

## DOC IT Security Evaluation Checklist: End User Responsibilities

A System End User is a DOC federal employee or contractor authorized to use DOC systems and networks to accomplish their official duties. This checklist provides end users with a self-assessment tool, and their supervisors or Contracting Officer's Technical Representatives with a performance evaluation tool, to evaluate the level of compliance with end user's duties as established by the

- *DOC IT Security Program Policy and Minimum Implementation Standards (ITSPP),*
- *DOC Remote Access Policy and Minimum Implementation Standards (RASP), and*
- *DOC Policy on Password Management (PPM).*

<b>This is an assessment of</b> (name/operating unit/office):	
<b>Self Assessment</b>	<b>Assessment Date:</b>
<b>Third Party Evaluation</b>	<b>Assessor</b> (name/title/org.):

Status Codes:    **1** = Not Started    **2** = In Process    **3** = In Place

Performance Levels:

- 1** End user is aware of DOC IT security policies in place
- 2** End user is aware of DOC IT security policies as well as detailed procedures in place
- 3** End user is familiar with DOC IT security policies and detailed procedures and follows them
- 4** End user is familiar with DOC IT security policies and detailed procedures, follows them, and periodically tests his/her compliance (for example, using this checklist evaluation tool)
- 5** End user is familiar with DOC IT security policies and detailed procedures and practices them as part of a fully integrated IT security program

	End User	DOC Policy References	Status	Performance Level
1	Read and understand all applicable training and awareness materials.	ITSPP 2.0.1; 3.13, RASP, PPM		
2	Read and understand all applicable user policies and other rules of behavior regarding use or abuse of operating unit IT resources.	ITSPP 3.6.2, 3.8.2.2, RASP, PPM		
3	Know which systems or parts of systems for which they are directly responsible (printer, desktop, etc.).	ITSPP 2.1.12		
4	Know the sensitivity of the data they handle and taking appropriate measures to protect it.	ITSPP 3.3.1.3; 3.8.2.1, RASP		
5	Report all incidents to the appropriate Computer Incident Response Capability (CIRC) or Computer Incident Response Team (CIRT) in a timely manner.	ITSPP 3.14.2, RASP		
6	Know and abide by all applicable DOC and operating unit policies and procedures.	ITSPP 2.1.12, PPM, RASP		
7	Use and distribute commercial software in accordance with copyright laws and licensing agreements.	ITSPP 3.6.2.10, 3.10.4.1		
8	Know and follow the mandatory practices of DOC and operating unit policy in the creation and management of user passwords.	PPM		
9	Obtain appropriate clearances through OSY before gaining access to national security systems	ITSPP 2.0.1		
10	Protect government data from loss, destruction, compromise, and leakage to unauthorized parties.	RASP		

	<b>End User</b>	<b>DOC Policy References</b>	<b>Status</b>	<b>Performance Level</b>
11	Protect DOC government information, including:	ITSP 3.8.2 and 11(a)-(d)		
	(a) Accurately categorize and label all electronic files, hard copy printouts, and removable media (diskettes and CD-ROMs) as Sensitive but Unclassified (SBU), For Official Use Only (FOUO), U.S. Code Title or Public Law protected data, or national security classification (confidential, secret, top secret, or other designation)	ITSP 3.8.2.1		
	(b) Enable audit logging on workstations and protect the logs	ITSP 3.8.2.1		
	(c) Assign sensitivity levels commensurate with the information to be protected	ITSP 3.8.2.1		
	(d) Make appropriate use of the following: <ul style="list-style-type: none"> <li>– locked media libraries;</li> <li>– operator instructions for handling tampering or other incidents;</li> <li>– read-only safeguards;</li> <li>– least-privilege doctrine for information availability; and</li> <li>– auditing of the safeguards as appropriate.</li> </ul>	ITSP 3.8.2.1		