Security Incident Management

Key steps:

1. **Prepare:** maintain an incident response plan with roles, communication trees, and escalation criteria.
2. **Detect and report:** ensure monitoring, logging and clear internal reporting channels.
3. **Classify:** use severity levels (critical, major, minor) and assign appropriate response teams.
4. **Contain and eradicate:** isolate affected systems and remove root causes.
5. **Recover:** restore services from trusted backups and validate integrity.
6. **Post-incident:** perform root-cause analysis, update risk registers, and publish lessons learned.

Revision #1
Created 27 November 2025 09:01:01 by RISA
Updated 27 November 2025 09:02:30 by RISA