

informatiebeveiliging

Doelstelling

Aantonen dat de organisatie een vastgesteld en actueel informatiebeveiligingsbeleid heeft, dat is goedgekeurd door de leiding, gecommuniceerd aan medewerkers en periodiek herzien.

Beleid – aanwezig en vastgesteld

- ☐ Is er een vastgesteld informatiebeveiligingsbeleid aanwezig?
- ☐ Is het beleid formeel goedgekeurd door de leiding (bestuur/directie)?
- ☐ Bevat het beleid de strategische uitgangspunten en randvoorwaarden voor informatiebeveiliging?
- ☐ Beschrijft het beleid de verantwoordelijkheden en rollen voor informatiebeveiliging?
- ☐ Is de samenhang met het algemene beveiligingsbeleid en informatievoorzieningsbeleid beschreven?

Beleid – inhoud en volledigheid

- ☐ Beschrijft het beleid de toewijzing van verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers?
- ☐ Zijn de verantwoordelijkheden en samenhang voor informatiebeveiliging, OT-beveiliging en BCM beschreven?
- ☐ Bevat het beleid doelstellingen of uitgangspunten die meetbaar of toetsbaar zijn?
- ☐ Is het beleid afgestemd op wet- en regelgeving (NIS2, AVG, BIO2)?

CISO – aangesteld en bevoegd

- ☐ Is een CISO aangesteld binnen de organisatie?
- ☐ Is de CISO bevoegd om onafhankelijk te adviseren aan het bestuur/controlerend orgaan?
- ☐ Rapporteert de CISO rechtstreeks over informatiebeveiliging aan het bestuur?

Communicatie en bewustwording

- ☐ Is het beleid beschikbaar en toegankelijk voor alle medewerkers?
- ☐ Zijn medewerkers actief geïnformeerd over het beleid?
- ☐ Volgen bestuurders en medewerkers regelmatig scholing over cyberbeveiligingsrisico's?
- ☐ Tonen bestuurders aantoonbaar kennis van de gevolgen van informatiebeveiligingsrisico's?

Beheer en herziening

- ☐ Wordt het beleid minimaal jaarlijks herzien?
- ☐ Vindt herziening ook plaats na significante wijzigingen (organisatie, wetgeving, incidenten)?
- ☐ Zijn versies en wijzigingen van het beleid gedocumenteerd?
- ☐ Is de datum van laatste herziening en goedkeuring zichtbaar in het document?

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