

## Personnel Accountability System (PAS) Acceptable Use Agreement

This document provides guidelines for use of the PAS system. The purpose of these guidelines is to increase awareness of computer security issues and to ensure that all users employ PAS in an efficient, ethical, and lawful manner.

By signing this document, you acknowledge and consent that when you access a Department of Defense (DoD) information systems, you are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

Please **READ each** section. **Sign and date** the document at the bottom. When the Navy Common Access Card Program Management Office (CAC PMO) receives this document with your signature, your application CD will be mailed to your site.

In the text below, "users" refers to all administrators, operators, and processors of PAS systems.

### POLICY STATEMENT

1.	PAS computing systems are unclassified systems. Therefore, classified information may not be processed, entered, or stored on this computing system.
2.	Users are responsible for protecting any information used or stored in the PAS database including sanitizing any documents, equipment, and machine-readable media before releasing outside the DoD.
3.	All users must have a current IA training certificate on file locally.
4.	Users shall not divulge access information (e.g. lists of user accounts).
5.	Users are requested to report any weaknesses in PAS computer security and any incidents of possible misuse or violation of this agreement to the CAC PMO.
6.	Users shall not attempt to access any data or programs contained on PAS systems for which they do not have authorization or explicit consent of the owner of the data/program or the PAS administrator.
7.	Users shall not share their PAS account(s) with anyone. This includes sharing access to the account.
8.	Users shall not purposely engage in activities to: harass other users, degrade the performance of systems, deprive an authorized PAS user access to a PAS resource, circumvent PAS computer security measures, or gain access to a PAS system for which proper authorization has not been given.
9.	Users shall not download, install, or run security programs or utilities which reveal weaknesses in the security of a system unless they have the written permission of the CAC PMO.
10.	At any time, the U.S. Government may inspect and seize data stored on this information system.
11.	This information system must include security measures (e.g., authentication and access controls) to protect U.S. Government interests including securing physical access to PAS equipment during work hours and locking it up in approved containers during non-work hours (DoD 5200.1-R). Include PAS in the local unit's regular security checks (i.e. end-of-day security checks) and keep a detailed log of all visitors that access PAS.
12.	Users are responsible for keeping PAS current with regard to IAVA patches.
13.	Users must set a password protected screensaver on any PAS equipment.
14.	Ensure PAS equipment is plugged into a power source with adequate surge protection when necessary.
15.	Integrate PAS into the local unit's incident response planning and vulnerability management processes.
16.	All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement.

Any noncompliance with these requirements constitutes a security violation and will be reported to the PAS system administrator and/or chain of command and will result in short-term or permanent loss of access to all PAS systems.

**I have read this agreement and I understand, agree and consent to each item.**

<b>Signature</b>	<b>e-mail Address</b>	
<b>Printed Name</b>	<b>Site Name</b>	<b>Date</b>