**DEPARTMENT OF HOMELAND SECURITY**

# U.S. Coast Guard

# AUTOMATED INFORMATION SYSTEMS (AIS) USER ACKNOWLEDGEMENT

**Privacy Act Notice**

**Authority**: 44 U.S.C. 3534.

**Purpose**: To conduct security validation prior to granting users' access to United States Coast Guard (USCG) Information Technology (IT).

**Routine Uses**: USCG commands will use this information to validate users' credentials, and to document and acknowledge user roles and responsibilities. Any external disclosures of data within this record will be made in accordance DHS/ALL-004, General Information Technology Access Account Records, 77 Federal Register 70792, November 27, 2012.

**Disclosure:** Furnishing this information is voluntary; however, failing to provide the information may impede or prevent your access to USCG Information Technology.

## REFERENCES

A. Department of Homeland Security (DHS), Policy Guide and Handbook for Sensitive Systems, Information Systems Management Directive, MD-4300A (series)

B. Department of Defense (DOD), Information Assurance Directive 8500.1 (series)

C. U.S. Coast Guard Security and Information Assurance Manual, COMDTINST M5500.13 (series)

D. Limited Personal Use of Government Office Equipment and Service, COMDTINST 5375.1 (series)

## SYSTEM ACCESS

- I understand that I am given access only to those system(s) for which I am cleared to access, and have a need-to-know to perform my required duties.
- I will not attempt/request access to systems I am not authorized to access.
- I will not attempt to bypass access control measures.
- I will maintain my annual Federal Cyber Awareness Challenge training.
- I understand that I have no expectation of privacy while using any CG equipment or network services.

## PASSWORDS AND OTHER CONTROL MEASURES

- I will choose passwords that meet “strong password” criteria.
- I will protect my passwords and access numbers (e.g., CAC PIN) from disclosure.
- I will shield my keyboard or PED from view as I enter my password.
- I will not share my passwords/PINs with any person(s), including System Administrators, or Supervisors.
- I will promptly change my password or PIN if suspected to be compromised.
- I will not leave my CAC unattended in a card reader.

## DATA PROTECTION

- I will use CG equipment, and not personally owned-equipment to remotely access CG systems and information (with exception of authorized CACRAS).
- I will protect sensitive information from disclosure.
- I will lock my CGSW or laptop computer whenever I am away from my work area.
- I will log off when I leave for the day, and not power down my computer unless otherwise directed.
- I will not process, or store classified information on unclassified CG equipment.
- I will remove and secure all removable media (e.g., CD/DVD, external hard drive, etc.) when not in use.
- If solicited for personal or organizational information, or asked to verify accounts or security settings, I will refrain from providing the information and immediately notify my respective Supervisor Information System Security Officer (ISSO), or the CGCYBER Security Operations Center (C-SOC).
- I will forward all suspicious emails to the CGCYBER Security Operations Center (C-SOC).

## INTERNET AND E-MAIL USE

- I will digitally sign and/or encrypt e-mails in accordance with Reference (A) through (C).
- I understand that auto-forwarding CG e-mail outside of USCG.MIL or DHS.GOV domain is strictly prohibited.

## INAPPROPRIATE USAGE

- I shall not process or store government information on my personal computer, nor shall I print any government information to my home printer.
- I understand that running a personal business of any kind, assisting family members or friends in business endeavors on a Government Furnished Equipment (GFE) or (Services) GFS is strictly prohibited.
- I will not install any unauthorized software on CG equipment.
- I understand that streaming of audio or video, social networking, peer-to-peer networking, software or music piracy, online gaming, webmail, Instant Messaging (IM), and hacking is prohibited.
- I understand that viewing pornographic or other offensive content is strictly prohibited on GFE and networks.

## ACKNOWLEDGEMENT STATEMENT

- I understand that I will be held accountable for my actions while accessing and using CG systems and IT resources.
- I will comply with CG policy regarding personal use of GFE and GFS.
- I will adhere to all security practices at all times, even while teleworking.
- I acknowledge that I have read, understand, and will comply with all terms of this agreement.
- I understand that failure to comply with this agreement could result in punitive or administrative action be taken against me.

## USER INFORMATION

| | |
|---|---|
| Name *(Rank/Grade)(First, Middle, Last)* | Date *(MM/DD/YYYY)* |
| Unit | EMPLID *(if applicable)* |



Reset