

Checklist

7.1 – Fysieke beveiligingsperimeters

Thema: Fysiek | ISO 27002: 7.1 | Gerelateerd: 7.2, 7.3

Doelstelling

Aantonen dat fysieke beveiligingsperimeters zijn ingericht om informatieverwerkingsfaciliteiten en gevoelige informatie te beschermen tegen ongeautoriseerde fysieke toegang.

Perimeterdefinitie en -ontwerp

- ☐ Zijn fysieke beveiligingsperimeters gedefinieerd voor alle locaties met informatieverwerkingsfaciliteiten?
- ☐ Zijn de grenzen van beveiligde zones duidelijk afgebakend (muren, hekken, deuren)?
- ☐ Is het ontwerp van de perimeter gebaseerd op een risicoanalyse?
- ☐ Zijn kwetsbare ingangen (laadperrons, nooduitgangen) meegenomen in de beveiligingsperimeter?

Toegangscontrole bij de perimeter

- ☐ Zijn toegangspunten tot beveiligde zones uitgerust met toegangscontrolesystemen (badge, pincode, biometrie)?
- ☐ Is toegang tot serverruimten en datacenters beperkt tot geautoriseerde personen?
- ☐ Worden bezoekers geregistreerd en begeleid binnen beveiligde perimeters?
- ☐ Zijn receptie of bewakingsposten aanwezig bij hoofdingangen van gevoelige zones?
- ☐ Worden onbevoegde toegangspogingen geregistreerd en opgevolgd?

Fysieke barrières en detectie

- ☐ Zijn muren, plafonds en vloeren van kritieke ruimten robuust genoeg om ongeautoriseerde toegang te weerstaan?
- ☐ Is inbraakdetectie (alarmsysteem) ingericht op kritieke locaties?
- ☐ Zijn cameratoezicht (CCTV) en opname ingericht bij toegangspunten en kritieke zones?
- ☐ Worden camera-opnames bewaard conform de retentietermijnen en beveiligingseisen?

Onderhoud en controle

- ☐ Worden fysieke beveiligingsmaatregelen periodiek geïnspecteerd en getest?
- ☐ Worden bevindingen uit inspecties gedocumenteerd en verbeterpunten opgevolgd?
- ☐ Worden toegangslogboeken van beveiligde zones periodiek gereviewd?



Is er een procedure voor het melden en opvolgen van fysieke beveiligingsincidenten?

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