

Checklist

5.2 – Rollen en verantwoordelijkheden voor informatiebeveiliging

Thema: Organisatorisch | ISO 27002: 5.2 | Gerelateerd: 5.1, 5.4

Doelstelling

Aantonen dat rollen en verantwoordelijkheden voor informatiebeveiliging zijn gedefinieerd, toegewezen en gecommuniceerd binnen de organisatie.

Definitie van rollen

- ☐ Zijn rollen en verantwoordelijkheden voor informatiebeveiliging formeel vastgelegd?
- ☐ Is de rol van CISO of vergelijkbare functionaris benoemd en beschreven?
- ☐ Zijn beveiligingsverantwoordelijkheden opgenomen in functiebeschrijvingen?
- ☐ Is duidelijk wie verantwoordelijk is voor de beveiliging van elk informatiesysteem?
- ☐ Is scheiding van functies (segregation of duties) toegepast voor kritieke rollen?

Toewijzing en communicatie

- ☐ Zijn rollen aantoonbaar toegewezen aan specifieke personen of functies?
- ☐ Zijn betrokkenen op de hoogte gesteld van hun beveiligingsverantwoordelijkheden?
- ☐ Worden beveiligingsverantwoordelijkheden meegenomen in onboarding van nieuwe medewerkers?
- ☐ Is er een actueel overzicht van wie welke beveiligingsrol vervult?

Coördinatie en samenwerking

- ☐ Is er overleg of coördinatie tussen beveiligingsrollen en andere disciplines (IT, HR, juridisch)?
- ☐ Is de beveiligingsfunctionaris betrokken bij beslissingen over nieuwe systemen en projecten?
- ☐ Is er afstemming met de functionaris gegevensbescherming (FG/DPO) waar van toepassing?
- ☐ Worden beveiligingsverantwoordelijkheden herzien bij organisatiewijzigingen?

Verantwoording en rapportage

- ☐ Leggen rolhouders aantoonbaar verantwoording af over hun beveiligingstaken?
- ☐ Worden beveiligingsprestaties per rol gerapporteerd aan het management?
- ☐ Is er een escalatieprocedure als een rolhouder zijn verantwoordelijkheden niet kan nakomen?

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