

Checklist

5.12 – Classificatie van informatie

Thema: Organisatorisch | ISO 27002: 5.12 | Gerelateerd: 5.13, 5.14

Doelstelling

Aantonen dat informatie wordt geclassificeerd op basis van vertrouwelijkheid, integriteit en beschikbaarheid, zodat passende beveiligingsmaatregelen worden toegepast.

Classificatiebeleid

- ☐ Is er een vastgesteld classificatiebeleid met duidelijke niveaus (bv. openbaar, intern, vertrouwelijk, geheim)?
- ☐ Is het classificatiebeleid afgestemd op wet- en regelgeving (AVG, BIO2, Wob/Woo)?
- ☐ Is het beleid gecommuniceerd aan alle medewerkers die informatie verwerken?
- ☐ Zijn de criteria voor elk classificatieniveau helder en toepasbaar in de praktijk?

Uitvoering van classificatie

- ☐ Wordt alle informatie bij aanmaak of ontvangst geclassificeerd?
- ☐ Is vastgelegd wie verantwoordelijk is voor de classificatie van informatie (eigenaar)?
- ☐ Worden classificaties herzien bij wijziging van het belang of gevoeligheid van informatie?
- ☐ Is de classificatie afgestemd op de BIV-eisen (Beschikbaarheid, Integriteit, Vertrouwelijkheid)?
- ☐ Worden ook e-mails, presentaties en vergaderdocumenten geclassificeerd?

Maatregelen per classificatieniveau

- ☐ Zijn per classificatieniveau de vereiste beveiligingsmaatregelen vastgelegd?
- ☐ Zijn toegangsrechten afgestemd op het classificatieniveau van de informatie?
- ☐ Is versleuteling verplicht voor vertrouwelijke en hogere classificaties?
- ☐ Is vastgelegd hoe informatie per classificatieniveau verstuurd, opgeslagen en vernietigd wordt?

Controle en naleving

- ☐ Worden medewerkers getraind in het classificeren van informatie?
- ☐ Worden classificatiefouten signaleerd en gecorrigeerd?
- ☐ Wordt naleving van het classificatiebeleid periodiek gecontroleerd?



Zijn afwijkingen of incidenten rondom onjuiste classificatie gedocumenteerd?

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