Defence & Security · GS - III

Protection of sensitive military information requires a robust security culture extending beyond technological safeguards. Analyse the importance of the need-to-know principle, personnel accountability and counter-intelligence in safeguarding India's defence preparedness.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 14/11/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Military intelligence, classified information, need-to-know principle, insider threats, operational security, personnel vetting, counter-intelligence, cybersecurity, security audits, institutional accountability.

Model Answer

Introduction

Military information is a critical national security asset. Its unauthorised disclosure can expose operational capabilities, weaken strategic preparedness and provide adversaries with intelligence advantages.

Importance of Security Mechanisms

- **Need-to-know principle:** Restricting access to information according to operational requirements minimises unnecessary exposure.
- **Personnel vetting:** Continuous background verification and security awareness help identify vulnerabilities arising from coercion or manipulation.

- **Counter-intelligence:** Identifying espionage networks and insider threats strengthens institutional protection.
- **Cybersecurity:** Encryption, secure communication and access monitoring protect sensitive digital information.

Institutional Reforms

Defence establishments should conduct periodic security audits, strengthen whistle-blower mechanisms and establish clear accountability for classified-information handling. Regular training can improve personnel awareness of social engineering and foreign intelligence tactics.

Conclusion

Defence security requires an integrated approach combining technology, personnel integrity and institutional vigilance. A strong security culture is essential for protecting India's strategic and operational interests.

BECOME IAS
AI POWERED UPSC PREP