



Communications and Information

***COMPUTER SECURITY FOR INFORMATION SYSTEMS
(NETWORKS) PROCEDURES AT THE SENSITIVE LEVEL***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: 919 MSS/SCB (MSgt Carol S. Earnest)

Certified by: 919 MSS/CC
(Lt Col Michael B. Black)

Pages: 12

Distribution: F

The purpose of this instruction is to establish operational security instructions for Information Systems (network) processing information at the sensitive level. It details how the risk of operating a network will be minimized by coordinated implementation of specialized disciplines of personnel security, physical security, operations security (OPSEC), computer security (COMPUSEC), information security, communications security (COMSEC), emanations security (EMSEC), and Fraud, Waste, and Abuse (FWA). It also specifies minimum-security measures for systems or networks interfacing with the network. This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*; DoD 5200.28 STD, *Department of Defense Trusted Computer System Evaluation Criteria*. This instruction pertains to all 919 SOW units and their members.

1. Security Objectives for Data Processing, Handling, and Storage:

1.1. This instruction does not replace security requirements or instructions of higher organizational levels. This instruction will not be changed without designated approving authority (DAA) approval. Conflict between requirement interpretation in this policy and higher level requirements shall be brought to the attention of the computer system security officer (CSSO).

1.2. Confidentiality. Only personnel with proper authorization and need-to-know will be allowed access to data processed, handled, or stored on network components. The Terminal Area Security Officer (TASO) will have at least one fully trained alternate appointed at all times to preclude security and operational impacts during periods of sickness or leave.

1.3. Integrity. Hardware and software resources for the system shall operate according to requirements and design documents. Unauthorized personnel will not be able to maliciously or unintentionally alter data processed, stored, or handled by the network and the data shall be accurate.

2. Additional Security Objectives Levied by DAA.

2.1. Mission Effectiveness. The network will ensure work can be accomplished in a timely manner with the degree of security assurance required by the mission. Disabling required computer security functions is not an acceptable method to achieve operational performance goals. If the impact is assessed to be beyond acceptable limits, users will formally submit to the DAA those features they require disabled. The DAA will be the approval authority for this request.

2.2. User Acceptance. 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. A network design goal is to ensure security mechanisms are useful tools and viewed as an ally, instead of an adversary, by the people who use it to accomplish their missions.

3. Basic System Facts:

3.1. Classification of Information Processed. Data processed on the network will be no higher than sensitive.

3.2. Categories of Information Processed. No formal categories of sensitive information exist, however, some types of information with special handling and access instructions processed on a network (specifically For Official Use Only (FOUO) and Privacy Act (PA) information) have some of the characteristics of compartments that require extra protection. The addition of formal categories of information requiring an increased need for protection and access restriction will require a new risk analysis, certification, and DAA accreditation.

3.3. Minimum and Maximum User Clearances. Although sensitive information does not require a formal clearance, only individuals authorized by the DAA or designated representative will be allowed access to the network data.

4. Password Control:

4.1. Method of Password Control. A combination of physical, personnel, and system security mechanisms shall control access to systems. This section focuses on the system security mechanisms and later sections address the physical and personnel aspects of access.

4.2. The system shall use the combination of a user identification for an individual user and password known only to that user to control initial system access. The CSSO shall not allow the use of group ID and passwords for initial system access. The TASO shall change, as soon as safely possible, vendor-provided default passwords not later than 30 days after installation. The user should protect against tampering with the computers and information on unattended computers. Provide protection by controlling physical access to the computer itself; by installing keyboard locks, passwords, password protected screen savers, etc.; or by establishing controls for removal and secure storage of information from unattended computers. Screen savers and screen saver passwords are required on all systems. All systems must be protected at all times, regardless of low or high usage.

4.3. Discretionary Access Control is the mechanism by which users, either individual or group, are limited to the objects they may access. The principle of least privilege for access to system-defined resources will be utilized. This is the principle that a user should be given the least amount of power or privilege that still enables the individual to do his or her job. The system shall allow the CSSO to define administrative groups of users with like resource access permissions and authority requirements for ease of security administration. If a user obtains access to a resource or performs a function as the result of a group permission or authority; the system shall identify the user ID performing the action in addition to the group permission or authority on which the decision is based.

4.4. Password length. Passwords must use eight characters (use upper and lower case) with at least one special character (@&+, etc.) and/or number. The CSSO shall protect passwords and automatically perform password administration such that only the user has knowledge of their own password. Personnel shall apply a DAA-approved alternative means of positive identification to components, which lack password capabilities.

4.5. Password Generation. Users shall generate their own personal passwords which conform to an operating system-controlled mask. The system shall not allow a new password which duplicates the old password nor shall it allow the new password to be the same as or a variation of the user-ID or the user's name. Variations are simple modifications to the user-ID or user name such as reversing the order of characters or adding a one digit prefix or suffix (OLDUSER becomes OLDUSER1, for example). Passwords shall be valid for no more than 90 days. The system shall prompt the user for a password change prior to expiration.

4.6. Password Destruction. The CSSO shall clear or destroy materials, which contain expired passwords, such as paper, or diskettes, which contain active passwords. The CSSO shall clear reusable magnetic media after 130 days. The CSSO shall destroy materials, which cannot be cleared or reused according to the DAA.

4.7. Password Protection. The system shall protect password files so that users cannot access them (except to allow a user to change their personal password). All users shall protect their passwords as FOUO. Users shall not write down passwords (unless they are locked in a safe) or reveal them to anyone else, including the CSSO. Only the CSSO have deletion rights to password files.

4.8. Changing Passwords. Users shall be able to change their own password anytime but no later than every 90 days.

4.9. The CSSO shall have the capability to immediately expire or invalidate user passwords. The system shall deny access to an expired password. To regain access privileges, the CSSO must reactivate the user's account. The CSSO shall require the user to enter a new password to maintain password confidentiality.

4.10. Situations that require a CSSO to expire a password immediately are when compromise of a user's password is suspected or known; when someone in the user's chain of command has identified an individual as a "disgruntled employee", when the supervisor notifies the CSSO that an individual having knowledge of a password is transferred, discharged, or reassigned; or when an individual's commander denies that person access to the IS information.

4.11. Password Lockouts. The CSSO shall limit the number of consecutive incorrect access attempts by a user ID to no more than three and shall automatically deactivate the user ID after the third unsuccessful logon attempt. The system's action to deactivate a user ID shall affect only that user ID and shall not disable or otherwise affect the system or a different user who attempts to use the system. In recording the number of consecutive unsuccessful attempts for a specific user ID prior to reaching the lockout threshold, the system shall reset the number to zero only after a successful login. For example, if a user has unsuccessfully tried to logon two consecutive times, he or she cannot reset the counter by either physically or logically disconnecting the terminal. The count may only be reset before the lockout threshold is met by logging on successfully. User cannot change their password no more than one time in 14 days. CSSO is responsible to furnish software to generate password change, to control time cutoff for passwords; to monitor the password system at all times.

4.12. Password Disclosure. Users shall not disclose their password to anyone. Users shall be responsible for actions attributed to the misuse of their password. If a user feels their password has been disclosed to another individual, they shall change it immediately and notify their CSSO.

5. Systems Manager or User Privileges. Users with special permissions or privilege shall use them only for the requested or intended purpose. The system administrator shall remove the permissions or privileges from those who abuse them. The system administrator shall reinstate user privileges only upon the DAA determination. The DAA shall be the only users allowed to grant permissions or privileges.

6. Password Manager Requirements. The CSSO shall be the password manager. When a user account is newly created, the CSSO will either deactivate the account (the preferred method) or change the password to a random sting. Deactivating the account is preferred because this allows the account to remain on the system, but in a completely unusable state. The user shall not use default passwords and shall not write the password down. Before the user logs on the first time, the CSSO shall ensure the user completes the required security awareness, training, and education (SATE) training and brief the importance of protecting passwords and choosing good passwords. After the initial password briefing is given, the CSSO shall reactivate the account or change the password. At the first login, the user shall enter a new password.

7. Dial-up and Remote Login Access. This is not available at Duke Field.

8. Personnel Security:

8.1. Security Clearances. Although no security clearance levels are required for sensitive information, a minimum of a favorable investigation (has a need-to-know) for all authorized users is required.

8.2. Need-to-Know. Personnel with system access must have a verified need-to-know for all data they can access. The CSSO shall make the need-to-know determination based upon an access request by the user's supervisor.

8.3. Situations Which Merit Denying Access. The CSSO shall immediately deny or remove a user's access if the user's organization removes access for cause. The CSSO shall, within 3 workdays, remove accounts of users who no longer require access in performance of their duties, have moved, or have retired. A user's organization will notify the CSSO if a user will not require access for a period of 30 days or more. The CSSO shall inactivate these accounts, and shall remove user accounts from the system if they have been inactive for a period of 180 days or more without prior coordination.

8.4. Physical Security. All personnel shall protect information systems (IS) resources (processors, terminals, communications media) from natural threats (e.g., flood, weather), physical disasters (e.g., fire, building collapse), human threats (intentional and unintentional), and any other identified physical security mechanisms, where deemed feasible and cost effective, to prevent or limit damage. Assistance in identifying physical security requirements can be obtained from AFI 31-209, *The Installation and Resource Protection Program*.

8.5. Resource Protection. IS personnel shall secure resources which process, store, or handle data within areas which provide adequate protection during and after duty hours. This requirement applies to all terminals, servers, routers and other equipment on the system. Removable storage media shall be stored in lockable containers when not in use.

8.6. Protection of Support Systems. Install surge protection or some form of electrical power conditioning on all electrical power sources serving IS resources.

8.7. Uninterruptable power supply (UPS) systems, which will allow the primary resources to be gracefully brought down in the event of power failure shall be installed. Primary resources are those necessary for the system to continue operation such as servers and routers.

8.8. Personnel shall ensure fire extinguishers are readily accessible in all areas where IS resources are located.

8.9. Hardware. The TASO shall ensure hardware security controls meeting the requirements of AFI 31-209 are in place, documented, and implemented for each IS resource. The TASO shall establish housekeeping procedures which prohibit eating, drinking, and smoking around IS assets and address their general exterior cleanliness and routine operator care.

8.10. Software. The use of the term software in this policy shall include operating system software and application software, to include database, spreadsheet, and word processing applications. TASOs will perform random checks throughout their area of responsibility to ensure there is no copyright violations of commercial off-the-shelf software and all computer systems are free of "pirate" software. Results of these checks will be maintained by each TASO.

8.11. No person shall load or execute privately owned or "bulletin board" software on the IS. For personally written or locally developed software follow guidelines in AFI 33-202, *Air Force Computer Security Program*.

8.12. If a user needs to install public-domain software or shareware on an IS, the DAA shall approve installation on a case-by-case basis upon CSSO certification that the software does not degrade/circumvent implemented security safeguards, and is safe for government use. In order to do this, the CSSO shall check to see if the software is listed in the evaluated product list (EPL) or Air Force assessed product list (APL). The CSSO may present an alternative method of certifying public-domain software or shareware for consideration as long as it provides a high degree of confidence that it will detect "Trojan horses" and other forms of malicious logic.

8.13. The CSSO and the Command Post (CP) personnel shall develop a standard contingency plan or Continuity of Operations Plan to reduce the impact caused by unanticipated interruption of an IS operation. 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, water damage, loss of all or part of the system's capabilities, inoperative components, defective storage media, maintenance problems, disruption to operations due to building evacuation, and complete or partial failure of security measures. AFM 10-401, *USAF Operation Planning Process (FOUO)*; AFI 32-4001, *Planning and Operations*; and AFSSI 5019, *Contingency Planning Guide* (when published) provides contingency planning guidance. The ECO shall ensure individual installations can meet contingency processing requirements.

8.14. Backup and Recovery. The CSSO and the CP shall maintain and make immediately available to unit's a roster of key people to be contacted during recovery operations. All sections shall ensure that backups or "save" actions of changed or updated files are made nightly. Critical files include security related and audit files as well as those designated as critical by operational personnel. All backups shall be stored in an off-site location if determined critical files.

8.15. Emergency Response. The CSSO and the CP shall maintain a roster of key people to be contacted during emergency operations.

8.16. Exercising and Testing. The CSSO shall review the contingency plan at least annually and conduct tests of the plan to ensure its adequacy. The CSSO shall document the test.

8.17. Marking/Labeling. Personnel shall ensure that unclassified materials which require special marking and handling, such as For Official Use Only (FOUO) mandated by the Freedom of Information Act (FOIA), or Privacy Act, are marked in accordance with AFI 31-401, *Information Security Program Management*.

8.18. Automated Marking. The CSSO should automate as much marking of printed outputs as possible to relieve users from manually marking. However, the CSSO shall ensure users receive continual training and reminders that they, not the system, are responsible for the accuracy of these markings.

8.19. Marking Storage Media. Personnel shall use Air Force approved pressure sensitive labels to mark storage media at the highest level for which it was ever used.

8.20. Marking Peripheral Devices. Peripheral devices are not required to be marked.

9. Maintenance:

9.1. Maintenance on Hardware Devices. System components shall be cleared of sensitive unclassified information using approved clearing procedures before releasing the equipment for maintenance.

9.2. Software Maintenance. The TASO shall ensure periodic checks of operational software are performed by comparing the original application to that used on the operational system to detect any unauthorized changes. The TASO shall ensure all original copies of software are write protected, inventoried, and copies and originals kept in a safe location.

9.3. Declassification/Destruction:

9.4. Declassification of Information. No special declassification procedures are necessary because classified information is not processed by information System covered under this policy.

9.5. Destruction of Storage Media. There is no requirement for the destruction of magnetic storage media containing sensitive unclassified information. Compact Discs are optical storage media that retain their highest sensitivity until destroyed. Destroy CDs in accordance with AFSSI 5020, Chapter 6.

9.6. Destruction of Output Products. FOUO and PA output shall be destroyed in accordance with their respective Air Force directive publications by tearing, shredding, or incineration. FOUO and PA printed outputs shall not be commercially recycled unless such activity is approved by the DAA. FOUO and PA printed output shall be locked up when not in use and destroyed when no longer needed. The recycle process at Duke Field will accept FOUO and PA material if it is packed up in a box with tape, marked with your name and phone number.

9.7. Inadvertent Classified Contamination. When classified information is discovered on the unclassified network, immediate action is required to minimize the unintentional exposure of classified information. The following is the sequence of actions required by the individual who discovers the classified information:

9.7.1. Individual discovering the classified information should immediately secure computer by turning off the monitor power, while leaving the power to the computer on. Post a guard. Contact Duke Command Post at 883-6701 and inform them of the current situation. Notify affected computer's Automated Data Processing Equipment (ADPE) custodian. Await disposition from 919 MSS/SCP, CSSO or authorized representative before using the affected system.

9.7.2. Individual discovering the incident should also notify the Wing Security Manager and provide all requested information concerning the incident.

9.7.3. The LAN Managers should immediately work to identify the servers containing the classified information so they can be shut down and sanitized to preclude further propagation of the classified information. The CSSO will also notify the TASOs responsible for any unclassified workstations that may have had classified information placed on them for sanitization.

10. Fraud, Waste, and Abuse (FWA). Prescribing directives formalized the Air Force commitment to prevent and eliminate fraud, waste, and abuse. It prescribes policy, establishes procedures, and provides guidance to make sure that resources allocated to the Air Force are applied effectively, to support national priorities. All users and managers at all level shall ensure fraud, waste, and abuse policies are supported. Additionally, no users shall violate copyright laws (specifically software and software documentation). Personnel must be aware of copyright restrictions placed on information system software.

11. Certification and Accreditation:

11.1. Security Certification Requirements. The CSSO will develop a security certification package in accordance with AFSSI 5024; Volume I, *The Certification and Accreditation (C&A) Process*, and provide this certification package to the DAA. The following documents shall comprise the certification package:

11.2. Security Plans. Security plans, mandate procedures and processes for end-using organizations to implement and use the system securely. Security plans, in combination with the security policy and security architecture, describe the required security environment for all at Duke Field.

11.3. System Description. A complete description, including hardware and software listings, of the standard information system.

11.4. Risk Analysis Report. The risk analysis shall provide an analysis of information containing the following activities and their associated stand-alone documents. See AFSSI 5024, Volume II, *The Certifying Official's Handbook*, for further information.

11.5. Sensitivity and Criticality Assessment. A sensitivity and criticality assessment shall document the importance to the operational mission of data processed by the information system and the extent to which its data must be protected from loss, unauthorized disclosure, or modification. See AFI 33-202 for further guidance on sensitivity and criticality.

11.6. Risk Assessment. The risk assessment includes a program level vulnerability assessment and threat assessment and shall document the information system vulnerabilities, threats common to most installations, likelihood of threat occurrence in a typical environment, degree of residual risk from matching threat vulnerability pairs, and the expected effectiveness of security measures.

11.7. Security Certification Requirements. The CSSO shall review all system changes and updates for security impact, and update all security documentation as necessary. Upon a major change to the security environment, or after 3 years, the CSSO will reaccomplish the risk analysis, recertify the system, and provide a new certification package to the designated DAA. The package will be provided to each TASO, who must certify achievement of all mandatory requirements, and document his certification to the DAA. If the TASO mandates additional requirements, or determines the conditions of the mandatory security environment cannot be met, the using organization will conduct additional risk analysis and determine if the necessary degree of assurance can be achieved.

11.8. Security Awareness, Training, and Education (SATE). Training shall promote proper and consistent application by users of basic information system security features and procedures to provide needed protection for information. It shall include training on procedures to report incidents and vulnerabilities. The CSSO shall implement the SATE program in accordance with Eglin AFB requirements. SATE training shall be accomplished and documented for all personnel prior to their obtaining access, and annual security awareness refresher training. The CSSO shall maintain the training documentation. Individual must take to the CSSO a copy of the SATE training quiz and AAC Form 7, **Eglin Computer Network (ECONET) Account Request**, before they will be allowed access.

11.9. Depth of Training. Required depth of training shall depend on the security management position. Depth of security awareness training requirements are:

11.9.1. The CSSO is to be the information system security expert. The CSSO must have a complete understanding of the security requirements and the reporting of incidents and vulnerabilities.

11.9.2. TASOs are responsible for the proper implementation of the system security program in their work area. Their training shall be primarily focused on the identification of practices dangerous to security and on the initial evaluation of suspected vulnerabilities or identified violations.

11.9.3. System Users. Depth of security awareness training for system users shall be primarily focused on the proper use of available system security features. TASOs are responsible for providing users familiarization training.

12. Newcomers: Newcomers will be briefed in the newcomer inbriefing. All small computer users must complete Security Awareness Training within 60 days of assignment. Security Awareness Training must be completed before individual will be able to obtain an E-Mail address or be permitted to use your system. Information will also cover that security includes the protection of machines against tampering, abuse, theft, and unauthorized disclosure of information.

13. Inability to Satisfy Requirements. There may be cases when implementing computer-based security hardware or software in an information system is not technically sound, violates the objective of economy by being prohibitively expensive, is time consuming, or will adversely impact the operational performance of the information system. Existence of such a case does not invalidate this policy. Its objectives, or requirements. Rather, it challenges information system personnel to implement alternate security mechanisms which will satisfy intent of the policy until a more appropriate solution can be acquired. The selection of alternative security mechanism to compensate for an unrealistic solution will be considered temporary and requires periodic DAA review for its continued appropriateness.

14. Virus Reporting Procedures. All ADPE account custodians or their designated representatives will ensure that an Air Force approved virus detection program is installed on all DOS/Windows/OS.2 computer systems and that each system is scanned at least once a week for virus infection. All account custodians are responsible for training and information for virus pattern identification, maintaining up to date virus software upgrades, informing users of virus reporting procedures, and assisting users in upchanneling virus report forms. In the event that a virus is discovered on a system, the person making the discovery or their supervisor will contact CSSO/SCB immediately. Then they will contact their ADPE account custodian even if automatic virus removal has occurred, and identify the equipment as being infected by viral activity in the following ways:

14.1. Notifying coworkers.

14.2. Labeling the system with a notice (i.e. sign or some other identifier) state the virus' name, date discovered, and removal states (infected/disinfected).

14.3. In all instances, submit a completed virus incident report form to the ADPE account custodian.

14.4. All ADPE account custodians or their designated representatives will forward all virus report forms to the Command Post for tracking purposes:

14.5. Command Post personnel will log the virus incident and forward report forms to the Wing Command before forwarding final report to AFRC.

15. Network Protocol Information Protection (IP) Address. CSSO from Duke Field must obtain IP addresses from 96 CG/SCTXN. These IP numbers must be current and up-to-date at all times. TASOs will request their IP numbers from the CSSO. The request must be submitted using the network address template provided by CSSO. The TASO will log the domain section as per this sample (EG-228-001/EG-228-099). The section that says Host Name will be left blank at all time.

15.1. The CSSO will need to order IP address numbers using a different template provided by 96 CG/SCTXN. They will not order IP numbers unless the accreditation package for that section has been approved by the DAA and a copy is maintained in the CSSO office.

16. Copyright Violations. TASOs will make random checks throughout the unit's to ensure there is no copyright violations of commercial off-the-shelf software and all computer systems are free of "pirate" software. TASOs will inform their commanders and the CSSO immediately of any misuse.

17. Public Web Site. There is no public web site at Duke Field at this time.

THOMAS M. STOGSDILL, Colonel., USAFR
Commander

ATTACHMENT 1
VIRUS INCIDENT REPORT

A1.1. Reporting period:

A1.2. Reporting Information:

- a. Name/Rank:
- b. Unit
- c. Base
- d. MAJCOM

A1.3. Malicious logic name (complete section 3a-e for each malicious logic detected).

- a. Number of systems infected:

TYPE SYSTEM*	# Detected Before Infection	# Detected After Infection
Mission Critical		
Mission Essential		
Mission Impaired		
Non-Mission Essential		

- b. Number of workhours expended.
- c. Operating system and version
- d. List standard system(s) affected (if applicable, i.e., GCCS, CAMS, FAMS).
- e. Source of infection, if known:
 - ___ AF software.
 - ___ COTS or outside source.
 - ___ Personal disks.
 - ___ Downloaded files.