

Checklist

6.4 – Disciplinaire procedure

Thema: Personeel | ISO 27002: 6.4 | Gerelateerd: 6.3, 6.2

Doelstelling

Aantonen dat de organisatie een formele disciplinaire procedure heeft voor medewerkers die het informatiebeveiligingsbeleid overtreden.

Disciplinair beleid

- ☐ Is er een vastgestelde disciplinaire procedure voor overtredingen van het beveiligingsbeleid?
- ☐ Is de procedure afgestemd op het arbeidsrecht en de cao?
- ☐ Is de procedure gecommuniceerd aan alle medewerkers?
- ☐ Zijn de mogelijke sancties (waarschuwing, schorsing, ontslag) beschreven per type overtreding?
- ☐ Is vastgelegd dat opzettelijke overtredingen zwaarder worden bestraft dan onopzettelijke?

Classificatie van overtredingen

- ☐ Zijn typen beveiligingsovertredingen geclassificeerd naar ernst?
- ☐ Is onderscheid gemaakt tussen nalatigheid, onopzettelijke fouten en opzettelijk wangedrag?
- ☐ Is vastgelegd welke sanctie bij welke ernst van overtreding hoort?
- ☐ Worden herhaalde overtredingen zwaarder gesanctioneerd?

Procedure en eerlijk proces

- ☐ Is er een procedure die een eerlijk onderzoek garandeert vóór sancties worden opgelegd?
- ☐ Heeft de medewerker het recht om zijn/haar standpunt toe te lichten?
- ☐ Is HR betrokken bij het disciplinaire proces?
- ☐ Worden disciplinaire maatregelen gedocumenteerd in het personeelsdossier?

Melden en opvolging

- ☐ Is er een proces voor het melden van beveiligingsovertredingen aan HR en management?
- ☐ Worden beveiligingsovertredingen geregistreerd voor trendanalyse?
- ☐ Is er aandacht voor herstel en verbetering naast sanctionering?



Worden lessen uit disciplinaire gevallen (geanonimiseerd) gebruikt voor bewustwording?

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