

Checklist

5.19 – Informatiebeveiliging in leveranciersrelaties

Thema: Organisatorisch | ISO 27002: 5.19 | Gerelateerd: 5.20, 5.21

Doelstelling

Aantonen dat de organisatie informatiebeveiligingsrisico's van leveranciers beheerst door passende eisen te stellen, contractueel vast te leggen en naleving te monitoren.

Leveranciersbeleid

- ☐ Is er beleid voor informatiebeveiliging in leveranciersrelaties?
- ☐ Worden leveranciers geclassificeerd op basis van hun risicoprofiel en toegang tot informatie?
- ☐ Is het beleid van toepassing op alle leveranciers met toegang tot systemen of data?
- ☐ Worden beveiligingseisen meegenomen in het inkoopproces vóór contractsluiting?

Contractuele eisen

- ☐ Bevatten leverancierscontracten expliciete informatiebeveiligingseisen?
- ☐ Is vastgelegd hoe de leverancier omgaat met vertrouwelijke informatie van de organisatie?
- ☐ Zijn incidentmeldingsverplichtingen (inclusief datalekken) contractueel vastgelegd?
- ☐ Is het recht op audit of inspectie bij de leverancier contractueel verankerd?
- ☐ Zijn AVG-verwerkersovereenkomsten afgesloten met alle relevante leveranciers?

Beoordeling en selectie

- ☐ Worden nieuwe leveranciers beoordeeld op hun beveiligingsvolwassenheid vóór gunning?
- ☐ Worden beveiligingscertificeringen (ISO 27001, SOC 2) meegewogen bij leveranciersselectie?
- ☐ Is er een risicoafweging bij gebruik van leveranciers uit landen buiten de EER?
- ☐ Worden sub-leveranciers (vierde partijen) meegenomen in de beoordeling?

Monitoring en opvolging

- ☐ Worden leveranciers periodiek beoordeeld op naleving van beveiligingseisen?
- ☐ Is er een escalatieproces bij beveiligingsincidenten bij leveranciers?
- ☐ Worden beveiligingsprestaties van leveranciers gerapporteerd aan het management?



Is er een exitstrategie die gegevensverwijdering en toegangsintrekking regelt?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.