

Evaluation Checklist: System Owner IT Security Responsibilities

A System Owner is a DOC employee responsible for day-to-day operation, maintenance, and security of IT systems. This checklist provides system owners with a self-assessment tool, and their supervisors with a performance evaluation to, to evaluate the level of compliance with system owner'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)*.

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

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

Performance Levels:

- 1** System owner has comprehensive IT security policies in place
- 2** System owner has comprehensive IT security policies as well as detailed procedures in place
- 3** System owner has comprehensive IT security policies and detailed procedures in place that are fully implemented for the owner's system
- 4** System owner has fully implemented and tested comprehensive IT security policies and detailed procedures in place
- 5** System owner has fully implemented and tested comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

	System Owner Responsibilities	DOC Policy References	Status	Performance Level
1	Include security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management).	ITSPP 2.1.9, 3.3.2.4, RASP, PPM		
2	Ensure the adequate security of data and application software residing on their system(s) by implementing effective controls, including	ITSPP 2.1.9 and 2(a)-2(j)		
	(a) Data integrity (virus & intrusion detection, vulnerability testing)	ITSPP 3.11.2, 3.2.2.2, 3.2.2.3		
	(b) Firewall/router/DMZ configuration and testing	ITSPP 3.16.3.5; 3.16.4.4, 3.16.4.9		
	(c) System audit trails	ITSPP 3.14.11, 3.17.2		
	(d) Physical and environmental security	ITSPP 3.7.2, 3.7.3, 3.7.6		
	(e) Configuration management plans and practices	ITSPP 3.10.1.2, 3.10.3.3		
	(f) Patch management plans	ITSPP 3.10.6		

System Owner Responsibilities		DOC Policy References	Status	Performance Level
2	(g) Password management	PPM		
	(h) Remote access user agreements	RASP		
	(i) Operating system software	ITSP 3.10.2.1		
	(j) Application software	ITSP 3.10.2.2		
3	Determine and implement an appropriate level of security commensurate with the levels of sensitivity;	ITSP 2.1.9, 3.3.1.2, 3.3.1.6		
4	Ensure adequate security for all general support systems and major applications under their responsibility, including	ITSP 2.1.9 and 4(a)-(f)		
	(a) Develop and maintain system security plans that document the security controls, business associations and dependencies of the system	ITSP 3.5.2, RASP		
	(b) Develop, test, and update contingency plans	ITSP 3.9.2		
	(c) Develop and maintain system documentation (e.g., hardware, software, and user manuals)	ITSP 3.11.2, 3.12		
	(d) Establish appropriate rules of behavior for all systems; develop and distribute rules to all system users	ITSP 3.6.2.2		
	(e) Participate in the system certification & accreditation process	ITSP 3.4.0.2, 3.4.0.3, 3.4.1.2		
	(f) Secure web and e-mail servers	ITSP 3.16.6.1, 3.16.6.3		
5	Perform risk assessments of operational systems when significant changes are made to a system as well as at least every three years to periodically re-evaluate the adequacy of system security.	ITSP 2.1.9, 3.1.3, 3.1.4		
6	Conduct self-assessments of system safeguards and program elements and ensure certification and accreditation of the system, including:	ITSP 2.1.9 and 6(a)-(c)		
	(a) Complete annual security self-assessment (NIST SP 800-26) of all systems under their responsibility	ITSP 3.2.1.2		
	(b) Develop corrective action plans (Plans of Action and Milestones, or POAMs)	ITSP 3.2.1.6		
	(c) Develop and execute periodic vulnerability tests of security controls	ITSP 3.2.2.3		
7	Report all incidents to the appropriate Computer Incident Response Capability (CIRC) or Computer Incident Response Team (CIRT) in a timely manner.	ITSP 2.1.9, 3.14.11		

System Owner Responsibilities		DOC Policy References	Status	Performance Level
8	Ensure systems users have proper and relevant IT security training (relevant to the system), including	ITSPP 2.1.9 and 8(a)-(b)		
	(a) System and position-specific specialized IT security training	ITSPP 3.13.9		
	(b) End user IT security training annual refresher	ITSPP 3.13		
9	Ensure IT contracts pertaining to the system include provisions for necessary security.	ITSPP 2.1.9, 3.3.2.3		
10	Ensure adequate security controls are implemented for all systems under his/her control, including:	ITSPP 2.0.1 and 10(a)-(e)		
	(a) Account management -- grant access privileges based on a legitimate need to have system access, and re-evaluate the access privileges annually. The system owner will grant individuals the fewest possible privileges necessary for job performance, and any privileges not specifically granted are denied	3.16.1		
	(b) Segregation of Duties -- separate sensitive positions to preclude any one individual from gaining the opportunity to adversely affect any system.	3.6.3		
	(c) Appoint an Information System Security Officer (ISSO) for large, complex systems that may have a greater need for attention to security than might a small, simple system	ITSPP 2.1.9		
	(d) Identification and authentication procedures	ITSPP 3.15.2, RASP, PPM		
	(e) Cryptography	ITSPP 3.16.7.3		