



**DEPARTMENT OF THE NAVY**  
NAVY RECRUITING DISTRICT, NEW ORLEANS  
400 RUSSELL AVE BLDG 192  
NEW ORLEANS, LOUISIANA 70143-5077

NAVCRUITDISTNOLAINST 5239.1J  
40  
20 Apr 2015

NAVCRUITDIST NEW ORLEANS INSTRUCTION 5239.1J

From: Commanding Officer, Navy Recruiting District New Orleans

Subj: AUTOMATIC DATA PROCESSING (ADP) SECURITY PROGRAM FOR  
NAVY RECRUITING DISTRICT NEW ORLEANS

Ref: (a) OPNAVINST 5239.1C  
(b) SECNAVINST 5239.19  
(c) DoDD 8570.01-M 19

Encl: (1) Microcomputer Standard Operating Procedures  
(2) Personally-Owned Computer Hardware/Software User  
Agreement-NAVCRUIT 5239/6 (Rev 3-08)  
(3) Department of Homeland Security Custody Receipt for  
Personal Property/Property Pass-DHS Form 560-1 (3/05)  
(4) COMNAVCRUITCOM Custody Card for Computers-NAVCRUIT  
5230-6 (Rev. 3-08)  
(5) COMNAVCRUITCOM Custody Card for Monitors-NAVCRUIT  
5230-6 (Rev. 3-08)  
(6) Acceptable Use Policy for NRD New Orleans Information  
Technology Resources

1. Purpose. To establish the Navy Recruiting District (NRD) New Orleans ADP Security Program and to issue uniform policies for all information systems, equipment, networks and processed data.

2. Cancellation. NAVCRUITDISTNOLAINST 5239.1H.

3. Background. Reference (a) requires commands to establish and maintain an ADP Security Program to protect ADP assets including hardware, data and communications.

4. Applicability. The policies and procedures in this instruction apply to all District staff, military and civilian personnel.

5. Discussion.

a. The use of ADP systems has proliferated through all levels of command, from centralized mainframe processing to decentralized microcomputer processing. Because of this transition, security concerns have increased dramatically.

Formerly, the implementation of countermeasures to protect the mainframe hardware, software and data was relatively simple. Now, however, use of microcomputers with a variety of configurations, locations and users must be made secure. Additionally, there now exists possible internal employee threats as well as outside hacker threats. Because employees may have unlimited access to government work spaces, possible internal employee threats, whether intentional or unintentional, must be identified and eliminated.

b. This instruction contains policies which, when properly implemented, will prevent ADP security violations and protect government property and information. The implementation of effective policies, systems accreditation and awareness training will serve to safeguard ADP resources against internal and external threats and will make the command less vulnerable to asset loss.

6. Organization and Responsibilities.

a. Commanding Officer (CO), Navy Recruiting District New Orleans. In accordance with reference (a), the CO is the Designated Approval Authority (DAA) for all ADP systems at the District. The CO is ultimately responsible for all activities and functions of the command. Thus, the CO is responsible for ensuring overall implementation of the ADP Security implementation of the ADP Security Program at NRD New Orleans.

b. Department Heads. Department Heads at NRD New Orleans will implement all the policies and regulations prescribed in this instruction.

c. Security Manager. The NRD New Orleans Security Manager is responsible for general oversight of the security program. This includes information and personnel security, physical security and ADP security.

d. Information Systems Security Officer (ISSO). The ISSO is the focal point for ADP security matters. The Commanding Officer, shall designate the ISSO in writing according with reference (a).

e. ADP System Administrator (SYSAD). The SYSAD is the focal point for ADP security for a specific Automated Information System (AIS) or department.

f. Users. All ADP users and their supervisors will familiarize themselves with the contents of this instruction and conform to the Microcomputer Standard Operating Procedures (SOP) in enclosure (1) and Mobile Recruiter Initiative Policy.

g. Supply Officer. The Supply Officer is responsible for receiving and notifying the ISSO and SYSAD of any new ADP equipment.

## 7. Policies and Regulations.

a. Security Incident Reporting. Security incident reporting is an integral part of any ADP security plan. The ADP Security Incident Report, per reference (b), will be used by the ADPSO to record all security incidents within twenty-four hours after the incident discovery.

b. Physical Security. Physical security will be accomplished by complying with the security procedures in reference (a) and enclosure (1) of this instruction and NAVCRUITDISTNOLAINST 5239.4C Paragraph R.

c. Removal of ADP Equipment and Media. Navy employees must obtain written authorization using enclosure (3) from their supervisor in order to remove government owned/leased computer equipment, software, or media from the office environment. Authorized contractors may also remove such equipment with written authorization (copy to the SYSAD). Property passes must accompany the above authorizations.

d. Official Use of ADP Equipment. SECNAVINST 5370.2J prohibits the use of government property for non-official business. Therefore, the use of ADP services for private organizations, private business purposes, games or bowling league standings is prohibited. However, the use of ADP equipment for education or training is permitted if it does not conflict with government use and is approved by the supervisor.

e. Personally-Owned Personal Computers (POPCs). Government work on POPCs, whether at home or in other non-government controlled work spaces and whether in dial-up mode or not, is discouraged but permitted. Supervisors should be conservative in granting permission to perform work on POPCs at home. Any work performed at home on a POPC will be done in accordance with requirements set forth in this instruction. The following regulations also apply in this situation:

(1) Level I data (classified) will not be processed on any POPC regardless of location. Level II data will not be processed off-site.

(2) Government work performed on POPCs must be approved in writing by the employee's supervisor using enclosure (2). This approval must specify what software may be used and caution against copying software for personal use. A copy of enclosure (2) must be kept on file by the ISSO.

(3) Use of POPCs for government work is a privilege. Owners will not be reimbursed for any costs related to the operation or maintenance of POPCs nor may equipment or use thereof, be claimed on income taxes as a business expense. If such equipment is brought to government work spaces, the government will not be liable in the event of damage, loss, or theft.

f. Security Access Control. The Department of Defense Password Management Guideline provides password related guidelines for ADP systems. The practices or equivalent procedures described in this reference will be used for all Level II systems.

g. Reproduction of Copyrighted Software. The copyright laws of the United States extend copyright protection to computer programs. Copyrighted material may not be reproduced without the permission of the copyright owner. Navy personnel (military or civilian) who infringe copyright laws will be liable, as private citizens, for these acts of infringement.

h. Contracting. Navy Recruiting District New Orleans personnel responsible for contracting functions will ensure that the contracts for ADP support comply with references (a) and (c) and the contents of this instruction. Contractors will not be used to conduct risk assessments (RAs), Security Tests and Evaluations (ST&Es), or test contingency plans without written approval from Commander, Naval Data Automation Command.

i. ADP Security Training. The ISSO will attend all training as specified in reference (c). In addition, the ISSOs will receive both general and individual training from their ISSO.

8. Action.

a. Information Systems Security Officer (ISSO) will:

(1) Recommend the assignment of ADPSOs as necessary for assistance.

(2) Advise the Security Manager and DAA of all ADP security matters.

(3) Maintain and recommend changes to the Districts ADP Security Instruction and Plan.

(4) Report security incidents to the DAA through the Security Manager.

(5) Guide and train SYSAD in the implementation of the ADP Security Program and development of SOPs for specific equipment.

(6) Coordinate with the Privacy Act Coordinator to identify Privacy Act data and ensure this data is properly secured.

(7) Coordinate with the Physical Security Officer to identify adequate physical protection for the systems.

(8) Ensure implementation of countermeasures for remote terminals connected to another activity's Automated Information System (AIS).

b. SYSAD. The SYSAD will:

(1) Coordinate with the ADPSO to implement the ADP Security Program.

(2) Develop SOPs for specific ADP equipment and ensure that users are trained in the Microcomputer SOPs (enclosure (1)).

(3) Report ADP security incidents to the ISSO within 24 hours after occurrence.

(4) Review the requests for the use of personally-owned hardware/software using enclosure (2) or use of government equipment off-site using per reference (b).

(5) Provide schedule input to the ISSO upon receipt of new equipment or change of function/location.

(6) Check in/out personnel to issue/delete log on IDs/passwords and to ensure the return of hardware, software and data owned by the Navy.

(7) Maintain and revise, as needed, a list of personnel authorized to use each system. This list shall be used as a department inventory of users and systems.

c. Users. All ADP users and their responsible supervisors will:

(1) Report any destruction, theft, or modification of any hardware, software or data per reference (b).

(2) Conform to the Microcomputer Standard Operating Procedures enclosure (1).

(3) Safeguard personal passwords as "Privacy Act" data.

9. Reports and Forms. The following forms are available from NRD New Orleans ADPSO and SYSAD.

a. Per reference (b), ADP Security Incident Report (SECNAV 5239.19)

NAVCRUITDISTNOLAINST 5239.1J  
20 Apr 2015

- b. Enclosure (3), Request and Approval for Off-Site Computing (DHS FORM 560-1)
- c. Enclosure (4), COMNAVCRUITCOM Custody Card for Computers
- d. Enclosure (5), COMNAVCRUITCOM Custody Card for Monitors

/s/  
C. A. WYNTER

Distribution List:  
Electronic only, via  
<http://www.cnrc.navy.mil/neworleans>

Copy to:  
CONNAVCRUITCOM (Code 73)

**MICROCOMPUTER STANDARD OPERATING PROCEDURES**

1. Introduction.

a. The Department of the Navy (DON) Automated Data Processing (ADP) Security Program, OPNAVINST 5239.1C, requires assurance that security procedures are developed, documented and presented to all users for all ADP systems. The directive was written to comply with that problem.

b. Navy Recruiting Command's microcomputer systems and related assets will be protected in accordance with standard operating procedures (SOP). Security requirements increase in stringency with level of data, mode of operation, type of environment, risk of exposure and costs. The operating procedures in this document will afford adequate protection for all microcomputer systems.

c. Reference made to an Automated Data Processing (ADP) System Security Officer (ADPSSO) in the following SOP manual refer to the immediate person at your activity who is responsible for ADP Security.

2. Policy. Compliance with applicable ADP security regulations is mandatory. Non-compliance with ADP security policy and regulations constitutes a security violation/incident. This includes but is not limited to, compromise of classified information or other data falling within the scope of ADP security (i.e., personal data, contract data, etc.) requiring protection.

3. Access Control.

a. Only properly trained and authorized personnel shall be permitted to use Navy Recruiting microcomputer systems.

b. A list of personnel authorized to use each system shall be maintained by the ISSO and shall be revised periodically to ensure its accuracy.

c. Meaningless character strings will be used for passwords. No persons, places, or things that can be closely identified with a user shall be used. Passwords shall be safeguarded by users.

d. Microcomputers that do not have key locks or software security shall not contain sensitive data.

e. Enclosure (4) COMNAVCRUITCOM Custody Card for Computers will be filled out and signed for each laptop or desktop computer system assigned to a user.

f. Enclosure (5) COMNAVCRUITCOM Custody Card for Monitors will be filled out and signed for each monitor assigned to a user.

#### 4. Operation Procedures.

a. Startup, operation, and shutdown of the systems shall be in accordance with the procedures listed in the system operator's manual.

b. The user shall abide by all proprietary software copyright/licensing agreements. The copyright laws of the United States extend copyright protection to computer programs. Copyrighted material may not be reproduced without the permission of the copyright owner. Navy personnel (Military or civilian) who infringe copyright laws are acting beyond the scope of their government employment and will be liable, as private citizens, for their acts of infringement.

c. Users will log out of systems during non-working hours or when not attended. Systems should only be shutdown when directed by the SYSAD.

d. Unclassified systems are not approved for processing of classified (Level I) data.

e. Individual, off-site use of government-owned, stand-alone microcomputers is permitted by Navy Recruiting District New Orleans. Approval will be granted in accordance with this directive.

f. The use of personally-owned software (POS) is discouraged, but may be approved on a case-by-case basis by the ISSO. The use of POS must benefit the Navy in some respect. If approved, the POS will initially be installed on an isolated system for a test period until the ISSO is able

to ensure that it does not contain a virus. Any data created or used by POS must be in a format readable by Navy standard software (e.g., Microsoft Office Suite). Any data created by POS is the property of the Navy.

g. For accreditation purposes, the ISSO must be notified of any relocation of ADP systems or components. Re-accreditation maybe required if the function or environment changes (i.e., software, users).

h. All military, civilian and contractor personnel have access to Navy Recruiting ADP systems will be required to check in/out with the ADPSO. Personnel who check out will be required to turn in any command-owned hardware, software, or data.

5. Physical Security. Physical security will be implemented in accordance with OPNAVINST 5239.1 series. In addition, the following physical security measures will be taken:

a. Personnel who remain in their immediate workspace may leave their terminal or microcomputer if there is no danger of unauthorized disclosure. Personnel who leave from their workspace must disconnect their terminals from the host by logging out or locking the terminal/system by pulling out the CAC, if connected, and return their microcomputer to the operating system. Printers in use may be left unattended after hours.

b. Working areas shall be secured during non-working hours.

c. All personnel are responsible for maintaining positive control of visitors in the spaces. Any unauthorized visitors in the spaces shall be assisted and escorted.

d. At no time shall computers or peripheral devices be left unattended (locked/unlocked) in vehicles (government/personal) to include the trunk.

6. Environmental Security

a. Mouse's, external disks and similar equipment are considered pilferable minor ADP components. These components must be physically secured after regular working hours and when not in use. Assistance in securing these items may be requested from the ISSO.

b. Major microcomputer components, such as processors, monitors and printers will be secured. Cable locks, locking PC cabinets, or a locked room may be used.

c. Do not operate the system if the temperature is less than 55 degrees or greater than 85 degrees.

d. Do not operate the system if the humidity is less than 50 percent or greater than 80 percent.

e. Do not use alcohol, thinners, or freon to clean disks. Chemical fumes can endanger the magnetic coating.

f. Do not eat, drink, or use any fluids within three feet of the equipment or disks. Spillage may cause damage.

g. The system shall be protected against electrical surges by a surge suppressor.

7. Emergency Procedures.

a. In the event of an evacuation because of fire, bomb threat, or other reason, and when time and safety permit, take the following action:

(1) Level II removable storage media shall be secured in a storage container or drawer.

(2) The microcomputer systems shall be shutdown.

(3) The lights shall be turned off.

(4) The door to the area shall be secured when exiting.

b. In the event of a fire in the immediate area, alarms shall be sounded and evacuation procedures described above shall be followed.

c. If a power outage occurs while the system is in operation, remove any CD's from the drives and turn off the power at the surge suppressor.

d. In case of civil disturbance, such as a potentially violent anti-military demonstration, computer systems shall be secured, even when spaces are occupied.

8. Level II Media Protection. All systems software and data shall be protected from theft and unauthorized access.

a. When listed separately, social security numbers and names are classified as Level III data. When listed together, they are classified as Level II data.

b. All printouts and CD's containing Level II data shall be secured in a locked container (e.g., desk or file cabinet) at the following times:

(1) During non-working hours;

(2) When the system is left unattended;

(3) When the system is being operated by an authorized user without a need to access Level II data.

c. All media (e.g., printouts, removable storage media) containing Level II data shall be marked or which reflect "For Official Use Only and Privacy Act".

9. Virus/Vulnerability. Please refer to reference (b). Notify the SYSAD immediately upon discovery of virus, trojan, worm or other unauthorized program.

<b>PERSONALLY-OWNED COMPUTER HARDWARE/SOFTWARE USER AGREEMENT</b>				
Name:	Code:	Phone Number	Building Number:	Room Number:
Computer Make:	Model:	Serial Number:		
<b>PRIMARY APPLICATION/SOFTWARE</b>				
<p>Rules and responsibilities for non-government personally owned computer hardware and software used for processing Government data:</p> <p>No Classified data is handled, processed, or stored on the personally owned computer.</p> <p>The Government is relieved of any liability for the personally owned computer hardware or software while on the premises.</p> <p>All application programs developed to manipulate or process Government business, financial, property or personal data on this personally owned computer are Government property.</p> <p>I, the owner, certify with my signature below that all Government property and data will be removed and the computer system sanitized prior to permanent removal from the command.</p>				
<p>The undersigned accepts the above responsibilities to use his/her personally owned hardware/software for Government uses. I will turn over the original copy of ownership documents and floppy or compact disks for my hardware/software to the Government for the period in which the hardware/software is in use within the command.</p>				
Owner Signature:			Date:	
<b>DEPARTMENT DIRECTOR</b>				
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved		Owner Signature:	Date:	
<b>ISSO</b>				
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved		Owner Signature:	Date:	
<b>REMOVAL OF PERSONALLY OWNED CERTIFICATION</b>				
<p>I _____, certify that all Government property and data has been removed and the system listed above has been sanitized prior to removal from the command.</p>				
<b>FOR OFFICIAL USE ONLY WHEN FILLED IN</b>				
NAVCRUIT 5239/6 (Rev 3-08)				

DEPARTMENT OF HOMELAND SECURITY <b>CUSTODY RECEIPT FOR PERSONAL PROPERTY/PROPERTY PASS</b>		
DESCRIPTION OF PROPERTY <i>(Include make, model, serial number, barcode number)</i>		
<b>PROPERTY ISSUED TO</b>		
NAME <i>(LAST, FIRST, MI)</i>		ORGANIZATION
BUILDING / ROOM	PHONE NUMBER	E-MAIL ADDRESS
PROPERTY OWNER <i>(Choose Owner from drop-down list)</i>		EXPIRATION DATE
<b>FOR GOVERNMENT-OWNED PROPERTY</b>		
<p>The property recipient will be relieved of accountability for this property by surrendering it to the Property Custodian in exchange for this receipt upon demand, transfer, or separation from the Government. The property must be surrendered to the Department immediately upon request.</p> <p>I understand that I am personally responsible for the property identified above, and that I may be held pecuniarily liable for its loss or damage, unless otherwise relieved of responsibility by Board of Survey action.</p> <p>I understand that the property is FOR OFFICIAL USE ONLY and it may not be transferred except by return to or approval of the issuing official.</p>		
SIGNATURE OF PROPERTY RECIPIENT		DATE
ISSUING OFFICIAL <i>(Typed or Printed Name &amp; Signature)</i>		DATE
PROPERTY MAY BE REMOVED FROM THE PREMISES? YES <i>(Choose YES or NO from drop-down list)</i>  REMOVAL AUTHORIZED/RESTRICTED BY  SIGNATURE OF AUTHORIZING OFFICIAL _____		

DHS Form 560-1 (3/05)

Distribution of Copies:

Original – Issuing Official

Copy 1 – Office of Asset Management/Administrative Services

Copy 2 – Property Recipient

**COMNAVCRUITCOM CUSTODY CARD FOR COMPUTERS**

1. NAVCRUITDIST: NRD New Orleans		2. NAVCRUITSTA: NRD HQ	
3. RECRUITER'S / MEMBER'S NAME:		4. SOCIAL SECURITY NUMBER: (LAST FOUR DIGITS ONLY)	
5. ACCEPTANCE OF CUSTODY:  I, _____, accept custody of the Computer (Name)  _____ assigned to me. I am thoroughly familiar with the (Asset # / Service Tag #)  provisions of NAVCRUIDISTNOLAINST 5239.1J. I understand that by accepting custody, I will be held accountable for the care and safety of the Computer assigned to me. At no time will computers or peripheral devices be left unattended (locked/unlocked n vehicles (GOV/Personal), to include the trunk.  <p style="text-align: center;"><b><u>PRIVACY ACT NOTIFICATION</u></b></p> <b>This document contains information covered under the Privacy Act of 1974, 5 USC 552a and its various implementing regulations and must be protected in accordance with those provisions. You, the recipient/user, are obliged to maintain it in a safe, secure and confidential manner. Re-disclosure without consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality subjects you to application of appropriate sanctions. If you have received this correspondence in error, please notify the sender immediately and destroy any copies you have made.</b>			
6.  _____ (Signature)		7.  _____ (Date)	

NAVCRUIT 5230/6 (Rev. 3-08)

**FOR OFFICIAL USE ONLY WHEN FILLED IN**

Enclosure (4)

**COMNAVCRUITCOM CUSTODY CARD FOR MONITORS**

1. NAVCRUITDIST: NRD New Orleans	2. NAVCRUITSTA: NRD HQ
3. RECRUITER'S / MEMBER'S NAME:	4. SOCIAL SECURITY NUMBER: (LAST FOUR DIGITS ONLY)
5. ACCEPTANCE OF CUSTODY:  I, _____, accept custody of the Monitor (Name)  _____ assigned to me. I am thoroughly familiar with _____ (Asset #)  the provisions of NAVCRUIDISTNOLAINST 5239.1J. I understand that by accepting custody, I will be held accountable for the care and safety of the Computer assigned to me. At no time will computers or peripheral devices be left unattended (locked/unlocked) in vehicles (GOV/Personal), to include the trunk.	
<p style="text-align: center;"><b><u>PRIVACY ACT NOTIFICATION</u></b></p> <p><b>This document contains information covered under the Privacy Act of 1974, 5 USC 552a and its various implementing regulations and must be protected in accordance with those provisions. You, the recipient/user, are obliged to maintain it in a safe, secure and confidential manner. Re-disclosure without consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality subjects you to application of appropriate sanctions. If you have received this correspondence in error, please notify the sender immediately and destroy any copies you have made.</b></p>	
6.  _____ (Signature of Recruiter/Member)	7.  _____ (Date)

NAVCRUIT 5230/6 (Rev. 3-08)

**FOR OFFICIAL USE ONLY WHEN FILLED IN**

Acceptable Use Policy for Navy Recruiting District New Orleans  
Information Technology Resources

Appropriately controlling access to, and personal use of, Navy IT resources is a leadership issue. Commanders, Commanding Officers, Civilian Leaders, and Officers in Charge (hereafter referred to as Commanding Officers) must engage with their users to ensure IT resources are being utilized in an acceptable manner and in accordance with the below policy. Following this policy and instilling a climate of accountability combined with an effective command training program will enhance productivity, maintain network stability, and support a solid defense-in-depth approach.

You have been issued/assigned government-owned computers and accessories. The use of these computer assets is intended to aid you of your duties as a service member or employee of Navy Recruiting District New Orleans for the United States Navy. There are certain policies that are needed to be followed to ensure proper operation which in turn reduces down time of your computer system if a failure were to occur. Penalties for violation of the rules republished in, and prescribed by, this policy include applicable criminal, civil, and administrative sanctions for current DoD employees, including punishment under the Uniform Code of Military Justice (UCMJ).

All computers are subject to spot inspections and monitoring at all times. Any modification of your computer by yourself or unauthorized personnel is unacceptable. This includes changes in software or hardware. Privately licensed software may not be installed unless permission from the Commanding Officer is obtained in writing. Illegal software can cause failures within the recruiting programs and other associated software, which can impact you and others of their duties. Illegal software applications include: personal Internet access, personal e-mail software, down loaded files or software from the Internet, pornographic material and any other applications.

Information and physical security of your computer is paramount. The replacement of a stolen computer system can be costly. It needs to be understood that you are responsible for your machine. If a computer is stolen and negligence is determined, you can be held liable for the replacement cost.

Also, the information stored inside your computer is of a sensitive nature and falls within Privacy Act guidelines. You should always take steps to guard against unauthorized access to this material. All computers are equipped with password software to prevent illegal entry and to prevent access to sensitive information. At no time will MRI computers be left unattended (locked/unlocked) in vehicles (GOV/Personal), to include the trunk.\_\_\_\_

Your computer has been provided with an e-mail capability. Your access will be through Microsoft Outlook by default. However, if you are in possession of a "Mobile Recruiter Initiative" computer (MRI) you will need to access your E-mail through the specified Microsoft Outlook Web Access. These services have been provided to help you function more effectively in your job. Remember that the Navy Recruiting Command server computer is not as large as commercial services. This means large amounts of personal e-mail will bottle neck the system and cause failures for everyone. Although the occasional e-mail note to a friend or a family member is as acceptable as receiving a personal phone call or two at work, abuse of the system will not be tolerated. The same applies to browsing on the Internet. Viewing or downloading pornographic material on the Internet is strictly prohibited. The use of your computer, Internet and e-mail services to manage, maintain, or operate any form of business or profit generating enterprise is strictly prohibited.\_\_\_\_\_

Navy personnel are authorized to access commercial web -based email using Navy IT resources for personal use within the limitations of reference (a), paragraph 5.D and reference (c). Use of commercial email for official business is only permitted when necessary to meet operational requirements in cases where Navy provided email is unavailable. This use must be endorsed by the command Information Assurance Manager (IAM) and approved in advance by the Designated Accrediting Authority (DAA) or the DAA\*s written designee. Users must follow specific guidelines defined in references (e) and (f) and to ensure controlled unclassified information (CUI), including personal identifiable information (PII), and for official use only (FOUO) is safeguarded. Commercial email cannot be authorized to transmit CUI (including PII). To ensure the confidentiality, integrity, availability, and security of Navy IT resources and information, users shall not:

(1) Auto-forward any email from a Navy account to a commercial email account (e.g., .com, .edu, etc.) or (2) Bypass, stress, or test cybersecurity or computer network defense (CND) mechanisms (e.g., firewalls, content filters, proxy servers, anti-virus programs, etc.).

To ensure the confidentiality, integrity, availability, and security of Navy IT resources and information, USERS SHALL NOT:

- (1) Auto-forward any email from a Navy account to a commercial email account (e.g., .com, .edu, etc.); \_\_\_\_\_
- (2) Bypass, stress, or test cybersecurity or computer network defense (CND) mechanisms (e.g., firewalls, content filters, proxy servers, anti-virus programs, etc.); \_\_\_\_\_
- (3) Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource; \_\_\_\_\_
- (4) Relocate or change equipment or the network connectivity of equipment without authorization from the local information assurance (IA) authority; \_\_\_\_\_
- (5) Use personally owned hardware, software, shareware, or public domain software without written authorization from the local IA authority; \_\_\_\_\_
- (6) Upload or download executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the written approval of the local cybersecurity authority; \_\_\_\_\_
- (7) Participate in or contribute to any activity resulting in a disruption or denial of service; \_\_\_\_\_
- (8) Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code; \_\_\_\_\_
- (9) Use Navy IT resources in a way that would reflect adversely on the Navy per reference (c). Such uses include: pornography, chain letter, unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information and PII, and other uses that are incompatible with public service; \_\_\_\_\_
- (10) Place data onto Navy IT resources processing insufficient security controls to protect that data at the required classification (e.g., secret data on unclassified IT asset). \_\_\_\_\_

To ensure the confidentiality, integrity, availability, and security of Navy resources and information, USERS SHALL:

- (1) Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse;

\_\_\_\_\_

- (2) Protect CUI, to include PII, and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information; \_\_\_\_\_
- (3) Protect authenticators (e.g., passwords and personal identification numbers) required for logon authentication at the same classification as the highest classification of the information accessed; \_\_\_\_\_
- (4) Protect authentication tokens (e.g., CAC, alternate logon token, personal identity verification, National Security System tokens) at all times. Authentication tokens shall not be left unattended at any time unless properly secured; \_\_\_\_\_
- (5) Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource; \_\_\_\_\_
- (6) Report all security incidents, including PII breaches, immediately per applicable procedures; \_\_\_\_\_
- (7) Access only that data, controlled information, software, hardware, and firmware for which they are authorized access by their Commanding Officer, have a need-to-know, and have the appropriate security clearance. Assume only those roles and privileges for which the user is authorized; \_\_\_\_\_
- (8) Observe all policies and procedures governing the secure operation and authorized use of a Navy information system; \_\_\_\_\_
- (9) Digitally sign and encrypt email when appropriate per reference (g); \_\_\_\_\_
- (10) Employ sound operations security measures per DoD, DON, Navy, and command directives; \_\_\_\_\_
- (11) Complete all required training needed to gain access to and maintain access to Navy/NRC/NRD computer information systems. To include, but not be limited to, Privacy and Personally Identifiable Information (PII) Awareness Training and DoD Cyber Awareness Challenge. \_\_\_\_\_

System Administrators have the capabilities to monitor computers, e-mail accounts and the locations you have visited on the Internet. Please be aware that any e-mail you transmit or receive can be requested by outside parties under the Freedom of Information Act. Contact the command System Administrators for any questions you may have regarding these policies.

Reference (a) is Department of the Navy (DON) Chief Information Officer (CIO) message on Acceptable use of DON Information Technology Resources. Reference (b) is Chairman of the Joint Chiefs of Staff Instruction 6510.01F, Information Assurance and Support to

Computer Network Defense. Reference (c) is Department of Defense (DoD) 5500.7-R CH7, Joint Ethics Regulation, Sections 2-301 and 10-100. Reference (d) is DoDM 5200.01, DoD Information Security Program Manual. Reference (e) is ALNAV 056/10 that provides Secretary of the Navy (SECNAV) guidance for official posts on internet-based capabilities. Reference (f) is ALNAV 057/10 that provides SECNAV guidance for unofficial posts on internet-based capabilities. Reference (g) provides SECNAV policy on the use of digital signatures and encryption with email.

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
(Print Name: Last, First, Middle) (Member's Signature) (Rank/Rate) (Date)

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
(Witness Signature) (Rank/Rate) (Date)