

Checklist

5.4 – Managementverantwoordelijkheden

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

Doelstelling

Aantonen dat het management actief betrokken is bij informatiebeveiliging, de juiste toon zet en medewerkers aanstuurt op naleving van beveiligingsbeleid.

Betrokkenheid van het management

- ☐ Stelt het management voldoende middelen (budget, mensen, tijd) beschikbaar voor informatiebeveiliging?
- ☐ Neemt het management aantoonbaar deel aan beveiligingsbeslissingen en -overleg?
- ☐ Worden beveiligingsrisico's periodiek besproken op managementniveau?
- ☐ Onderschrijft het management het informatiebeveiligingsbeleid aantoonbaar (ondertekening, communicatie)?

Aansturing van medewerkers

- ☐ Zijn leidinggevenden op de hoogte van hun verantwoordelijkheden voor beveiliging binnen hun team?
- ☐ Worden medewerkers door hun leidinggevende aangesproken op naleving van beveiligingsregels?
- ☐ Is beveiliging onderdeel van functioneringsgesprekken of prestatiebeoordelingen?
- ☐ Worden medewerkers die beveiligingsbeleid overtreden hierop aangesproken conform HR-beleid?

Bewustwording en cultuur

- ☐ Geeft het management het goede voorbeeld op het gebied van informatiebeveiliging?
- ☐ Worden beveiligingsbewustwordingscampagnes actief ondersteund door het management?
- ☐ Is er een veiligheidscultuur waarin medewerkers zich vrij voelen incidenten te melden?
- ☐ Wordt beveiliging als strategisch thema behandeld en niet alleen als IT-vraagstuk?

Rapportage en verantwoording

- ☐ Ontvangt het management periodieke rapportages over de beveiligingsstatus?
- ☐ Worden beveiligingsincidenten en risico's tijdig gerapporteerd aan het management?
- ☐ Legt het management verantwoording af over informatiebeveiliging aan het bestuur of toezichthouder?

Verantwoordelijke:

Datum controle:

Afdeling:		Score:	/ 19
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident	Status:	☐ Voldoet ☐ Actiepunt ☐ N.v.t.