SSDLC Training — Checklist

AI-Augmented Coding Safety Checklist

RCI pattern and trust-but-verify workflow

Before Using AI Assistants

- ■ Verify AI tool is on the approved list (Tier 1 or Tier 2)
- ■ Confirm data classification permits AI tool usage for this code
- ■ Telemetry/data sharing settings reviewed and configured
- ■ Repository-level AI policies documented (.aiconfig or AGENTS.md)

RCI Pattern (Review-Correct-Integrate)

- ■ REVIEW: Read all AI-generated code line by line before accepting
- ■ CORRECT: Fix security issues, remove hallucinated APIs, validate logic
- ■ INTEGRATE: Run tests, SAST scan, and code review before merge

Critical Anti-Patterns to Avoid

- ■ Never paste secrets, credentials, or PII into AI prompts
- ■ Never accept AI-generated security logic without expert review
- ■ Never skip tests for AI-generated code (it needs MORE testing, not less)
- ■ Never assume AI output is correct — verify all API calls, imports, logic
- ■ Never use AI-generated regex for security validation without testing
- ■ Never let AI tools access production data or systems