Naval Sea Systems Command (NAVSEA)

SeaPort System Rules of Behavior

General User Agreement

The SeaPort System Rules of Behavior included in this agreement delineate the responsibilities and expectations of all individuals with access to the SeaPort information system. All individuals will review and acknowledge these rules prior to being granted access to the SeaPort system.

As a user of SeaPort, I acknowledge my responsibility to conform with the following requirements and conditions.

1) I acknowledge my responsibility to use the SeaPort system only for official business.
2) I understand that the SeaPort system operates at a Controlled Unclassified Information (CUI) level. I will not introduce or process data that the system is not specifically designed to handle as specified by DoDI 5200.48.
3) I understand I am responsible for all actions taken under my account. I will not attempt to "hack" the system or attempt to gain access to data for which I am not specifically authorized.
4) I will not use social media/networking sites in conjunction with my SeaPort access.
5) I will not publish data from SeaPort to any social media/networking sites.
6) I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall:
    a. Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
    b. Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
    c. Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.
    d. Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
    e. Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.
    f. Report all security incidents including PII breaches immediately in accordance with applicable procedures.

g. Access only that data, control information, software, hardware, and firmware for which I am authorized access by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.

h. Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.

i. Digitally sign and encrypt e-mail in accordance with current policies.

j. Employ sound operations security measures in accordance with DOD, DoN, service and command directives.

7) I further understand that, when using Navy IT resources, I shall not:

a. Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g., .com).

b. Bypass, stress, or test Information Assurance (IA) or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).

c. Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.

d. Relocate or change equipment or the network connectivity of equipment without authorization from the Local IA Authority (i.e., person responsible for the overall implementation of IA at the command level).

e. Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.

f. Upload/download executable files (e.g., exe, .com, .vbs, or .bat) onto Navy IT resources without the written approval of the Local IA Authority.

g. Participate in or contribute to any activity resulting in a disruption or denial of service.

h. Write, code, compile, store, transmit, transfer, or Introduce malicious software, programs, or code.

i. Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include pornography, chain letters, 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.

   j. Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret onto Unclassified).

8) I acknowledge my responsibility to conform with the requirements of the SeaPort System Rules of Behavior. I also acknowledge that failure to comply with these policies and procedures may constitute a security violation resulting in denial of access to the SeaPort system, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.

I acknowledge receipt of these Rules of Behavior /General User Agreement, understand my responsibilities, and will comply with these provisions when accessing the SeaPort information system.

Print Name	Date
Signature	Organization