

**4 NOVEMBER 2003**



**Communications and Information**

**ELECTRONIC CLASSIFIED PROCESSING**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

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

---

OPR: 927 CF/SCBS (John Benzel)

Certified by: 927 CF/CC  
(Capt John T. McMahon, Jr.)

Pages: 6

Distribution: F

---

This instruction implements AFD 33-2, *Information Protection*, (will become Information Assurance). It establishes an electronic classified processing security instruction for the 927 ARW processing of classified information in a networked or non-networked environment. It applies to all individuals processing classified information electronically.

**1. General:** All classified processing will be done in accordance with all applicable Air Force directives and regulations. Only systems that have been properly accredited and EMSEC certified are authorized to process classified information electronically.

1.1. All classified systems must operate under one of two conditions:

1.1.1. The system has only removable media, operates in an environment approved for the degree of classified processed, and uses periods processing (processes classified and unclassified in separate sessions with separate sets of magnetic media). All classified materials and media are secured in an approved storage container when unattended. Unless specifically approved for open storage, do not use PCs that have fixed storage media to process, store, or view classified information.

1.1.2. The entire system is permanently located in an area cleared for the open storage of classified, or secured in an approved storage container when unattended. The system itself and all components containing non-volatile memory are labeled and protected at the highest level of classified processed.

1.2. The individual responsible for each classified processing system must ensure each user understands this security instruction and continuously uses proper procedures when processing data on the system.

1.3. A copy of this instruction will be present with each classified system and signed off by authorized users yearly as an acknowledgement and understanding of its contents. Any discrepancies or

problems with this instruction will be brought to the attention of the Wing Information Assurance Office (WIAO).

## 2. Physical Security:

2.1. Microcomputers are high-value items, vulnerable to loss or theft. Even when no classified is present on the system, required protective measures are mandated by AFI 31-101, *The Air Force Installation Security Program*.

2.2. During classified processing, microcomputers must be protected to the same degree and by the same methods required to protect all classified material.

2.3. Systems processing classified data will have all major components (i.e., CPU, Monitor, Printer, etc.) marked with the highest classification of information authorized for processing.

2.4. Each classified computer will have an authorized user access list that names all individuals who have been granted unescorted access to that system. Access to systems and information is based on clearance, authorization, and need-to-know. Clearances must be verified by the appropriate security manager; authorization and need-to-know are determined by management (e.g. division or branch). Authorized users are responsible for ensuring that only properly cleared personnel are allowed access to the system or area when classified processing is underway.

2.5. Prior to beginning classified processing the doors and windows to the room will be secured to prevent any unauthorized viewing. Position computer monitors, display terminals, and printers so unauthorized personnel cannot observe them through doors, windows, or by casual observation. The monitor should be positioned so you can observe personnel entering the work area. A sign will be posted on the door indicating classified processing in progress.

2.6. All classified storage media and material must be in positive control by appropriately cleared personnel until stored in a GSA approved safe or placed in an area approved for open storage. **Never leave a classified system unattended when in use, unless it is operating in an approved classified open storage area.**

2.7. A physical inspection of the area will be performed at the end of each duty day. This inspection will verify that all classified material has been properly secured. The check will be recorded on Standard Forms (SF) 702, **Security Container Check Sheet**, and SF 701, **Activity Security Checklist**.

## 3. Computer Security:

3.1. All classified equipment and storage media (i.e., removable hard drive, floppy disks, etc.) will be labeled with the highest classification level for which the system is authorized to process.

3.2. Users are responsible for ensuring that all printed products are reviewed and marked at the top and bottom of each page with the highest classification contained.

3.3. Any disk inserted into the system assumes the highest classification of the system and must be labeled as such with the appropriate Standard Form Classification Label and ADP Media Label.

3.4. All files copied from the system to any removable media will assume the highest classification of the system.

3.5. Permit only authorized personnel to perform maintenance. Do not allow users to perform maintenance, make modifications to the system, or tamper with the equipment covers and cabling. Do not

provide classified diskettes, cartridges, or ribbons to maintenance personnel for system testing - use unclassified media only. If cleared maintenance personnel are not available, the system should first be properly sanitized and all maintenance must be observed by technically qualified and appropriately cleared personnel. Report any suspicious practices to your ISSO, supervisor, or security manager.

3.6. The use of modems in classified processing computers is strictly prohibited unless specifically approved by the DAA. There are inherent risks associated with modem use which presents a danger to all other computers using the same network.

#### **4. Emission Security:**

4.1. "EMSEC (Emission Security)" is the protection resulting from all measures taken to deny unauthorized persons information of value, which might be derived from intercept, and analysis of compromising emanations from crypto-equipment, information systems, and telecommunications systems. Air Force EMSEC efforts are concerned with the control of compromising emanations at all Air Force organizations with equipment or systems that process classified information.

4.2. Air Force organizations and contractors acquiring or using systems to process classified information must apply EMSEC proportional to the threat of exploitation and the potential damage to national security if the classified information is compromised.

4.3. The Wing EMSEC Manager determines the required countermeasures and specific installation procedures according to EMSEC guidelines/procedures based on the classification level and the amount of information processed. There are three parts to the assessment: information systems, communications systems, and cryptographic equipment. Each part has three outcomes: Not applicable; no countermeasures are required; or countermeasures are required. The Wing EMSEC Manager will explain these to you, and what will be required of you.

4.4. Users must be sure to maintain the continuous separation of electrical and electronic circuits, components, equipment, and systems which handle classified plain text (RED) information in electrical signal form from those which handle unclassified (BLACK) information in the same form. All unclassified electronic devices (i.e., phone, radio, PC, etc.) must be physically separated from any classified electronic processing device.

4.5. Remember, the telephone is our greatest security hazard. It picks up more than the voice of the person holding it, i.e., other voices or equipment sounds in the background. Don't discuss classified information within the area when someone is on the phone. Never leave the phone off the hook. Equipment sounds may reveal the text being processed!

#### **5. Periods Processing:**

5.1. One of the biggest security concerns occurs when classified computer components and unclassified components are introduced to one another. There are a few circumstances where this is permissible, providing that certain procedures are followed, however, this process must be approved during the accreditation process. You must be careful in instances like this so that you do not compromise classified information.

5.2. If you are using a computer for periods processing (meaning that you have one hard drive for classified processing and one for unclassified processing), there are several precautions that must be taken. You must ensure that you are disconnected from all unclassified resources (i.e. LAN connec-

tions, shared printers, etc.). This needs to be done prior to powering up in a classified mode, or vice versa.

5.3. As before, you must ensure that all components are appropriately labeled. This is especially important when you deal with removable hard drives used in periods processing. If you are using a printer for classified printing, there may be specific requirements to clear it when you are done. Ensure that there are written procedures in place for all these items, and that users are aware of them.

5.4. Prior to changing security modes, unclassified to classified, or vice versa, the user must ensure completion of the following steps:

5.4.1. Power the system down for at least one (1) minute.

5.4.2. Ensure all removable media of one classification is properly stored away before bringing out removable media of another classification.

5.4.3. Ensure the hardware is labeled with the appropriate classification.

5.4.4. If the system is both unclassified and classified network connected, the network connection of the one must be physically disconnected prior to beginning processing of the other. **NOTE:** The user must visually inspect to ensure this is accomplished.

5.4.5. Prior to any classified processing, all normal security procedures must be followed (e.g., securing the affected area, posting signs that classified processing is being done, etc.).

5.4.6. When processing classified, the user must ensure that all EMSEC requirements identified for the system are complied with (e.g. physical separation from unclassified processors, etc.)

## 6. Remanence Security:

6.1. Magnetic remanence is the magnetic representation of residual information that remains on automated information systems' (AIS) storage media after it is erased by overwriting, degaussing, and so on. The proliferation of various types of AIS storage media (e.g., magnetic tapes and disks, optical media, solid state semi-conductor memory, etc.) has resulted in the development of separate procedures for clearing, sanitizing, and destruction. Procedures for the declassification or Destruction of Components or Media are contained in AFSSI 5020.

6.2. Remanence security is the use of prescribed safeguards and controls to prevent reconstruction or disclosure of sensitive information to persons who do not have the proper clearance or need-to-know for this information. (**NOTE:** "sensitive information," as used in this document, refers to both classified and sensitive but unclassified [SBU] information).

6.3. Writable storage media that retains data after power is removed (nonvolatile) must be protected for the highest classification of information processed or stored on the AIS. Retain classification controls until the media is sanitized or destroyed in an approved manner.

6.4. Air Force policy is to safeguard sensitive data, no matter what the storage or transmittal media. Safeguarding sensitive information in computer memory and storage media is particularly important during routine maintenance, product end of life, and reuse. All Air Force personnel must prevent accidental disclosure of processed or stored sensitive information, especially during system hardware, firmware, or software upgrade or replacement. To do this, they must be knowledgeable of clearing, sanitizing, and destroying procedures and have the tools available to assist them. Contact the WIAO for assistance when in any doubt on proper procedures to be followed in your particular circumstance.

## **7. Transmission of Classified on an Unclassified system:**

7.1. Notify the ISSO of any e-mail message (or any other electronic correspondence) containing classified information which was transmitted over one or more unclassified LANS. The ISSO will then contact the System Administrator (SA) and the Wing COMPUSEC Manager. AFSSI 5020, *Remanence Security*, provides clearing, purging, and declassification guidance, and lists references for Air Force and DoD evaluated products approved for declassifying magnetic media.

7.2. The UCM and SA contact their commander and e-mail originator. Find out who all the addressees of the e-mail are, including their organizations. In addition, request the following information from the e-mail recipients:

7.2.1. Was a hard page copy of the information made? If yes, secure the hard page copy and sanitize the printer IAW AFSSI 5020.

7.2.2. Was the information saved to a system's hard drive or removable magnetic storage media such as a floppy disk? If yes, purge the data from the hard drive or removable storage device. If the storage device is not to be purged immediately, secure it accordingly. Again, identify variances. 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. Recover and then purge the information.

7.2.3. Was the e-mail or information resent to anyone else? If yes, contact the new addressees and SA and restart the cycle. Maintain documentation on all purging (i.e., declassification actions).

7.3. Recovery action should be a team effort. As a minimum, team members should include ISSO, SA, and Network Control Center personnel. Each of these members has expertise and skills to answer questions and provide assistance to SA 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 Management*. Other actions associated with a security incident are the responsibility of the unit security manager (USM). When an incident occurs ensure someone in the affected unit notifies the USM.

## **8. Destruction of Classified Material:**

8.1. All classified material will be destroyed by utilizing an appropriate device depending on the material to be destroyed.

8.1.1. Paper products will be destroyed by an NSA approved cross-cut shredder. The WIAO can provide information about NSA approved shredders.

8.1.2. Three and one-half inch floppy diskettes can be removed from their plastic cover and the "film" destroyed in an approved cross-cut shredder used for paper shredding.

8.1.3. Compact Disks (CDs) can be destroyed in the approved "CD Destroyer" located in the WIAO.

8.1.4. The National Security Agency has facilities for the destruction of other types of media such as: microfiche, film, aluminum disks, computer chips, circuit boards, and magnetic media to

include VHS, BETA, reel-to-reel tapes, tape cartridges, ZIP and hard disks. Contact the WIAO for specific information on disposing of this media.

KENNETH D. SUGGS, Colonel, USAFR  
Commander