

Checklist

8.25 – Levenscyclus van veilige ontwikkeling

Thema: Technisch | ISO 27002: 8.25 | Gerelateerd: 8.26, 8.27, 8.28

Doelstelling

Aantonen dat informatiebeveiliging is geïntegreerd in de volledige levenscyclus van softwareontwikkeling, van ontwerp tot buiten gebruik stelling.

Secure development beleid

- ☐ Is er beleid voor veilige softwareontwikkeling (Secure SDLC)?
- ☐ Zijn beveiligingseisen verplicht onderdeel van elk ontwikkelproject?
- ☐ Is security by design en privacy by design als principe vastgelegd?
- ☐ Worden ontwikkelaars getraind in veilig programmeren?
- ☐ Is het beleid van toepassing op zowel intern als uitbesteed ontwikkelwerk?

Beveiligingseisen in ontwerp

- ☐ Worden beveiligingseisen vastgesteld in de initiatiefase van een project?
- ☐ Wordt een dreigingsmodellering (threat modeling) uitgevoerd voor nieuwe applicaties?
- ☐ Zijn beveiligingsarchitectuurprincipes (defense in depth, fail secure) toegepast?
- ☐ Worden privacyvereisten (DPIA) meegenomen in het ontwerp?

Veilig coderen en testen

- ☐ Worden secure coding guidelines gehanteerd (OWASP, CWE)?
- ☐ Worden code reviews uitgevoerd met aandacht voor beveiligingskwetsbaarheden?
- ☐ Wordt statische code-analyse (SAST) geautomatiseerd uitgevoerd in de CI/CD-pipeline?
- ☐ Wordt dynamische applicatietesting (DAST) uitgevoerd vóór livegang?
- ☐ Worden dependency-scans (SCA) uitgevoerd op gebruikte bibliotheken?

Acceptatie en buiten gebruik stelling

- ☐ Is beveiliging een formeel acceptatiecriterium vóór livegang?
- ☐ Worden beveiligingsbevindingen uit tests aantoonbaar opgepakt vóór release?

- ☐ Is er een procedure voor het veilig buiten gebruik stellen van applicaties (data-sanitisatie, toegangsintrekking)?
- ☐ Worden lessen op beveiligingsgebied na afronding vastgelegd en gedeeld?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.