OPSEC Policy Checklist

OPSEC Policy: An OPSEC policy is set of rules, regulations or guidelines that define an organizations position on how to employ OPSEC. The level of detail is at a very high level and may contain roles, responsibilities, and sometimes consequences on actions relating to OPSEC. In essence, an OPSEC policy is a clear statement of rules employees are to follow.

A useful format for an OPSEC Policy is as follows:

1. Title / Date
2. Subject: Identifies the document (OPSEC Policy).
3. Purpose: To establish OPSEC Policy within an organization, group, or activity.
4. Intent: What is the policy trying to fulfill? Concise statement of the policy.
5. References: List out any supporting references.
6. Definitions: Terms, words, or phrases used in the document.
7. Responsibilities: Who is responsible?
8. Implementation: What happens if policy is not followed?
9. Point of Contact: Listed titles, phone number, and email.
10. Signature: Commander or Organization Senior Leader
11. Tabs, attachments, or appendices? (for threat.. such as HUMINT, SIGINT, OSINT…etc.)

Key points to remember:

1. An OPSEC policy is not an OPSEC program.
2. An OPSEC policy can be part of an OPSEC program.
3. An OPSEC policy alone does not give enough guidance.
4. An OPSEC Policy establishes OPSEC rules.
5. An OPSEC Program organizes efforts used to address a problem.

OPSEC Policy Document Development Checklist			
Action	**YES**	**NO**	**N/A**
1. Does the document have a Title / Number?			
2. Does the document have a publication / release date?			
3. Does the document contain appropriate Subject?			
4. Does it have a "Purpose"? (State the purpose of having an OPSEC Policy)			
5. Does the document contain a Commanders Intent?			
6. Are there any references cited?			
7. Is there a section containing an abbreviations, definitions, or glossary? a. Operations Security (OPSEC) b. Critical Information c. Threat d. Vulnerability e. Risk / Risk Assessment f. Countermeasures g. OPSEC Assessment			
8. Does it reference an established Critical Information List? (What unclassified information needs protection?)			
9. Does it identify high-level responsibilities? a. Commander / Senior Leadership b. Staff sections c. Individual			

Action	YES	NO	N/A
10. Is there an OPSEC Point of Contact (POC) Listed? (Website, office, phone number, email address, etc.) Is there an alternate POC listed?			
11. Has the document been signed by leadership?			
12. Are there any tabs, attachments, or appendices? (Such as for the different threat types… HUMINT, SIGINT, or OSINT…etc.)			
Additional Notes/Comments			