



PSCINST 5200.1A

PERSONNEL SERVICE CENTER INSTRUCTION 5200.1A

MAY -7 2015

Subj: POLICY ON PROTECTION OF SENSITIVE AND PERSONALLY IDENTIFIABLE INFORMATION

Ref: (a) Coast Guard Freedom of Information & Privacy Acts Manual, COMDTINST M5260.3
(b) Safeguarding Sensitive But Unclassified (For Official Use Only) Information, DHS MD11042.1
(c) Coast Guard Public Affairs Manual, COMDTINST M5728.2
(d) Coast Guard Security and Information Assurance Manual, COMDTINST M5500.13C, Chapter 5
(e) Privacy Incident Response, Notification, and Reporting Procedures for Personally Identifiable Information (PII), COMDTINST 5260.5

1. **PURPOSE.** This Instruction establishes policy on protection and proper use of sensitive but unclassified (For Official Use Only (FOUO)) information and safeguarding of Personally Identifiable Information (PII) for all Divisions at the Personnel Service Center (PSC).
2. **ACTION.** Personnel assigned to PSC shall familiarize themselves with and follow this directive. All personnel reporting to any Division within PSC shall review and sign the PSC Non-Disclosure Agreement (Enclosure 1). The signed form shall be maintained by each Division Chief where it will be scanned, retained electronically and discarded upon transfer of each member.
3. **DIRECTIVES AFFECTED.** PSCINST 5200.1 is cancelled.
4. **DISCUSSION.** This directive prescribes policy for identification and protection of information compiled and utilized to execute official business at PSC. This policy supplements DHS and Coast Guard policy in references (a) through (e).
5. **CONCEPT.** PSC is a central point of collection, utilization and dissemination of highly sensitive PII and sensitive information for members throughout the Coast Guard. This includes but is not limited to results of boards and panels, e-resumes, service policy changes, medical deliberations, retirement and separation proceedings, personnel records, evaluations, and other information only suitable for viewing by those with a "need to know" in the course of official service business. The loss or misuse of this type of information can result in substantial harm to service personnel and PSC staff shall exercise the utmost professionalism and discretion managing all forms of sensitive information. The information and data, if disclosed to unauthorized sources, could violate the Privacy Act, and/or result in financial loss or adverse legal actions. Certain information may be disclosed under the guidance of the Freedom of Information Act (FOIA), but extreme care shall be taken to ensure any information released is done so according to applicable guidelines.
6. **PRESUMPTION OF FOUO.** PSC staff shall presume the substance of oral, electronic or hardcopy information used for official business are FOUO.

7. CRITICAL INFORMATION LIST. The PSC Critical Information List (CIL) includes all sensitive but unclassified information processed in the conduct of official business. It includes information including or related to:
 - a. PII of any active duty, retired, reserve, civilian, auxiliary or separated Coast Guard member.
 - b. Any information regarding assignments, e-resumes, medical history or determinations, separation, retirements, service history evaluations, discharges, disciplinary proceeding, results or deliberations of boards and panels and service policy changes.
 - c. Any Command investigations, legal deliberations, processes or casework.
 - d. Any layout details, emergency response or security procedures for the PSC Office Spaces outside of released public information.

8. PROTECTION OF CIL INFORMATION. To appropriately protect CIL information PSC personnel shall:
 - a. Only access, or attempt to access, personal information for which access is granted and there is an official "need to know."
 - b. Not divulge password(s) or share them with others for any reason.
 - c. Not disclose any unauthorized data, employee information, or agency specific sensitive but unclassified information which could adversely affect the Coast Guard's interest or privacy to which individuals are entitled.
 - d. Not use, release, or disclose any sensitive but unclassified information in any form whatsoever, to any person or entity other than authorized individuals without authorization from the appropriate chain of command. This stipulation includes premature release of any board or panel results and assignment decision or results.
 - e. Protect PII in accordance with the provisions of the Privacy Act (PA) and other pertinent laws and regulations governing the confidentiality of privileged information, and only release information under established PA and/or FOIA guidelines.
 - f. Review and follow the guidelines for transmitting CIL information over electronic mail from reference (d).
 - g. Review and sign the attached PSC Non-Disclosure Agreement (Enclosure 1).

9. TRANSPORTATION OF SENSITIVE INFORMATION. Due to business imperatives, PSC personnel are permitted to transport PII and Sensitive Information to alternate work locations when authorized in writing by their respective chains of command. The above provisions apply to all Coast Guard information resources whether individually controlled or shared, stand-alone or networked. They apply to all computers and communication facilities owned, leased, operated, or contracted by the Coast Guard. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers and any associated peripherals and software, regardless of whether used for administration, research, or other purposes. To appropriately protect PII/SPII information the following actions shall be completed:

- a. Each Division shall designate a person to track all PII/SPII information being transported.
 - b. Each Division shall designate, in writing, all individuals authorized to transport PII/SPII information. This designation shall be maintained at the Divisional level with the PII/SPII coordinator. A copy shall be sent to the Command Security Officer as well.
 - c. A Divisional “in and out” log shall be maintained via an electronic tracking system or in a log book inclusive of the following information: items being transported, date and time the items were taken and returned, and person(s) name and signature.
 - d. Items must be transported in a lockable rolling tote.
10. **REPORTING.** Any unauthorized use, release or disclosure of non-public information in violation of applicable standards shall be reported in accordance with references (d) and (e). For military members, failure to comply may result in adverse administrative or disciplinary action, including action under the Uniform Code of Military Justice (UCMJ). Additionally, the obligations and prohibitions contained in this policy and references (d) and (e) are also applicable to all civilian employees of the Coast Guard and violations of these policies may serve as grounds for disciplinary or administrative action.
11. **RESPONSIBILITIES.** If you have any questions regarding this policy, please seek guidance from your chain of Command and the Command Security Officer.
12. **DISCLAIMER.** This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance to Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.
13. **ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.**
- a. The development of this directive and the general policies contained within it have been thoroughly reviewed by the originating office and are categorically excluded under current USCG categorical exclusion (CE) #33 from further environmental analysis, in accordance with Section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series).
 - b. This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policies in this Manual must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Council on Environmental Policy NEPA regulations at 40 CFR Parts 1500-1508, DHS and Coast Guard NEPA policy, and compliance with all other environmental mandates.
14. **DISTRIBUTION.** No paper distribution will be made of this Instruction. An electronic version will be location on the following website: <http://www.uscg.mil/psc/hra/pscinst.asp>

15. RECORDS MANAGEMENT CONSIDERATIONS: This Instruction was thoroughly reviewed during the directives clearance process and it was determined there are no further records scheduling requirements in accordance with the Federal Records Act, 44 U.S.C. 3101, et seq., NARA requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not have any significant or substantial change to existing records management requirements.
16. FORMS/REPORTS. PSC Non-Disclosure Agreement (Enclosure 1).
17. REQUEST FOR CHANGES. Units and individuals may recommend changes by writing via the chain of command to: Commander, Coast Guard Personnel Service Center; Mail Stop 7200, 4200 Wilson Blvd, Suite 1100; Arlington, VA 20598-7200.



M. L. AUSTIN
Commander, Personnel Service Center

Encl: (1) PSC Non-Disclosure Agreement



5211

MEMORANDUM

From: PSC (CSO)

To: {Member's Name} _____

Subj: PERSONNEL SERVICE CENTER NON-DISCLOSURE AGREEMENT

Ref: (a) Policy on Protection of Sensitive and Personally Identifiable Information
PSCINST, 5200.1 (series)

1. Personnel Service Center (PSC) is a central point of collection, utilization and dissemination of highly sensitive Personally Identifiable Information (PII) and sensitive information for members throughout the Coast Guard. This includes, but is not limited to results of boards and panels, e-resumes, service policy changes, medical deliberations, retirement and separation proceedings, personnel records, evaluations and other information only suitable for viewing by those with a "need to know" in the course of official service business. The loss or misuse of this type of information can result in substantial harm to service personnel and PSC staff shall exercise the utmost professionalism and discretion managing and transporting all forms of sensitive information.

2. The following terms and conditions apply:

a. Only access, or attempt to access, personal information for which access is granted access authorization, have a "need to know", or require access to the information to perform your duties.

b. Do not disclose any confidential data, employee information, or agency specific sensitive but unclassified information which could adversely affect the Coast Guard's interest or privacy to which individuals are entitled.

c. Do not use, release, or disclose any sensitive but unclassified information in any form to any person or entity other than authorized individuals without authorization.

d. Protect PII in accordance with the provisions of the Privacy Act and other pertinent laws and regulations governing the confidentiality of privileged information. If you become aware of any improper use, release or disclosure of non-public information, you must advise the command as soon as possible.

e. Any unauthorized use, release or disclosure of non-public information in violation of applicable standards may subject you to appropriate adverse actions depending on the severity of the violation.

f. Any transportation of PII outside the workplace shall be logged in your Divisional "in and out" log. Log entries shall include the items that are being transported, date and time the items were taken and returned, your name, and signature.

g. All transported PII items shall be transported in a lockable rolling tote. You should take great care in the safe-keeping and storage of these items.

3. See reference (a) if you have any questions regarding this agreement or seek guidance from your chain of command or PSC's Command Security Officer.

#

I will abide by the guidance provided above: _____
Signature