

Checklist

8.12 – Voorkomen van gegevenslekken

Thema: Technisch | ISO 27002: 8.12 | Gerelateerd: 5.12, 8.11

Doelstelling

Aantonen dat de organisatie maatregelen heeft genomen om onbedoelde of ongeautoriseerde openbaarmaking van gevoelige informatie te detecteren en te voorkomen.

DLP-beleid en -strategie

- ☐ Is er beleid voor het voorkomen van gegevenslekken (Data Loss Prevention)?
- ☐ Zijn gevoelige gegevenstypen geïdentificeerd die beschermd moeten worden (BSN, financieel, medisch)?
- ☐ Is het DLP-beleid afgestemd op de informatieclassificatie?
- ☐ Zijn verantwoordelijkheden voor DLP belegd bij een eigenaar?

Technische DLP-maatregelen

- ☐ Is DLP-software ingericht op endpoints (laptops, werkstations)?
- ☐ Is DLP ingericht op e-mailgateways om ongewenste verzending van gevoelige data te blokkeren?
- ☐ Is DLP ingericht op webgateways (uploads naar cloudopslag, sociale media)?
- ☐ Worden gegevensoverdrachten naar externe media (USB) gemonitord of geblokkeerd?
- ☐ Zijn DLP-regels gebaseerd op classificatielabels en/of patroonherkenning (regex, vingerafdrukken)?

Monitoring en detectie

- ☐ Worden DLP-overtredingen centraal gelogd en gerapporteerd?
- ☐ Is er een proces voor opvolging van DLP-meldingen?
- ☐ Worden trends in DLP-meldingen geanalyseerd en gerapporteerd aan management?
- ☐ Worden ernstige DLP-incidenten behandeld als beveiligingsincident?

Bewustwording en handhaving

- ☐ Worden medewerkers getraind over gegevenslekken en hun verantwoordelijkheden?
- ☐ Is er een sanctiebeleid bij opzettelijk lekken van gevoelige informatie?
- ☐ Worden DLP-overtredingen consequent opgevolgd en gedocumenteerd?



Is er een procedure voor het melden van vermoedelijke gegevenslekken door medewerkers?

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