

Checklist

5.20 – Informatiebeveiliging in leveranciersovereenkomsten

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

Doelstelling

Aantonen dat overeenkomsten met leveranciers alle relevante informatiebeveiligingseisen bevatten en dat deze eisen aantoonbaar worden nageleefd.

Inhoud van de overeenkomst

- Bevatten leveranciersovereenkomsten een beschrijving van de te leveren diensten en bijbehorende beveiligingseisen?
- Is de classificatie van informatie die de leverancier verwerkt vastgelegd in de overeenkomst?
- Zijn eisen voor toegangsbeveiliging, versleuteling en logging opgenomen?
- Is beschreven hoe de leverancier omgaat met beveiligingsincidenten en datalekken?
- Zijn retentietermijnen en verwijderingsverplichtingen voor data vastgelegd?

Continuïteit en beschikbaarheid

- Zijn SLA's voor beschikbaarheid en hersteltijden (RTO/RPO) vastgelegd?
- Is continuïteitsplanning van de leverancier een contractuele eis?
- Is vastgelegd hoe de leverancier optreedt bij calamiteiten die de dienstverlening raken?
- Worden continuïteitsplannen van leveranciers periodiek getest en gedeeld?

Toezicht en auditrechten

- Heeft de organisatie het recht om audits of inspecties bij de leverancier uit te voeren?
- Kunnen certificeringsrapporten (ISO 27001, SOC 2, ISAE 3402) worden opgevraagd?
- Is de leverancier verplicht wijzigingen in zijn beveiligingsmaatregelen te melden?
- Worden auditbevindingen aantoonbaar opgevolgd door de leverancier?

Beëindiging en overgang

- Is in de overeenkomst geregeld hoe data wordt teruggegeven of vernietigd bij contractbeëindiging?
- Is er een overdrachtsplan voor continuïteit bij wisseling van leverancier?
- Worden toegangsrechten van de leverancier direct ingetrokken na beëindiging?



Is het exitproces getest of doorgelopen bij eerdere leverancierswisselingen?

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