M&I/Partners/

NIS2 maatregel uit artikel 21 lid 2	NEN7510-1/NEN7510-2 Maatregel
Artikel 21.2 a	**NEN7510-1:**
Beleid omtrent risicomanagement en de beveiliging van informatiesystemen	**5.2 Beleid**
	6.1.2 Risicobeheersing van informatiebeveiliging
	6.1.3 Behandeling van informatiebeveiligingsrisico's
	8.2 Risicobeoordeling van informatiebeveiliging
	8.3 Informatiebeveiligingsrisico's behandelen
	NEN7510-2:
	5.1.1 Beleidsregels voor informatiebeveiliging
Artikel 21.2 b	**NEN7510-2:**
Incidentbehandeling- en management	16.1.1 Verantwoordelijkheden en procedures
	16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen
	16.1.4 Beoordeling en besluitvorming over informatiebeveiligingsgebeurtenissen
	16.1.5 Respons op informatiebeveiligingsincidenten
	16.1.6 Lering uit informatiebeveiligingsincidenten
	16.1.7 Verzamelen van bewijsmateriaal
Artikel 21.2 c	**NEN7510-2:**
Bedrijfscontinuïteit	17.1.1 Informatiebeveiligingscontinuïteit plannen
	17.1.2 Informatiebeveiligingscontinuïteit implementeren
	12.3.1 Back-up van informatie
	17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten
Artikel 21.2 d	**NEN7510-2:**
Toeleveringsketenbeveiliging	15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties
	15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
	15.1.3 Toeleveringsketen van informatie- en communicatietechnologie
	15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers.
Artikel 21.2 e	**NEN7510-2:**
	8.1.2 Inventariseren van bedrijfsmiddelen

Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen	12.1.1 Gedocumenteerd bedieningsprocedures
	12.6.1 Beheer van technische kwetsbaarheden
	13.1.1 Beheersmaatregelen voor netwerken
	13.1.2 Beveiliging van netwerkdiensten
Artikel 21.2 f	**NEN7510-1:**
Beleid en procedures omtrent het aantonen van de effectiviteit van maatregelen tegen informatieveiligheidsrisico's	9.1 Monitoren, meten, analyseren en evalueren
	9.2 interen Audit
	9.3 Directiebeoordeling
	NEN7510-2:
	18.2.1 Onafhankelijke beoordeling van informatiebeveiliging
Artikel 21.2 g	**NEN7510-1:**
Basis cyberhygiëne en trainingen op het gebied van informatiebeveiliging	7.2 Competentie
	7.3 Bewustzijn
	7.4 Communicatie
	NEN7510-2:
	7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Artikel 21.2 h	**NEN7510-2:**
Beleid en procedures over het gebruik van cryptografie en encryptie	10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen
Artikel 21.2 i	**NEN7510-2:**
Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa	7.1.1 Screening
	7.1.2 Arbeidsvoorwaarden
	7.2.3 Disciplinaire procedure
	7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband
	9.1.1 Beleid voor toegangsbeveiliging
	9.1.1 Registratie en afmelden van gebruikers
	9.2.2 Gebruikers toegang verlenen
	8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen
	8.1.1 Inventariseren van bedrijfsmiddelen
Artikel 21.2 j	**NEN7510-2:**

Het gebruik van multifactor-authenticatie en beveiligde (nood)communicatie	9.4.2 Beveiligde inlogprocedures
	9.3.1 Geheime authenticatie-informatie gebruiken
	9.2.4 Beheer van geheime authenticatie-informatie van gebruikers
Artikel 21.3	**NEN7510-2:**
Procedures voor beveiligd ontwikkelen	12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen.
	14.2.1 Beleid voor beveiligd ontwikkelen
	14.1.1 Analyse en specificatie van informatiebeveiligingseisen
	14.1.2 toepassingen op openbare netwerken beveiligen
	14.1.3 Transacties van toepassingen beschermen
	12.1.2 Wijzigingsbeheer
	14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen
	14.2.5 Principes voor engineering van beveiligde systemen
	14.2.6 Beveiligde ontwikkelomgeving
	14.2.7 Uitbestede softwareontwikkeling
	15.2.8 Testen van systeembeveiliging
	14.2.9 Systeemacceptatiestests
	14.3.1 Bescherming van testgegevens.
Artikel 21.4	**NEN7510-1:**
Passende en proportionele corrigerende maatregelen	10.1 Afwijkingen en corrigerende maatregelen

NIS2 maatregel	Nieuwe maatregelen t.o.v. NEN7510
Registratieplicht	
	Bepaal of de organisatie essentieel of belangrijk is
	Registreer de organisatie bij het NCSC
Governance	
	Alle bestuursleden moeten periodiek trainingen over informatieveiligheid volgen
	Alle bestuursleden moeten aantoonbaar kennis en ervaring hebben op het gebied van informatieveiligheid
	Het bestuur moet actief toezien op de informatieveiligheid in de organisatie (impliciet onderdeel in de NEN7510)
Meldplicht	
	Richt een proces in voor medewerkers om incidenten te melden (zowel cyberincidenten als datalekken)
	Informeer medewerkers binnen de organisatie over het proces om meldingen te maken
	Richt een proces in om meldingen te maken bij de toezichthouder (en de CSIRT)
CSIRT	
	Meld de organisatie aan bij de aangewezen CSIRT voor de sector
	Regel een procedure in om relevante informatie vanuit het CSIRT te internaliseren in de organisatie
	Regel een procedure in om relevante informatie met het CSIRT te delen