DEPARTMENT OF THE NAVY
NAVY RECRUITING DISTRICT RICHMOND
411 EAST FRANKLIN STREET
SUITE 101
RICHMOND, VA 23219-2243

NRDRICHINST 5211.1C
Code 10
03 Apr 12

NAVCRUITDIST RICHMOND INSTRUCTION 5211.1C

From: Commanding Officer, Navy Recruiting District Richmond

Subj: NAVY RECRUITING DISTRICT RICHMOND PERSONALLY INDENTIFIABLE INFORMATION AND PRIVACY ACT INFORMATION PROGRAM

Ref: (a) COMNAVCRUITCOMINST 5211.4A
(b) GENADMIN/Policy for Handling Protected Personal Information (PPI) and Privacy Act Training Requirements
(c) HTTP://WWW.PRIVACY.NAVY.MIL
(d) Navy Telecommunications Directive (NTD) 04-07, Use of Removal Storage Media

Encl: (1) Standard Form 701, Activity Security Checklist

1. Purpose. To implement reference (a), to ensure that all NRD Richmond military members, civilian, and contractor employees are made fully aware of their rights and responsibilities under the provisions of the Privacy Act of 1974 (PA).

2. Cancellation. NRDRICHINST 5211.1B

3. Personally Identifiable Information (PII). PII is any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, birth date, home address, home phone number, or biometric records.

4. Rules of Conduct. All Navy Recruiting District (NRD) Richmond personnel shall be familiar with the responsibilities and duties imposed by reference (a) and this instruction.

5. Action.

a. Commanding Officer. The Commanding Officer (CO) will ensure the Privacy Act Coordinator is designated in writing and reference (a) is adhered to throughout NRD Richmond.

b. Privacy Act Coordinator. The NRD Richmond Privacy Act Coordinator responsibilities include but are not limited to:

(1) Oversee the PII throughout NRD Richmond utilizing reference (a) and to provide guidance and training to recruiting personnel to ensure the security of privacy act information.

(2) Provide PII orientation training, per reference (b) and (c), to new command personnel during check-in and refresher training to all personnel.

(3) Ensure specialized, management, and Privacy Act systems of records training is provided to Department Heads and Systems Managers.

c. Department Heads and Division Leading Chief Petty Officers (D-LCPO). Department Head's and D-LCPO responsibilities include but are not limited to:

(1) Complete familiarization and implementation of reference (a).

(2) Ensure all personnel receive quarterly and annual training, per reference (b) and (c), on the proper handling of PII and systems processes.

(3) Upon entering the recruiting stations each day, the responsible recruiter will initial and date enclosure (1), which will be mounted permanently inside the entrance of the recruiting station.

(4) Upon securing the recruiting station each evening, the responsible recruiter will walk through each space to ensure that all spaces are free of any PII. Check all safes, cabinets, and drawers ensuring they are secured and initial and date enclosure (2) prior to exiting the station.

d. Command Duty Officer (CDO). The CDO's responsibilities include but are not limited to:

(1) Walk through each space prior to securing each evening to ensure that all spaces are free of any PII. Check all safes ensuring they are secured, place your initials and time on the Standard Form 701 under the Guard Check column located outside the safe.

(2) Report and document any lost or stolen PII to include laptops or portable storage devices.

6. Safeguarding PII. The PA requires that safeguards be taken to ensure the security and confidentiality of PII contained in paper documents, electronic storage devices, electronic files, and systems of records.

a. Storage. During working hours storage must be so that PII can only be openly viewed by those persons with an official need to know. Spaces in which PII is stored shall have limited access (i.e., locked doors, cabinets or drawers) after working hours.

b. Portable Storage Devices (PSDs). In accordance with reference (c), the use of any PSDs (to include but are not limited to floppy disks, compact discs, USB flash media drives "thumb drives", SD chips, Digital Cameras, or any other non-issued storage media) are strictly prohibited and will not be used under any circumstances.

c. Training Jackets. Training jackets will not contain any social security numbers or any sensitive information about the individual.

d. Transmittal. When transmitting any PII through email or fax, the originator must take every step to properly mark the correspondence so that the receiver of the information is apprised of the need to properly protect the information. When transmitting documents or PSDs with PII, it shall be marked "FOR OFFICIAL USE ONLY (FOUO) - "PRIVACY SENSITIVE". Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

e. Disposal. Per reference (a), PA records must be disposed of by rendering the material unrecognizable or beyond reconstruction. The method for disposal of paper containing PA information is destruction by a cross-cut shredder or local contractor provided by NRD Richmond. Never dispose of paper containing PA information in trash receptacles without first rendering them unrecognizable.

f. Laptop/Desktop Computers

(a) Computers will have the Common Access Card (CAC) removed by the user each time they step away from its proximity.

All computers will be secured each time the recruiter departs for any out of office activity (SOAR, PDC, Interview, MEPS run... etc.) The Laptop will be undocked and the "two-lock rule" should be followed. The "two-lock rule" means the computer should be stored in a drawer or a cabinet with a lock enclosed in a room with a locking entrance door.

(b) In the event that a laptop must be removed from the office, the owner will request permission by completing enclosure (1) and will obtain written approval from their immediate supervisor. If the immediate supervisor is not available, contact the Command Duty Officer or progress further up the chain of the command. Upon returning the laptop to the office, the form must be signed by the supervisor and maintained on file for a period of one year and is subject to inspection.

g. Personal Digital Assistants and Cellular Telephones. Extra caution must be used by personnel who maintain PII on blackberry devices and similar mobile devices to ensure information is properly safeguarded against loss or compromise. These devices must be locked utilizing the keypad before it leaves the station.

h. Transportation and Delivery. The preferred method of transportation and delivery of any PII material is by hand carrying the document. In the event that it is not feasible to hand carry it, it may be mailed; however a signature of acceptance and a return receipt must follow the delivered document.

i. Lost or Stolen PII. In the event that any device containing PII is lost or stolen, you will immediately contact the Command Duty Officer and the Commanding Officer via the Chain of Command.

7. All personnel will ensure to properly store any PII material before they leave their office space. Check if locks are properly working and report to the chain of command on any areas where you do not have proper storage.

Budd Bergloff

B. E. BERGLOFF

Distribution:
NRDRICHINST 5216.1H
List III, V

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)*	FROM *(If required)*	THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate)																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															