



Communications and Information

COMPUTER SECURITY PROCEDURES
FOR STAND-ALONE COMPUTERS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This instruction is available electronically on the HQ AFRC Public Website. To access it, go to the website at: <http://www.afrc.af.mil/afrcpubs/pubs>.

OPR: 446 MSS/SCBN (SMSgt J. Stenklyft) Certified by: 446 AW/CC (Col Thomas Gisler, Jr.)
Pages: 12
Distribution: F

This publication implements AFD 33-2, *Information Protection*, AFI 33-202, *Computer Security*, AFI 33-203, *The Air Force Emission Security*, AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type I*, and Air Force System Security Instruction (AFSSI) 5020, *Remembrance Security*. It provides guidance for the physical and electronic security to all users who process classified information. This is an extension of the Security Awareness, Training, and Education (SATE) Program, which encompasses Communications Security (COMSEC), Computer Security (COMPUSEC), and Emission Security (EMSEC). This instruction applies to all personnel operating stand-alone small computers or word processors, laptop computers, micro computers, intelligent terminals, memory typewriters and/or memory calculators located within the 446th Airlift Wing (446 AW). These devices are referred to as small computers and/or computer systems throughout this instruction.

1. Responsibilities. All personnel operating or having access to computer systems have responsibilities under this instruction and all applicable Air Force instructions.

1.1. Workgroup Area Security Officer (WASO) will:

1.1.1. Ensure that training is provided to all personnel operating small computers.

1.1.2. Ensure that Risk Analysis/Accreditation is completed and approval to operate is obtained from the Designated Approval Authority (DAA) prior to operation.

1.1.3. Forward Fraud, Waste, and Abuse (FW&A) reports, security violations, and virus reports to Wing Information Assurance Office (WIAO).

1.1.4. Perform random walk-through inspections to ensure adherence to this instruction.

1.1.5. Perform random checks of personal computers to ensure only authorized software is being used.

1.1.6. Ensure that passwords are secure. Passwords must contain a mixture of numeric, letters, and special characters and must be at least eight characters and digits long. Passwords must not contain dictionary words or contain portions of the username.

1.1.7. Change administrator logon passwords every 30 days.

1.1.8. Change user logon passwords every 90 days.

1.1.9. As a minimum, ensure that anti-viral signatures are updated every 30 days.

1.1.10. Ensure that no users are granted access to the system unless they have completed authorized Information Protection Awareness Training.

1.2. Individual Users shall:

1.2.1. Ensure that all security requirements for classified and sensitive unclassified information are followed.

1.2.2. Ensure they are fully trained for the computer/software operations to be performed.

1.2.3. Report all suspected incidents of computer FW&A and computer virus infection to your WASO.

1.2.4. Report computer security violations to the Unit COMPUSEC Manager (UCM)/WASO.

1.2.5. Provide appropriate physical security for classified materials and high value computer equipment.

2. General Procedures:

2.1. Classified processing up to and including Secret will be accomplished only on accredited computer systems.

2.2. Classified processing will only be accomplished with the knowledge and approval of the WASO.

2.3. Access to the computer will be controlled during the processing of classified information. Personnel will not be permitted into the building and/or office when classified information is being processed, unless they: a) have a valid security clearance of the same or higher level than that of the information being processed and b) have a valid need-to-know.

- 2.4. The Classified Processing Checklist (see Atch 1) will be completed whenever classified material is being processed. This instruction will be used with the checklist to ensure that classified information is afforded the proper protection.
- 2.5. Each individual must annually certify that they have read, understood, and will comply with these procedures.
- 2.6. Only authorized individuals will operate the system. The annual training certification log may serve as a list of authorized users.
- 2.7. Comply with 446AWI 33-201, *Network Systems Security*. This directive applies to all 446 AW users of unclassified systems having current Designated Approval Authority (DAA).
- 2.8. Processing classified on personally owned computers is prohibited. Processing classified information on a government computer in a location other than for which it is certified is prohibited.
- 2.9. Government software may not be used for processing classified information unless authorized, in writing, by the unit commander. Furthermore, all copyright restrictions and licensing restrictions are followed including de-installation from government computers as required before removal of the software from the office.
- 2.10. Consumption of food and/or beverages is prohibited within three feet of the computer system.
- 2.11. Protect the system as required by AFI 31-209. During periods of use, doors, partitions, cabinets, and other methods may be used to restrict traffic flow. During periods of short absence (less than 30 minutes) shutdown and storage of operational software and data will suffice during unclassified operations. During periods of longer absence the software and data disks should be secured and the system secured behind two locked doors or tie downs used.
- 2.12. All output products and diskettes will be marked as required by appropriate regulations.
- 2.13. Mark output products as required by AFSUPDODR 5400-7, *DOD Freedom of Information Act (FOIA) Program*, for FOUO information, AFI 37-132, *Air Force Privacy Act Program*, for Privacy Act Information, and AFI 31-401, *Information Security Program Management*, for classified information.
- 2.14. Use Standard Forms (SF) 706, **Top Secret ADP Media Classification Label**, 707, **Secret ADP Media Classification Label**, and 708, **Confidential ADP Media Classification Label**, for classified diskettes, SF 711, **ADP Media Data Descriptor Label**, for both unclassified, classified diskettes and Privacy Act information.
- 2.15. If a virus is suspected, stop processing and contact your UCM and/or WASO immediately. **DO NOT TURN THE MACHINE OFF** as this may cause further damage to the system. **DO NOT TRANSFER DISKETTES TO ANOTHER SYSTEM AND CONTINUE**

PROCESSING, this may spread the virus. If a virus is detected, complete an incident report form and forward it to Wing Information Assurance Office (WIAO).

2.16. Classified information may only be processed on systems specifically certified and DAA approved for classified processing.

2.17. Non-mobile and mobile systems in garrison approved for the processing of classified information must not be modified, moved or rearranged in any manner without consulting with the Base EMSEC Manager and subsequently updating the system/facility's accreditation prior to reuse.

2.18. Separate sets of systems and applications software will be maintained for each level of information processed, at least one for classified processing (if authorized) and one for unclassified processing. Processing will be performed in the Dedicated Security Mode using "Periods Processing." By this procedure the classification level of the machine may be changed using the procedures in paragraphs 3 and 4 below.

2.19. Maintain a checklist and log of all classified processing sessions.

3. Modem Usage:

3.1. Unapproved modems will not be used with small computers approved for processing classified information. These classified systems must be connected to approved cryptographic equipment including embedded cryptographic Systems, additional operating instructions for connection/usage are given in paragraph 10.

3.2. NOTE: When systems that are part of a classified network (connected via COMSEC equipment and modems) are used for standalone processing, the user will disconnect or power down the COMSEC device and modem prior to initiating a classified session.

3.3. Modems, for unclassified systems, will not be used in the auto-answer mode (whether by a switch on the modem or software that controls the auto-answer option).

4. System Set-up for Classified Processing:

4.1. Inspect the immediate area and equipment to ensure that unauthorized recording or transmitting devices, coffeepots, phones, etc., have not been placed near the system.

4.2. Make sure all equipment covers are in place. Briefly inspect the equipment for signs of tampering (screws missing, pry marks, scratches). If you find such signs immediately notify your UCM.

4.3. Ensure that anyone who does not have the appropriate clearance and need-to-know is restricted from accessing the system or the information processed. If necessary, lock the doors to control physical access to the system.

4.4. When processing classified information, you should remove all unnecessary unclassified documents, papers, printer ribbons, diskettes, and cartridges from the immediate work area to prevent intermixing of classified and unclassified materials.

4.5. Before processing classified information, check the configuration of the system to ensure that only approved devices are connected. The System Description Sheet identifies the specific system configuration approved for classified use.

4.6. Remove all storage media and remove all power from the system using the master power switch. This ensures that all programs are cleared from memory. Wait at least 30 seconds before turning the power back on.

4.7. If the system is connected to a local area network (LAN), the connections **must be distinctly marked for unclassified processing only and must be disconnected during classified processing sessions**. Identify these disconnect points on the System Layout/ Diagrams.

4.8. Insert the media containing the operating system and program software classified at the approved operational level.

4.9. During operating sessions, use only media classified at the same level as the system's current classification.

4.10. If unclassified software or data diskettes (or classified diskettes of a lower classification than the data processed) are used during classified operations the previously unclassified (or classified) diskettes must be upgraded to the same classification level as the highest classification processed or accessed.

4.11. Replace the unclassified printer ribbon with a ribbon classified to the level of the material to be printed. All ribbons used for printing classified products will be marked, stored in a GSA approved security container, destroyed as classified waste.

4.12. Ensure that the Classified Processing Procedures Checklist (see Atch 1) is reviewed and annotated prior to processing classified information.

5. Classified Processing Procedures. You are responsible for the security of the system!

5.1. Protect the computer and all classified papers, software, etc. at all times.

5.2. Remain constantly aware of other activity within the room. Do not allow unauthorized personnel to approach the system, screen, and/or peripherals.

5.3. **NOTE: Unattended classified processing may only be done when the area is certified for open storage at the same classification level being processed.**

- 5.4. Use classified diskettes and cartridges to process and store all information processed.
- 5.5. Ensure that all diskettes, paper products, residue, etc., to include printer ribbons and classified working papers and waste are properly marked. Protective boxes, sleeves, and covers for classified diskettes will be marked at the same classification level of the disks they contain. Use light-colored labels if the box or sleeve is too dark for these markings to appear. Ensure classification markings on diskettes are visible when the diskette is placed within a protective sleeve.

6. Classified Processing Shut-Down Procedures:

- 6.1. The computer and all peripherals will be powered off, to include pulling the plug from the power source, to prevent residual information from remaining in memory.
- 6.1.1. The printer used to output classified data will be cleared in accordance with AFSSI 5020. **NOTE:** Laser printers will have a minimum of three blank sheets run through them before power is cut-off.
- 6.2. Remove all removable magnetic media from the system.
- 6.2.1. Ensure that any newly classified storage media have been marked as required by AFI 31-401.
- 6.2.2. Hard drives and/or data diskettes that contain or reveal classified information will be marked with the highest classification of the data it contains. These classified drives and/or diskettes will be removed from the computer and stored in the safe to ensure they are properly protected. **NOTE:** These drives and/or diskettes are considered nonvolatile memory devices. Once they have been identified as being classified, they remain classified until physically destroyed in accordance with (IAW) AFSSI 5020. Erasing a file moves a pointer within the file but leaves the data intact. (Programs that recover erased files can be used to retrieve such data).
- 6.3. Remove any remaining output from the printer or plotter, mark it, and store it in a GSA approved security container. Inspect the platen and the plotter bed for any typing or other information that may have extended beyond the paper width. If any information is visible, thoroughly clean the platen or plotter (using an alcohol based cleaner). **NOTE:** The platen is the cylinder behind the paper in letter quality printers, and the long bar behind the paper (where the print head strikes) in dot matrix printers.
- 6.4. Destroy all classified waste including carbons and working papers, IAW applicable directives. **NOTE:** The three blank copies run on the printer will also be treated as classified waste.
- 6.5. Remove all other classified materials, including classified printer ribbons, from the work area and store them IAW DOD 5200.IR/AFI 31-401.

6.6. All working papers and/or drafts will be marked with the highest level of classification they contain and secured or disposed of in accordance with security requirements.

6.7. A final check of the immediate area around the computer, to include desktop and waste can, will be conducted to ensure all classified materials (drives, working papers, drafts, disks) have been secured.

6.8. Ensure the Classified Processing Procedures Checklist (see Atch 1) is completed.

7. Emergency Procedures While Processing Classified Information:

7.1. In case of an emergency requiring immediate evacuation from the facility, such as fire, fire alarm or tornado warning, as time permits, take the appropriate measures to protect classified information.

7.2. The protection of human life takes precedence over the protection of classified materials.
If:

7.2.1. Time permits, ensure emergency notifications are made.

7.2.2. Time permits, turn off power to the equipment.

7.2.3. Time permits, secure the classified material in the safe or maintain control of the material until the emergency condition has been terminated.

7.2.4. Time permits, close and lock the safe if it is open.

7.2.5. Time permits, do a quick final check to ensure all classified materials have been secured or protected before evacuation.

7.2.6. Time permits, quickly gather all classified material including, classified diskettes (floppy and removable hard drive), classified working papers, classified publications, classified printer ribbon, classified printer outputs, STU-III or SECURE DATA DEVICE (SDD) key (if in use), and any other classified material in use.

7.3. When authorized to return, account for all classified materials IAW local procedures. Inspect printer platen and plotter bed at this time. Notify your security manager if classified information is found on these devices. Annotate the checklist and log at this time if secure processing will not resume. **NOTE: The protection of human life takes precedence over the protection of classified materials.**

8. Declassification and Cleaning of Cartridges and Diskettes:

8.1. All classified media must be properly controlled and stored until declassification by one of the following methods or destruction by approved methods and facilities.

8.2. All declassification/clearing software and procedures must be approved by the DAA. The UCM should contact the WIAO for the latest information on the availability of approved declassification software.

8.3. Always destroy, shred or use other authorized methods using approved facilities/equipment for any unnecessary and/or inoperative floppy disks rather than using declassification methods.

8.4. Operative and/or inoperative magnetic hard disks and cartridges may be cleared by degaussing, using a NSA approved degausser and procedures. (The WIAO maintains a list of approved degaussers.) By using approved declassification software and procedures (completely operational equipment only), or by removing the platters and scouring them with steel wool or emery cloth to remove all magnetic material from the disk. (NOTE: This process will result in the destruction of the hard disk or cassette.)

9. Data Transmissions using approved Cryptographic Equipment Operational Requirements:

9.1. Only approved operators (specifically certified on the annual training certification log) will perform data transfer actions with small computer systems connected to STU- III equipment.

9.2. Audit logs of all data transfers (send or receive) will be maintained for one year. This log is in addition to the classified checklist and log required by paragraph 3 above. The log may be classified based upon content, and will include:

9.2.1. Date and time of data transfer.

9.2.2. Classification of the computer system and information to be transferred.

9.2.3. Sender's name, office symbol, and phone number.

9.2.4. Recipient's name, office symbol, and phone number.

9.2.5. Description of material sent [Title, Date-Time-Group (DTG), etc.].

9.3. Verify telephonically the receiving system's DAA accreditation for processing information up to and including the level of information to be transferred. Secure transmissions are only possible when both computer systems are operating at the same classification level.

9.4. Ensure that the computer operating software is classified with the same classification of the data to be transmitted [i.e., use unclassified system software for unclassified data transmissions and classified system software (of at least the classification of the data to be transmitted) for classified transmissions].

9.5. Initiate STU-III secure communications and verify that no media or information to be transferred is classified higher than the classification shown on the STU-III display.

9.6. The auto-answer mode of STU-III operations will not be used.

10. Protection of System from Fraud, Waste, and Abuse (FW&A), Damage, Theft and Tampering:

10.1. The system must be used for official purposes only. This may include Professional Military Education (PME) or other further education if approved, in writing, by the unit commander.

10.2. Report all occurrences of known or suspected FW&A to your UCM or commander.

10.3. **NOTE:** If the system is capable of connecting to the Internet, use **MUST** be limited to official government business. Any unauthorized use of or access to, government systems and/or networks may result in punitive action.

10.4. Turn the system off during non-duty periods or when leaving the system operating environment unattended for extended periods of time (i.e., more than 30 minutes).

10.5. Secure all unclassified media (write-protected system diskettes and media used exclusively during unclassified sessions) in a locked cabinet or desk. This helps prevent media theft, and unauthorized use or misuse of the system and data files.

10.6. Use approved password controlled screen savers or disk-lock software.

10.7. Turn off the system to remove all information from system memory.

10.8. Secure the system with two locked doors or appropriate tie down devices.

10.9. The system(s) must be included (by quantity only) on the SF 701, **Activity Security Checklist**, to be checked at the end of each duty day.

10.10. Fire extinguishers should be located within 50 feet of the system area.

10.11. The system(s) must be equipped with surge suppressers to protect them from damage caused by power surges. (These may be internal or external devices.)

11. Processing Privacy Act Information:

11.1. Do not process personal information (as defined in AFSUPDODR 5400-7) without obtaining proper approval to do so IAW appropriate directives.

11.2. Protect visual displays and printed output containing Privacy Act information from unauthorized viewing. Mark displays and printed output IAW AFI 33-332.

11.3. Use the media declassification procedures described above before releasing or discarding any magnetic media that have processed Privacy Act information.

12. Software Security:

12.1. The WASO will maintain an inventory of all government-purchased/ licensed software. Master copies of operating systems and applications software must be maintained in a safe location for all purchased and/or leased software used on that system. Back-up copies of this software will be used in day to day operations.

12.2. All software must be used within the constraints and limitations of copyright laws and licensing agreements.

12.3. Personal software will not be used on government computers.

12.4. All files/disks identified as critical or that would require more than one (1) day to recover will be backed up at least weekly, and stored in a separate location or safe.

12.5. All storage media will be labeled as required by current regulations.

12.6. Public domain software may be used only if acquired through the Small Computer shop, tested for virus infection and accredited by the DAA.

12.7. Original Master unclassified software disks and supporting documentation will be maintained in by the WASO for all government purchased or licensed software.

13. Laptop Computers:

13.1. Laptop computers will not be used for processing classified information, unless specifically certified and accredited by the DAA for classified processing.

13.2. Laptop computers must receive adequate physical protection at both the prime storage location and the use site.

13.3. Users should maintain the asset under close personal observation while in use.

13.4. Keep the asset under double lock when unattended.

13.5. Only legal, authorized software will be used with laptop computers, copyright restrictions will be followed. Master copies of software will be maintained in the prime office location.

14. Computer Maintenance:

14.1. Modification to the computer (notebooks, printer) to include user-added devices will not be permitted without prior coordination through the 446 MSS/SCBN and 62 CS/SCBS.

14.2. Only authorized personnel will perform maintenance on or make modifications to AF owned computer systems. These personnel will normally be limited to authorized contractor personnel and/or Small Computer shop personnel. All classified and sensitive unclassified

information and diskettes must be removed from the system prior to maintenance. Only unclassified write protected diskettes will be used during maintenance procedures. Use of user/owner diagnostic software is preferred over the use of contractor diagnostic software.

15. Requirement:

15.1. The requirement found in this instruction comes from multiple sources. User should be familiar with this instruction, Air Force instructions, and Air Force Security Systems Instructions (AFSSI) dealing with the operation of small computer. AFI 33-202, AFI 33-203, AFI 33-204, *Information Protection Security Awareness, Training and Education (SATE) Program*, AFI 33-209, AFI 33-212, *Reporting COMSEC Deviations*, AFI 33-229, *Controlled Access Protection*, AFI 33-230, *Information Protection Assessment and Assistance Program*, AFSSI 5020, *Remanence Security*, AFSSI 5024, Volume I, *Certification and Accreditation (C&A)* and Volume II, *The Certifying Officials Handbook*.

THOMAS M. GISLER, JR., Colonel, USAFR
Commander

CLASSIFIED PROCESSING PROCEDURES CHECKLIST							
BEFORE/ AFTER PROCESSING CLASSIFIED	ITEM	INITIAL/ DATE	INITIAL/ DATE	INITIAL/ DATE	INITIAL/ DATE	INITIAL/ DATE	INITIAL/ DATE
Before	Have the posted processing procedures been reviewed?						
Before	Is the computer certification to process classified on-hand and/or posted?						
Before	Has the Commander approved processing of classified data?						
Before	Has the "Classified Processing In Progress" sign been posted on the office door?						
Before	Has the door been locked?						
Before	Have all the window shades been lowered and/or closed?						
Before	Has the list of authorized personnel been checked for user's name?						
Before	Has the computer been set up 3 feet away from all other computer, phones, jacks, radios, etc...?						
Before	Has the HP LaserJet printer been connected so the red signal line (cable) does not touch and/or cross other computer cables, power lines, or telephone cords?						
Before	Has the unclassified hard drive been replaced with classified one from the safe?						
Before	Has the modem card been removed and placed into the carrying case for storage?						
After	Was computer powered off and unplugged from power source when processing was completed?						
After	Was printer properly cleared - three blank sheets run and then turned off?						
After	Were all classified hard drives and disks removed, properly marked and stored in the safe?						
After	Were all working papers and drafts properly marked and stored in safe or destroyed?						
After	Was a final area check (i.e., desktop, waste can, etc.) conducted to ensure all classified materials were proper secured?						

AF FORM 3132, MAY 83 (EF)

PRECEDENCE FORMS WILL BE USED.

GENERAL PURPOSE (11 X 8-1/2")