

Checklist

5.5 – Contact met overheidsinstanties

Thema: Organisatorisch | ISO 27002: 5.5 | Gerelateerd: 5.6, 6.8

Doelstelling

Aantonen dat de organisatie passende contacten onderhoudt met relevante overheidsinstanties en toezichthouders op het gebied van informatiebeveiliging.

Identificatie van relevante instanties

- ☐ Zijn de relevante overheidsinstanties en toezichthouders geïdentificeerd (NCSC, AP, politie, etc.)?
- ☐ Is per instantie vastgelegd wanneer en hoe contact wordt opgenomen?
- ☐ Zijn contactgegevens van relevante instanties actueel en beschikbaar voor betrokkenen?
- ☐ Is vastgelegd wie binnen de organisatie bevoegd is contact op te nemen met overheidsinstanties?

Meldingsverplichtingen

- ☐ Is de organisatie op de hoogte van wettelijke meldingsverplichtingen (AP, NCSC, toezichthouder)?
- ☐ Is er een procedure voor het melden van datalekken aan de Autoriteit Persoonsgegevens (72 uur)?
- ☐ Is er een procedure voor het melden van significante cyberincidenten aan het NCSC (NIS2)?
- ☐ Worden meldingen gedocumenteerd inclusief tijdstip, inhoud en ontvangstbevestiging?

Samenwerking en informatie-uitwisseling

- ☐ Neemt de organisatie deel aan relevante informatie-uitwisselingsnetwerken (ISAC, Z-CERT, etc.)?
- ☐ Worden dreigingsinformatie en waarschuwingen van het NCSC actief gemonitord en opgevolgd?
- ☐ Is er een proces voor opvolging van beveiligingsadviezen van toezichthouders?
- ☐ Worden contacten met overheidsinstanties geregistreerd in een logboek?

Crisiscoördinatie

- ☐ Is er een procedure voor contact met overheidsinstanties tijdens een cybercrisis?
- ☐ Is de woordvoering richting overheid en toezichthouders belegd bij een specifieke functionaris?
- ☐ Zijn afspraken gemaakt over informatie-uitwisseling met politie bij cybercriminaliteit?
- ☐ Worden contactprocedures periodiek geoefend in crisisoefeningen?

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