will accomplish systems access procedures.

4.1.1.1. The user will fill out sections 1 through 9 of DISA Form 41, **System Authorization Access Request (SAAR)**, AFRS Overprint (Attachment 6).

4.1.1.2. The USM will verify all user clearances to ensure they have the required need to know, and clearance to use the AFRS systems. The USM will fill out sections 10 through 15.

4.1.1.3. The user's supervisor will fill out sections 16 through 23.

4.1.1.4. The user will receive IAAP training in accordance with AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*, prior to receiving LAN passwords.

4.1.1.5. The user's SA or WM will send the completed DISA Form 41 (AFRS Overprint) to the help desk for account creation.

4.1.1.6. Send the completed copy of DISA Form 41 (AFRS Overprint) to HQ AFRS/RSIAP.

4.1.2. Each user must use a personal password to logon to the AFRS network. Nonwindows NT/2000 systems must have BIOS or boot-up password and a screen saver password. The consent to monitoring banner statement must be on all systems. When leaving the workstation or turning over control to another person, users will log-off the system. The SA maintains LAN passwords in an encrypted format on the file server.

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

4.2. Audit Requirements:

4.2.1. Audit mechanisms for sensitive information must record any event that attempts to change the security profile. As a minimum, the SA will provide a mechanism for recording the following:

4.2.1.1. Login and logout.

4.2.1.2. User actions to open, close, create, execute, modify, or delete programs or files.

4.2.1.3. Date and time of the event.

4.2.1.4. Type of event.

4.2.1.5. Success or failure of the event.

4.2.1.6. Name of program or file introduced, accessed, modified, or deleted.

4.3. Password Management for LAN Workstations. SAs assign individuals a user identification (USERID) and password for their respective LANs. All USERIDs and passwords are unclassified but should be protected as for official use only (FOUO). Users will maintain BIOS and screen saver passwords on all computers assigned to the AFRS LAN, while the UCM ensures all have complied with this requirement (see paragraph 4.3.2).

4.3.1. Users gain access to the LAN through workstations the USERIDs and personal passwords. Access will be restricted to directories, applications, and files that the user is authorized to access. USERIDs should remain constant (in cases such as marriage, legal name change, modification may be required); however, all users will change their passwords every 90 days. Passwords will expire after 90 days. The user will follow instructions provided when notified to change their passwords (Attachment 7).

4.3.2. Passwords must be at least eight characters long and include alpha-numeric, upper and lower case, and special characters (passwords should not be based on sport teams, pets, spouses, children, dictionary words, social security numbers [SSNs], birthdays, etc.). Users must not write down or release passwords to another individual. When assigned the initial password, the user will sign a statement of understanding concerning responsibilities for accountability and protection from compromise. The SA will maintain these forms in the continuity folder.

4.3.3. Users will report suspected compromises to the CSO, NM, or SA within 24 hours. The SA will delete the old password and issue a new password.

4.3.4. Personnel assigned to the squadron will in process through the SA, who will issue a USERID and password. Additionally, personnel will out process through the SA, who will deactivate their user accounts. Upon notification of personnel actions by the supervisor, the SA will suspend passwords within one duty day for the following reasons:

4.3.4.1. Pending or current punitive action.

4.3.4.2. Commander suspends user access to the system.

4.3.4.3. Extended temporary duty (TDY) (more than 3 months).

4.4. Transmission of Information via the Internet, AFI 33-129, *Transmission of Information via the Internet*:

4.4.1. The commander and supervisor will:

4.4.1.1. Ensure assigned personnel use government equipment for official or authorized use only.

4.4.1.2. Authorize only legal and ethical use of the Internet that is in the best interest of the Air Force.

4.4.1.3. Authorize personal use of e-mail only when that use complies with the following stipulations:

4.4.1.3.1. Does not interfere with the performance of official duties.

4.4.1.3.2. Is of reasonable duration and frequency.

4.4.1.3.3. Serves a legitimate Air Force interest.

4.4.1.3.4. Creates no additional expense to the Air Force.

4.4.1.4. Obtain Internet access through the supporting CSO.

4.4.2. The users will:

4.4.2.1. Use government equipment, and access the Internet only for official business or authorized activities.

4.4.2.2. Determine the sensitivity, and apply appropriate protection to all information transmitted using the Internet.

4.4.2.3. Adhere to copyright restrictions.

4.4.2.4. Protect passwords and access codes.

4.4.2.5. Ensure all official records created while using the Internet are placed in the official records management system.

4.4.3. Prohibited uses of the Internet:

4.4.3.1. Any use of government-provided computer hardware or software for other than official and authorized government business.

4.4.3.2. Activities for personal or commercial financial gain. This includes, but is not limited to, chain letters, commercial solicitation, and sales of personal property.

4.4.3.3. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material.

4.4.3.4. Storing or processing classified information on any system that is not approved for classified processing.

4.4.3.5. Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

4.4.3.6. Participating in chat lines or open forum discussion unless for official purposes, and after approval by appropriate public affairs office.

4.4.3.7. Using another person's account or identity without appropriate authorization or permission.

4.4.3.8. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without the appropriate authorization or permission.

4.4.3.9. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission (such as for legitimate system testing or security research).

4.4.3.10. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

4.4.3.11. Permitting any unauthorized individual access to a government-owned or government-operated system.

4.4.3.12. Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.

4.5. Dial-up Access. Dial-up access to Internet service providers, such as America On-Line, CompuServe, Earthlink or others, is prohibited for users with Internet access through base and deployed networks except when an organizational subscription is established for official business, and the account is submitted by the DAA representative and authorized by the DAA.

4.6. Prohibited Information on a Web Site. Under no circumstances will the following types of information be placed on web sites available to the general public.

4.6.1. Classified information.

4.6.2. Privacy Act protected information.

4.6.3. FOUO information.

4.6.4. DOD contractor proprietary information.

4.6.5. Scientific and technical Information (STINFO) (see AFI 61-204, *Disseminating Scientific and Technical Information*).

4.6.6. Unclassified information requiring special handling.

4.6.7. Critical information as outlined in AFI 10-1101, *OPSEC Instructions*.

4.6.8. Freedom of Information Act (FOIA) exempt information for which the agency declines to make a discretionary disclosure.

4.7. E-mail Management and Use:

4.7.1. The Unit Commander will:

4.7.1.1. Manage the use of e-mail within their command that is consistent with Air Force and MAJCOM policy.

4.7.1.2. Setup initial and annual refresher training programs to make sure all e-mail users are trained on Air Force e-mail policy and appropriate use.

4.7.1.3. Setup procedures for internal storage and control of e-mail consistent with Air Force information security and records management policies.

4.7.1.4. Make sure unit out-processing includes removal of unnecessary e-mail accounts.

4.7.2. Network Managers will:

4.7.2.1. Implement and monitor compliance with Air Force e-mail policy.

4.7.2.2. Manage the day-to-day operations of the assigned e-mail systems, and act as the primary point of contact for e-mail policy implementation.

4.7.2.3. Report violations of policy to appropriate authorities for further action.

4.7.2.4. Implement Air Force and Defense Information Systems Agency (DISA) electronic messaging registration procedures according to AFI 33-127, *Electronic Messaging Registration and Authority*.

4.7.2.5. Ensure the confidentiality of e-mail viewed in the performance of their duties.

4.7.3. E-Mail Users will:

4.7.3.1. Comply with AFI 33-119, *Electronic Mail (E-Mail) Management and Use*.

4.7.3.2. Maintain sole responsibility for the content of e-mail messages, and ensure messages sent meet Air Force directives regarding appropriate use of e-mail.

4.7.3.3. Make sure information received or transmitted, that constitutes an Air Force record, is maintained according to Air Force records management directives, AFMAN 37-123, *Management of Records*, AFI 37-138, *Records Disposition—Procedures and Responsibilities*, and AFMAN 37-139.

4.7.3.4. Make sure the account from which e-mail message is sent is clearly identified.

4.7.3.5. Get approval through the chain of command before subscribing to, or participating in unofficial e-mail list servers and newsgroups.

4.7.3.6. Report any suspected violations of e-mail policy to the supervisor, information assurance office, or NM.

4.7.3.7. Verify the authenticity of messages received if the authorization of the message is uncertain.

4.7.4. Protection from Disclosure:

4.7.4.1. Protect the following from disclosure in e-mail: marital status, number or sex of dependents, gross salary of military personnel, civilian education degrees and major areas of study, school and year of graduation, home of record, home address or phone number, age or date of birth, present or future assignments for overseas, or for routinely deployable or sensitive units, office, unit address, and duty phone for overseas, or for routinely deployable or sensitive units.

4.7.4.2. SSNs are FOUO and need to be protected as such. When sending SSNs across the Internet or in e-mail, use encryption to prevent unintentional or unauthorized disclosure.

4.7.5. Protect from Unintentional or Unauthorized Disclosure. Protect the following from unintentional or unauthorized disclosure: classified information, internal personnel rules and practices, information specifically exempted from disclosure by other statutes, confidential commercial information, inter- or intra- agency records that are deliberative or predecisional in nature, information whose disclosure would constitute an invasion of privacy, investigative record or information gathered for law enforcement purposes, records of an agency that regulates or supervises financial institutions, records with geological and geographical information and data, including maps concerning wells.

4.8. Physical Protection. Physical protection is the easiest part of computer security to control, but it is also the easiest to circumvent. Personnel will lock offices during nonduty hours. Failure to follow established procedures subjects resources to unnecessary risks.

4.9. Software Security. The UCM provides virus protection software (Attachment 8). The SA or the WM will load this software on all information systems and LANs.

4.9.1. Virus protection software scans the memory and hard drive daily. The user will follow instructions provided when notified to update antivirus signature files. Additionally, users will scan all floppy diskettes before use; this includes commercial software purchased for installation. Users will only use software owned by the government on government systems.

4.9.2. Users should label all removable media (not including commercial off the shelf installation disks) with:

4.9.2.1. Classification.

4.9.2.2. Point of contact with a phone number.

4.9.2.3. File name, content.

4.10. Portable Computer Security. While used in an office environment, the security and environmental requirements for a portable computer are the same as those for a stationary system (keep in mind portable computers can be easily stolen)(see Attachment 9).

4.10.1. Absolutely **NO CLASSIFIED PROCESSING** is allowed on loaded portable computers. In addition, the user must acknowledge that all information is of a sensitive nature and take appropriate steps to safeguard the equipment, the data it contains, and the media used on the system.

4.10.2. Physical security must be a prime concern when using loaned equipment. Due to the small size and portability of laptop computers, a significant danger of theft exists if the equipment is left or stored in an uncontrolled area. The user should secure the laptop for protection when left unattended (for example, in a locked cabinet or locked room).

4.10.3. The IT custodian will obtain a statement of liability from the office to which the computer is assigned. The borrower will complete the statement of liability accordingly prior to system use. The IT custodian retains a copy. The borrower will also keep a copy and present it, if necessary, to show authorized use of the equipment. The borrower will return the equipment to the appropriate office, and will certify it is not damaged and functions properly. If not damaged, the borrower will then be given the

original receipt. If damaged, the IT custodian will process actions for replacement or repair of the equipment.

4.11. Virus Prevention. A virus is a self-replicating, malicious program segment that attaches itself to an application program or other executable system component, and leaves no external signs of its presence. It can cause corruption or erasure of data, and can even lead to unauthorized access or transmission of data. To help prevent penetration of a virus on a computer system, the following rules apply (Attachment 10):

4.11.1. Frequently backup files.

4.11.2. Limit access to information systems.

4.11.3. Use antivirus software to scan all floppies, hard disk drives, e-mail messages, and attachments.

4.11.4. Scan hard disk drives after systems return from repair centers.

4.11.5. Don't use illegal copies of software or disks brought from home.

4.11.6. Beware of borrowed or unsolicited software.

4.11.7. Scan all commercially procured software before installing; even new commercial software can have viruses.

4.11.7.1. If one set of disks will install multiple copies on different computers, ensure all the disks are write protected to avoid possible virus spreading.

4.11.7.2. If someone identifies a computer as infected, isolate immediately (no exceptions).

4.12. Virus Reporting. DO NOT ATTEMPT TO USE AN INFORMATION SYSTEM SUSPECTED OF CONTAINING A VIRUS! Use the chain of command to report virus infections of computer systems. Notify immediate supervisors, the ISSO, and the UCM as a minimum. If the antivirus software detects and stops the virus, no reporting is necessary. ISSOs and UCMs will use AFSSI 5021, Attachment 10, to report viruses that have infected the information system.

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

4.13.1. Preventive Maintenance. External components should be cleaned with a mild soap and water solution. **DO NOT USE AMMONIA PRODUCTS.** In addition to physical cleaning, the hard drive should be examined (using software) for proper configurations and optimized regularly.

4.13.2. System Failure. Users will report system failure or problems to their ISSO. The ISSO will examine the workstation or other components, and attempt to resolve the problem. An authorized service technician must repair problems that cannot be resolved.

4.13.3. Workstation Failures. Should a workstation fail and need extensive repairs, the CSO will develop a plan to work around the station’s loss (additional guidance can be found in paragraphs 4.14, 4.15 and 7). Proper data backup procedures will prevent catastrophic losses.

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

4.13.5. LAN Connectivity Failures. LAN connectivity failures are normally software related problems. To prevent this type of failure, do not change system files config.sys or autoexec.bat without consulting the SA. Nonsoftware connectivity failures usually occur when components are physically disconnected from the LAN cabling. Only network management personnel, designated WMs and SAs, are authorized to disconnect and connect components to the LAN.

4.14. Workgroup Manager (WM). In accordance with AFI 33-115, Volume I, *Network Management*, the WMs will be utilized first for any information system problem. The SA is the primary interface between the WMs and the help desk.

4.15. Help Desk. The help desk is the primary interface for any information system problem the WMs/SAs cannot resolve. The help desk receives all trouble or install calls, and assesses or determines the type of problem. Help desk technicians record, track, and close reported problems, and offer technical advice and solutions for network systems, software applications, and mainframe data processing. Technicians route problems to trouble teams, network (NCC) functional areas, or other technical support centers like the Defense Mega Center, DISA or the Standard System Group at Gunter AFB. The help desk is the primary interface between the NCC and the WMs/SAs within AFRS. Help desk personnel are responsible for updates in the domain name server (DNS), and the global address list (GAL). They take care of passwords and profiles for e-mail access.

4.16. Wireless Local Area Network (WLAN) And Personal Digital Assistant (PDA). AF/SC has implemented AF/SC Policy Memorandum 10-1-2001, Air Force Policy for Wireless Local Area Network (WLAN) and Personal Digital Assistant (PDA) (see https://www.afca.scott.af.mil/prodeval/Reports/WLAN-PDA_guidance_10oct01.pdf). All users of PDA's must complete the required PDA training and documentation (see AFI33-202, Attachment 3).

5. Transmission of Classified on an Unclassified System:

5.1. Notify ISSO and UCM of any e-mail message (or any other type electronic correspondence) containing classified information that was transmitted over one or more unclassified LANs. The UCM will then contact the SA and the wing COMPUSEC manager. AFSSI 5020, *Remanence Security*, provides clearing, purging, declassification guidance, and lists references for Air Force and Department of Defense (DoD) evaluated products approved for declassifying magnetic media.

5.2. The AFRS COMPUSEC manager will contact the e-mail originator to ascertain all addressees of the e-mail including their organization. In addition, the AFRS COMPUSEC manager will request the following from the e-mail recipients:

5.2.1. If a hard page copy of the information was made instruct the recipient to secure the hard page copy, and sanitize the printer IAW AFSSI 5020.

5.2.2. If the information was saved to a system's hard drive, or removable magnetic storage media such as a floppy disk instruct the recipient to purge the data from the hard drive or removable storage device. For example, if the addressee saved the information to a hard drive or floppy disk, and then later deleted the file, the information is still available. The AFRS COMPUSEC manager will instruct the recipient to recover and then purge the information.

5.2.3. If the e-mail or information was sent to anyone else contact the new addressees and SA, and restart the cycle. The AFRS COMPUSEC manager will maintain documentation on all purging (for example, declassification) actions.

5.3. The SA will purge the e-mail from the LAN. The method used to purge the e-mail will vary depending on specific LAN hardware and software configurations. The SA must use an Air Force approved purging method, and must identify variances such as when a user deletes an e-mail message.

Normally this action only deletes systems pointers to the information, not the data itself. The SA will first retrieve the information, and then purge the data rendering it unrecoverable. If the incident occurs over a timeframe in which system backups were performed, secure and purge the backup media.

5.4. Recovery action should be a team effort. As a minimum, the team should include members from WMs, SAs, help desk (AFRS Customer Support Center), applicable base/NCC support and IA. Each member has expertise and skills to answer questions, and provide assistance to SAs or individual users responsible for purging their systems. The transmission of classified information over an unclassified LAN is a security incident reportable under AFI 31-401, *Information Security Program*. IA personnel are responsible for ensuring the information is purged from computer systems. The USM will perform other actions associated with the security incident. When an incident occurs, ensure the USM is notified.

6. Remenance Security. Nonvolatile storage media containing classified and/or sensitive material (sensitive material includes, but is not limited to, Privacy Act and FOUO material) must be cleared in accordance with AFMAN 33-223, *Identification and Authentication,* before turn-in or before uncleared maintenance personnel begin work on the system. To clear a drive, either degauss or use an authorized wipe disk utility. Reformatting or deleting is not acceptable as information may still be recovered.

7. Configuration Management. All LAN and server accreditations will be recertified every 3 years or when significant changes occur, to include amendments to accreditations.

8. Screen Saver Policy:

8.1. Instructions. SAs may adapt the following message to brief applicable users:

8.1.1. Users may temporarily disable the screen saver only when the mission requires (for example, movies, PowerPoint presentations, etc.

8.1.2. The user will reapply the screen saver with a maximum time of 10 minutes.

8.2. Users must comply with AFI 33-202, *Computer Security,* when leaving their terminal unattended, even for a brief period, and should activate a password protected screen saver**.** (***NOTE:*** Using password-protected screen savers in conjunction with BIOS passwords afford maximum protection for sensitive information. Using screen saver alone provides minimal protection.)

9. Forms Adopted. DISA Form 41, AF Form 1297, AF Form 2519, and SF 711.

EDWARD A. RICE, JR., Brigadier General, USAF
Commander

10 Attachments
1. Glossary of References and Supporting Information
2. Unit COMPUSEC Sample Appointment Memorandum
3. Information Assurance Awareness Program Manager Sample Appointment Memorandum
4. AETC Inspection Guidance
5. Computer-Based Training
6. Sample DISA Form 41 (AFRS Overprint)
7. Password Management
8. Antivirus Software Information
9. Laptop Computer Physical Security
10. Antivirus Signature File Update Message

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-2, *Information Protection*
AFI 31-401, *Information Security Program Management*
AFI 33-115, Volume 1, *Network Management*
AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*
AFI 33-119, *Electronic Mail (E-Mail) Management and Use*
AFI 33-127, *Electronic Messaging Registration And Authority*
AFI 33-129, *Transmission of Information via the Internet*
AFI 33-202, *Computer Security*
AFI 37-138, *Records Disposition--Procedures and Responsibilities*
AFI 61-204, *Disseminating Scientific And Technical Information*
AFMAN 33-223, *Identification and Authentication*
AFMAN 37-123, *Management of Records*
AFIMAN 37-139, *Records Disposition Schedule*
AFSSI 5020, *Remanence Security*
AFSSI 5021, *Time Compliance Network Orders and Vulnerability and Incident Reporting*

Abbreviations and Acronyms

AFI—Air Force instruction
AFMAN—Air Force manual
AFSSI—Air Force system security instruction
BIOS—Basic input output system
CBT—Computer-based training
COMPUSEC—Computer security
CSO—Communication and Information Systems Officer
DAA—Designated approval authority
DISA—Defense Information Systems Agency
DITSCAP—DoD Information Technology Security Certification and Accreditation Process
DNS—Domain name server
DOD—Department of Defense
FOUO—For official use only
IA—Information assurance
IAAP—Information assurance awareness program
ISSO—Information systems security officer
IT—Information technology
LAN—Local area network
NCC—Network control center
NM—Network manager
NSO—Network security officer
PDA—Personal digital assistant
SA—System administrator
SSN—Social security number

STINFO—Scientific and technological information
TCNO—Time compliance network order
UCM—Unit COMPUSEC manager
UCMJ—Uniform Code of Military Justice
USM—Unit security manager
WM—Workgroup manager

Attachment 2

UNIT COMPUSEC SAMPLE APPOINTMENT MEMORANDUM

(Date)

MEMORANDUM FOR HQ AFRS/RSIAP

FROM: (Organization/Office Symbol)

SUBJECT: Appointment of Unit COMPUSEC Manager (UCM)

1. In accordance with AFI 33-202, paragraph 2.11, the following individuals are appointed as the primary and alternate COMPUSEC manager for (your organization):

NAME	RANK	OFFICE SYMBOL	TELEPHONE	E-mail

2. This memorandum supersedes all prior memorandums of appointment, same subject.

(COMMANDERS SIGNATURE BLOCK)

Attachment 3

INFORMATION ASSURANCE AWARENESS PROGRAM MANAGER SAMPLE APPOINTMENT MEMORANDUM

(Date)

MEMORANDUM FOR HQ AFRS/RSIAP

FROM: (Organization/Office Symbol)

SUBJECT: Appointment of Unit Information Assurance Awareness Program (IAAP) Manager

1. In accordance with AFI 33-204, paragraph 15.1, the following individuals are appointed as the primary and alternate IAAP manager for (your organization):

NAME	RANK	OFFICE SYMBOL	TELEPHONE	E-mail

2. This memorandum supersedes all prior memorandums of appointment, same subject.

(COMMANDERS SIGNATURE BLOCK)

Attachment 4

AETC INSPECTION GUIDANCE

ALL PURPOSE CHECKLIST	PAGE 1 OF 3 PAGES
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA NETWORK LICENSING AND CERTIFICATION (AFI 33-115, Vol 2)	OPR AFRS/RSIA DATE

NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
1	Have all information systems support personnel (systems administrators and information management) completed the Computer Use IBT (Information Systems User Module), the INFOCON IBT, and the Information Systems Administrators/Workgroup Manager IBT, or met host base requirements (if on an	☐	☐	☐
2	Has every individual who has access to the Air Force Network (af.mil) domain been licensed prior to network access by completing the Computer Use IBT (Information Systems User Module) and the INFOCON IBT, or met host base requirements (if on an Air Force base)? (Para 4.2)	☐	☐	☐
3	Have all systems administrators and information managers completed or are they on track to complete their AFRS certifications as functional systems administrators and workgroup managers, respectively? (Para 5 and AFRS/RSI Memo, 15 Apr 02)	☐	☐	☐
	COMPUTER SECURITY (AFI 33-302)			
1	Has the unit commander appointed a unit COMPUSEC manager? (Para 2.11)	☐	☐	☐
2	Has the DAA accredited all information systems and applications under their authority prior to operation? (Para 2.7.11, 3.1.1, and AFPD 33-2, para 1.4)	☐	☐	☐
3	Are all information systems recertified and reaccredited every 3 years unless changes to the information system or environment baseline impact security, thereby necessitating recertification or reaccreditation sooner? (Para 3.1.2)	☐	☐	☐
4	Is anti-virus software implemented on all information systems and networks? (Para 3.13.1)	☐	☐	☐
5	Are users using only anti-virus tools and signature files/datafiles obtained from the AFCERT FTP or DoD Computer Emergency Response Team (CERT) web sites? (Para 3.13.1.1)	☐	☐	☐
6	Have users pulled down the newest signature files from a controlled site as soon as notified they are available? (Para 3.13.1.3)	☐	☐	☐
7	Have procedures been established to rapidly obtain, distribute, and install changes to anti-virus software on all information systems (including network servers)? (Para 3.13.1.4)	☐	☐	☐
8	Have virus prevention, detection, eradication, and reporting procedures been included in user training? (Para 3.13.8)	☐	☐	☐
9	Are malicious logic attacks properly reported according to AFSSI 5021, Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting? (Para 3.13.4)	☐	☐	☐

AF FORM 2519, 19911101 *(IMT-V1)* PREVIOUS EDITIONS ARE OBSOLETE.

ALL PURPOSE CHECKLIST	PAGE 2 OF 3 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OPR	DATE	

NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
10	Has the ISSO performed an initial evaluation of each vulnerability or incident and taken corrective or protective measures, and has he/she reported them according to AFSSI 5021? (Para 2.11.3.5)	☐	☐	☐
11	Are the following password requirements being met? Composition: non-dictionary words; alphanumeric characters (upper & lower case) with at least one special character whenever possible; unrelated to one's personal identity, history, or environment (i.e.,	☐	☐	☐
	Length: minimum of 8 characters where capability exists? Life-cycle: changed every 90 days Protection/storage: All passwords must be protected based on the sensitivity of the information or	☐	☐	☐
	is itself classified SECRET). At a minimum, you must safeguard all passwords as "For Official Use Only" (FOUO). (AFMAN 33-223, para 3.3-3.6)	☐	☐	☐
	INFORMATION ASSURANCE AWARENESS PROGRAM (AFI 33-204)	☐	☐	☐
1	Has the unit commander appointed a unit IAAP Manager and an alternate? (Para 15.1)	☐	☐	☐
2	Is the Unit IAAP Manager supporting and implementing the IA awareness program and coordinating IA awareness materials with the IA office as needed (includes host wing IA office for those located on a base)? (Para 16.1)	☐	☐	☐
3	Are users of DoD telecommunications, including contractors and their employees, notified that using United States government telecommunications systems constitutes consent to telecommunications monitoring? (AFI 33-219, para A3.3)	☐	☐	☐
	COMPUTER SYSTEMS MANAGEMENT AND ACCOUNTABILITY - Activity Commanders	☐	☐	☐
1	Did the commander establish policies and procedures for management and support of organization's IT	☐	☐	☐
2	Did the commander designate, in writing, an adequate number of ECs to ensure proper safeguarding and accountability of IT equipment? (AFI 33-112, AETC Sup 1, para 7.5)	☐	☐	☐
3	Did the commander annually certify to the AFRS ECO the appointment of ECs and that an annual physical inventory was accomplished for all computer systems and IT equipment under his/her control? (AFI 33-112, para 7.6)	☐	☐	☐
4	Did the commander ensure departing ECs out process through AFRS ECO? (AFI 33-112, para 7.5.2)	☐	☐	☐
5	Did the commander establish procedures to ensure all IT equipment, including those purchased using the GPC card, is reported to the EC and ECO to ensure inventory accountability? (AFI 33-112, AETC Sup 1, para 7.10)	☐	☐	☐
	Computer Systems Equipment Custodians (EC)	☐	☐	☐
1	Did the EC sign for and manage all accountable IT equipment within his/her span of control? (AFI	☐	☐	☐

ALL PURPOSE CHECKLIST	PAGE 3 OF 3 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OPR	DATE	

NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
2	Did the EC monitor his/her IT equipment inventory and notify the AFRS ECO of new, excess, transferred, and/or missing equipment? (AFI 33-112, para 11.1, 11.4, 11.5, 11.8, 11.11, and 24.3 and AETC Sup 1, para 11.5, 11.8, 11.15, 24.3)	☐	☐	☐
3	Did the EC perform an annual physical inventory of his/her assigned IT equipment following guidance and direction from the AFRS ECO? (AFI 33-112, para 11.1.1)	☐	☐	☐
4	Did the EC notify the AFRS ECO, in a timely manner, when IT equipment becomes excess? (AFI 33-112, para 11.11 and 33)	☐	☐	☐
5	Did the EC ensure that excess IT equipment is stored securely and properly to prevent damage, deterioration, and unauthorized cannibalization until the equipment can be properly disposed of? (AFI 33-112, para 11.15 and 33)	☐	☐	☐
6	Did the EC ensure that a current IPMS bar code label is attached to each accountable IT equipment item? (AFI 33-112, AETC Sup 1, para 11.2 and 24.1-24.3)	☐	☐	☐
7	Did the EC immediately notify the commander of any lost, damaged, or destroyed IT equipment items? (AFI 33-112, para 11.12)	☐	☐	☐
8	Did the EC maintain coordination with the AFRS ECO and provide status throughout the process of Reports of Survey, including a copy of the final report? (AFI 33-112, AETC Sup 1, para 11.12)	☐	☐	☐
9	Did the outgoing EC perform a joint physical inventory before transferring responsibility and processing out through the AFRS ECO? (AFI 33-112, para 11.9 and 11.10)	☐	☐	☐
	UNIT SOFTWARE LICENSE MANAGEMENT - AFI 33-114, AETC Sup 1	☐	☐	☐
1	Has the unit commander appointed a software license manager to administer the unit's software license	☐	☐	☐
2	Has the unit software license manager ensured all newly assigned personnel receive software license training within 30 days of arrival? (Para 19.11)	☐	☐	☐
3	Has the unit software license manager coordinated on all software acquisitions? (Para 19.1)	☐	☐	☐
4	Is the unit software license manager promoting user awareness concerning unauthorized or illegal use of	☐	☐	☐

AF FORM 2519, 19911101 *(IMT-V1)* PREVIOUS EDITIONS ARE OBSOLETE.

Attachment 5

COMPUTER-BASED TRAINING (CBT)

A5.1. Site Address. The Information Assurance Awareness Program (IAAP) can be found at the Air Force CBT site, http://afcbt.den.disa.mil.

A5.2. CBT Requirements:

A5.2.1. Users will take the Network User Licensing, and INFOCON CBTs. Users have to pass both tests with a minimum of 70 percent, and provide documentation (a printout is acceptable) of their score prior to getting an account for e-mail or AFRISS.

A5.2.2. WMs (AFSC 3A0X1), in addition to Network User Licensing, and INFOCON, will take the Workgroup Manager CBT.

A5.2.3. SAs (AFSC 3C0X1), in addition to Network User Licensing, and INFOCON, will take the Systems Administrators CBT.

Attachment 6

SAMPLE DISA FORM 41 (AFRS OVERPRINT)

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY:	EXECUTIVE ORDER 10450, 9397, AND PUBLIC LAW 99-474, THE COMPUTER FRAUD AND ABUSE ACT
PURPOSE OF USE:	TO RECORD NAMES, SIGNATURES, AND SOCIAL SECURITY NUMBERS FOR THE PURPOSE OF VALIDATING THE TRUSTWORTHINESS OF INDIVIDUALS REQUESTING ACCESS TO DEPARTMENT OF DEFENSE (DOD) SYSTEMS AND INFORMATION.
ROUTINE USES:	THOSE GENERALLY PERMITTED UNDER THE 5 U.S.C. 522A(B) OF THE PRIVACY ACT AS REQUIRED.
DISCLOSURE:	DISCLOSURE OF THIS INFORMATION IS VOLUNTARY; HOWEVER, FAILURE TO PROVIDE THE REQUESTED INFORMATION MAY IMPEDE, DELAY OR PREVENT FURTHER PROCESSING OF THIS REQUEST.
NOTE:	RECORDS MAY BE MAINTAINED IN BOTH ELECTRONIC AND/OR PAPER FORM.

TYPE OF REQUEST: ☒ INITIAL ☐ MODIFICATION ☐ DELETION ☐ USER ID _____ | DATE: 14 Feb 2003

SYSTEM NAME *(Platform or Applications)*: RAAFRS35WZ | LOCATION *(Physical Location of System)*: Bldg 35

PART I: *(To be completed by Requestor)*

USER (STEP 1)

1. NAME *(LAST, FIRST, MI)*: Gonzales, Larry		2. SOCIAL SECURITY NUMBER
3. ORGANIZATION: HQ AFRS	4. OFFICE SYMBOL/DEPARTMENT: RSIA	5. PHONE *(DSN or Commercial)*: 7-6555
6. OFFICIAL E-MAIL ADDRESS: larry.gonzales@rs.af.mil	7. JOB TITLE & GRADE/RANK: MSgt	
8. OFFICIAL MAILING ADDRESS		

USER AGREEMENT (COMPLETE BLOCK 29 OR 30 AS APPROPRIATE)

I accept the responsibility for the information and DOD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DISA/DOD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

9. USER SIGNATURE	10. DATE: 14 Feb 2003

UNIT SECURITY MANAGER (STEP 3)

PART II: SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OF CLEARANCE INFORMATION.

11. CLEARANCE LEVEL	11a. ADP DESIGNATION	
12. TYPE OF INVESTIGATION	12a. DATE	
13. VERIFIED BY: *(Print name)*	14. SIGNATURE	15. DATE

SUPERVISOR (STEP 2)

PART III: ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number and date of contract expiration in Block 16).*

16. JUSTIFICATION FOR ACCESS

17. TYPE OF ACCESS REQUIRED: ☐ AUTHORIZED ☐ PRIVILEGED

18. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify Category)*

☐ OTHER _____

19. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☐	19a. EXPIRATION DATE FOR ACCESS *(Specify date if less than 1 year)*	
20. SUPERVISOR'S NAME *(Print name)*	21. SUPERVISOR'S SIGNATURE	22. DATE
23. SUPERVISOR'S ORGANIZATION/DEPARTMENT		23a. PHONE NUMBER

24. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR (STEP 4)	24a. PHONE NUMBER	24b. DATE

25. SIGNATURE OF ISSO (STEP 5)	26 ORG./DEPARTMENT	27. PHONE NUMBER	28. DATE

DISA Form 41, APR 2002 (EF) (AFRS OVERPRINT) (DISA IR) (DTS, Inc.) FormFlow 2.15, V1.00

29. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS: (*Complete as required for user or functional level access*)

☒ I HAVE COMPLETED DOD INFORMATION AWARENESS CD. DATE 2 Mar 2001

30. SYSTEM ADMINISTRATOR/DISA SSP CERTIFICATION LEVEL:

☐ LEVEL I

☐ LEVEL II *(Indicate Operating System(s))* _____

☐ LEVEL III _____

31. OPTIONAL INFORMATION

PART IV: COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED	PROCESS BY: *(Print name and sign)*	DATE
DATE REVALIDATED	REVALIDATE BY: *(Print name and sign)*	DATE

DISA Form 41, APR 2002 (EF) (AFRS OVERPRINT) (DISA IR) (DTS, Inc.) FormFlow 2.15, V1.00

INSTRUCTIONS

A. Part I: The following information is provided by the user when establishing or modifying their USERID.

(1) Name: The last name, first name, and middle initial of the user
(2) Social Security Number: The social security number of user.
(3) Organization: The user's current DISA organization (i.e. DISA CIO, DOD and government agency or commercial firm)
(4) Office Symbol/Department: The office symbol within the current organization (i.e. CIO/IAD)
(5) Telephone Number/DSN: The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
(6) Official Email Address: The user's official email address.
(7) Job Title/Grade/Rank: The job title civilian (EX. Systems Analyst, GS-14, Pay Clerk, GS-5)/, military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
(8) Official Mailing Address: The user's official mailing address
(9) User's Signature: User must sign the DISA Form 41 with the understanding that they are responsible and accountable for their password and access to the system(s).
(10) Date: The date that the user signs the form.

B. Part II. Certification of Background Investigation or Clearance.

(11) Clearance Level: The user's current security clearance level (Secret, Top Secret).
(11a) ADP Designation: The user's ADP Designation (ADP1, ADP3, etc).
(12) Type of Investigation. The user's last type of background investigation. (i.e., NAC, NACI, or SSBI)
(12a) Date : Date of last investigation.
(13) Verified By: The Security Manager or his representative print his/her name that the above clearance and investigation information has been verified
(14) Signature: The Security Manager or his representative signature indicates that the above clearance and investigation information has been verified.
(15) Date: The date that the form was signed by the Security Manager or his representative.

C. Part III. The below information requires the endorsement from the User's Supervisor or the Government Sponsor.

(16) Justification for Access: A brief statement is required to justify establishment of an initial USERID. Provide appropriate information if the USERID or access to the current USERID is to modified.
(17) Type of Access Required: Place an "X" in the appropriate box. (Authorized- Individual with normal access) (Privileged- Those with privilege to amend or change system configuration, parameters, or settings)
(18) User Requires Access to: Place an "X" in the appropriate box. Specify Category.
(19) Verification of Need to Know: To verify that the user requires access as requested.
(19a) Expiration Date for Access: The user must specify expiration date if less than 1 year.
(20) Supervisor's Signature (Print Name): The supervisor or representative prints his/her name that the above information has been verified and access is required.
(21) Supervisor's Signature: Supervisor's signature is required by the endorser or his/her representative.
(22) Supervisor Date: Date he/she signs the form.
(23) Supervisor's Organization/Department: Supervisor's organization and department
(23a) Supervisor's Phone Number: Supervisor's phone number
(24) Signature of Functional Data Owner/OPR: Signature of the functional appointee responsible for approving access to the system being requested.
(24a) Phone Number: Functional appointee phone number
(24b) Date: The date the Functional appointee signs the DISA Form 41
(25) Signature of ISSO: Signature of the ISSO or sponsoring office responsible for approving access to the system being requested.
(26) ORG./Dept: ISSO's organization and department
(27) Phone Number: ISSO's Phone number
(28) Date: The date ISSO signed the SAAR Form.
(29) IA Training and Awareness Certification Requirements: User must indicate if they have completed the DOD Information Awareness CD and the date
(30) System Administrator/DISA SSP Certification Level: Place an "X" in the appropriate certification level box.
(31) Optional Use: This section is intended to add site specific information, as required.

D. Part IV. This information is site specific and can be customized by either the DECC, functional activity, or the customer with approval of the DECC. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DECC or by the Customer's ISSO. Recommend file be maintained by ISSO adding the user to the system.

DISA Form 41, APR 2002 (EF) (AFRS OVERPRINT) (DISA IR) (DTS, Inc.) FormFlow 2.15, V1.00

Attachment 7

PASSWORD MANAGEMENT

A7.1. Password Format Compliance Message. The following is an automated message users may receive if their password has been compromised:

A7.1.1. A recent check of password strength indicates your password was cracked by HQ AFRS/RSIAP. Ensure your new password meets requirements stated in AFMAN 33-223, *Identification and Authentication,* paragraph 2.4.

A7.1.2. Your password must have at least:

Eight characters One upper-case character One lower-case character One number One special character Also do not choose passwords based on spouses, children, pets, sports teams, dictionary words, etc.

Please change your password as soon as possible and ensure it meets the requirements mentioned above.

A7.2. Changing Your Email Password: Log into one of the Outlook web access web pages at:

360th Group https://afrsmail360.rs.af.mil/exchange 367th Group https://afrsmail367.rs.af.mil/exchange 369th Group https://afrsmail369.rs.af.mil/exchange 372nd Group https://afrsmailwest.rs.af.mil/exchange

A7.2.1. At the Yellow MS Outlook Web Access page:

Log on using your (Firstname.Lastname@rs.af.mil)

A7.2.2. When you get the grey login box:

Enter afrs/firstname.lastname for the Username and your password.

A7.2.3. Once you are in email, click on the Options icon on the left side.

A7.2.4. Click on the change password button (you may need to scroll down to see it). You will then get the Internet Service Manager window. Change the Domain to read AFRS, enter your firstname.lastname as the account, then your old and new passwords.

A7.3. Password Policy. Direct password policy questions to HQ AFRS Information Assurance office at DSN 487-6555 or COMM (210) 652-6555.

A7.4. Assistance with Passwords. HQ AFRS personnel will contact their WM if they require help to change their passwords. Contact the AFRS Help Desk at DSN 487-2251 or COMM (210) 652-2251 if additional help is needed to change your password.

A7.5. Password Expiration Notice: The following is an automated password expiration notification:

A7.5.1. Our records indicate your e-mail account password will expire in 4 days. AFMAN 33-223, paragraph 2.6, states passwords will be changed every 90 days. Please change your password as soon as possible or your account will be automatically locked out. Ensure your new password meets requirements stated in AFMAN 33-223, paragraph 2.4.

Attachment 8

ANTIVIRUS SOFTWARE INFORMATION

NOTE: The Symantec Norton Antivirus and Firewall solution is the AFRS standard (if supported by a base follow their standard).

A8.1. Licensing. The DoD has licensed an extensive offering of computer security software. This software includes products from Symantec and McAfee. The software can be used on all military and DoD civilian work systems. DoD contractors may use the software only on DoD-owned computer systems, noncontractor owned systems. Military and DoD civilian workers may also take a copy of the computer security software home to install on their home machines. DoD contractors cannot take the software home.

A8.2. Software Availability. What software is available? The list of software available from McAfee and Symantec is pretty extensive. It includes antivirus software for computers, PDAs, and software firewalls for computer systems. The software available from McAfee is McAfee VirusScan, Virex for McAfee, and McAfee VirusScan for PDAs. Symantec offers Norton Antivirus Corporate Edition, Norton Antivirus for Palm, and Symantec Desktop Firewall.

A8.2.1. McAfee's VirusScan is available for Windows 9x, NT, W2K, OS/2, Unix, and ME. McAfee's Virex is available for those using Macintosh OS. McAfee VirusScan for PDAs 2.0 protects PDAs running Windows CE/Pocket PC, Palm, and EPOC operating systems.

A8.2.2. Norton Antivirus is available for Microsoft DOS, Windows 9x, NT, W2K, XP, and ME; Macintosh; and OS/2 operating systems. Norton Antivirus for Palm will only protect systems running the Palm OS. The Symantec Desktop Firewall is available only for Windows 9x, NT, or W2K.

A8.2.3. The antivirus software will protect computers and PDAs from viruses (if the signature files are kept up to date). The firewall software will protect systems connected by broadband connections (via cable modems or DSL) to the Internet by filtering and blocking potentially dangerous attacks.

A8.3. Obtaining Software. The software is available several ways:

A8.3.1. Download directly from the DoD CERT site at http://www.cert.mil. A .mil address is required for access. The HQ AFRS IA office has copies of the software in the e-mail Public Folders (go to Public Folders, select All Public Folders, select AFRS HQ, and then select Information Assurance) for users that do not have a .mil address. One word of warning, though, the software is quite large and may take a while to download, especially over a dialup connection. Your SA may be able to make a copy of the software on CD and mail to you.

Attachment 9

LAPTOP COMPUTER PHYSICAL SECURITY

A9.1. Overview. This attachment establishes physical security policy, guidelines, and other pertinent information relating to use, storage, and transportation of laptop computer systems for all AFRS personnel. With advancing technology and AFRS initiatives to maximize use, laptops are an integral part of our recruiting efforts. Laptops are, however, highly pilferable items, and demand specialized attention to prevent loss or damage. Education, awareness, training, and accountability are the keys to our success. Everyone is expected to fulfill his or her responsibilities as outlined below.

A9.2. Hand Receipts. Before the SA or EC issues a laptop, the user must receive training on the care and protection of government laptop computers. The user must also sign a hand receipt, AF Form 1297, **Temporary Issue Receipt,** verifying the necessary training.

A9.3. Office. As with all IT equipment, the laptop should be secured in an inaccessible, safe location when not in use.

A9.3.1. If the user must leave the office unattended for *any* period of time, secure the government laptop in a safe location (for example, a locked cabinet, locked safe, or locked desk with limited access). When possible, lock the office doors and windows each time when leaving.

A9.3.2. Do not rely on others sharing the office to secure the area, resources, or government laptop computer. The user is personally accountable, and must protect these resources with vigilance.

A9.4. Vehicle. Keep the laptop out of sight and secured while in the vehicle. Protect the laptop at all times during transport, whether in a government-owned vehicle sedan, van, privately owned vehicle, or other vehicle.

A9.4.1. When leaving the office or home, if possible, place the laptop securely in the trunk or on the floor behind the driver's seat in order to prevent it from sliding, tumbling or sustaining damage due to movement of the vehicle. If these areas are unsuitable due to the design of the vehicle, place the laptop in another area that provides sufficient protection.

A9.4.2. Do not invite theft. If user is unable to take the laptop, lock in the trunk or other concealing area of the vehicle.

A9.4.3. If securing in the trunk, do so *before* departure instead of upon arrival. Be aware that thieves may be watching movements as laptops are secured.

A9.4.4. Never leave a laptop in a vehicle overnight, no matter how secure.

A9.5. Airport. Thieves use multiple approaches to pilfering laptops in airports. Never leave IT equipment unattended or out of your sight. Awareness is paramount to safe transport of the laptop through an airport.

A9.5.1. When at the ticketing area, place the laptop on the counter in front of you so that it remains in sight as you take care of ticketing tasks with the agent.

A9.5.2. Avoid checking your laptop in as baggage; the airline will not bear the responsibility for damage, even if the laptop is safely packed. Luggage handling can damage laptops, particularly the display screen.

A9.5.3. When walking to the terminal, place the laptop in the x-ray machine only after you have a clear path to proceed through the metal detector and retrieve it. One strategy of thieves is to activate the alarm in front of you to block your path while another casually takes your laptop as it exits the x-ray machine. Thieves may also try to take the laptop from the x-ray machine before it passes through.

A9.6. Hotel. As in all other situations, secure the laptop in an inaccessible location when not in use, such as in a room safe, or front desk safe. If these options are not available, take reasonable measures to secure the laptop. If conditions warrant, keep the laptop in your possession while away.

A9.7. Other. Accidents caused by users can present as much of a loss as theft.

A9.7.1. When walking, place the laptop in its carrying case, preferably one equipped with a shoulder strap. Also use any internal safety straps the laptop case may have, which provides support as well as a safety check for the case's zipper, or velcro closures.

A9.7.2. Carry the laptop firmly at all times to avoid dropping it, should you bump into something or someone.

A9.7.3. Never place a drink, or other potentially dangerous material, or liquid near the laptop, as spilling can cause extensive damage. The keyboard, inputs, drive doors, speakers, SCSI ports, and many other avenues exist that would inadvertently permit liquids to damage the equipment.

A9.8. Lost, Stolen, or Damaged. If the laptop is lost, stolen, or damaged, initiate a Report of Survey. If the user is found negligent, the user will likely be held financially responsible to some extent for the loss or damage. The cost of a typical recruiter's laptop is approximately $2,500. While you may find yourself in many unique situations, remember that the laptop is <u>your</u> responsibility. In all situations use sound judgment and keen awareness. If situations exist that are not covered by this policy act as a reasonable and prudent individual would act under the same or similar circumstances.

A9.9. General. Laptop computers are relatively fragile, considerably expensive, and very important to our recruiting goals. But possibly more valuable than the laptop is the information it contains. In a world where individual privacy, and the security of personal data are being viewed with greater scrutiny, it is essential to protect this information. The laptop may contain a great deal of personal information regarding applicants. Loss of this information must be avoided. Should negligence in handling the laptop lead to the loss of personal information on applicants, the user may be held personally responsible for any legal repercussions that follow.

A9.10. Point of Contact. For further assistance, please contact the AFRS ECO (HQ AFRS/RSISR), at DSN 487-5256 or commercial (210) 652-5256.

Attachment 10

SAMPLE ANTIVIRUS SIGNATURE FILE UPDATE MESSAGE

-----Original Message-----
From: Duarte Mario MSgt AFRS/RSIAP
Sent: Thursday, July 11, 2002 8:40 AM
To: 311RCS SQ All; 313RCS SQ All; 314RCS SQ All; 318RCS SQ All; 319RCS SQ All Flt Sec; 331RCS SQ All; 332RCS SQ All; 333RCS SQ All; 338RCS SQ All; 342RCS SQ All; 343RCS SQ All; 344RCS SQ All; 345RCS SQ All; 347RCS SQ All; 348RCS SQ All; 349RCS SQ All; 362RCS SQ All; 364RCS SQ All; 367RCS All; 368RCS SQ All; AFRS All System Administrators; AFRS HQ Work Group Manager
Cc: AFRS Information Assurance
Subject: Please Update Your Norton Antivirus

New virus definitions dated **10 Jul 02** are available. Follow these steps to update your Norton Antivirus:

1. Click on "Start" in the lower left-hand corner of your screen.
2. Click on "Programs" in the menu that pops up.
3. Locate "Norton Antivirus Corporate Edition."
4. Click on the "Norton Antivirus Corporate Edition" shortcut that pops out.
5. Check the date of your definition file. This will be in the "Version Definition File" section of the Norton Antivirus Corporate Edition main screen
6. If your definitions are not current, get the signature files from the AFRS Public Folders found in "Outlook":
   Public Folders -> All Public Folders -> AFRS HQ -> Information Assurance -> Antivirus -> Signature Files

Note: If you have difficulty getting them from the AFRS Public Folders, you may use the LiveUpdate functionality located on the main screen of the Norton Antivirus Corporate Edition (found at step four).
   a. Follow steps one through four to get there.
   b. Click on LiveUpdate to update your signature files.

Users: This message has been coordinated with your System Administrator for distribution.

System Administrators/HQ AFRS WMs: Please ensure update advisories are distributed to all applicable users not listed above as recipients [360RCG, 319RCS All (319RCS All Flt Sec is listed above), ... 330RCS, 336RCS, 337RCS, 339RCS, ...369RCG, 341RCS,..... 372RCG, 361RCS, 369RCS].

FYI: IAW AFI 33-202, Computer Security, Para 3.13.1.1, the primary source for antivirus tools and signature files/datfiles is either the AF Computer Emergency Response Team (AFCERT) File Transfer Protocol (FTP) or DoD Computer Emergency Response Team (DoD-CERT) web sites (DoD-CERT performs quality assurance checks and signature lab testing prior to making them available to DOD. This often results in an update being available later than the date listed on the signature itself). Once released by DOD-CERT, Information Assurance (Network Control Center function) then informs our users to adhere to the above signature file update steps (which include using the LiveUpdate functionality as a secondary source).