

## Bijlage 1 NIS2 maatregelen - NEN 7510

NIS2	NEN 7510
beleid inzake risicoanalyse en beveiliging van informatiesystemen	7510-1 6.1 Maatregelen om risico's te beperken en kansen te benutten 7510-1 8.2 Risicobeoordeling van informatiebeveiliging
incidentenbehandeling	7510-2 16 Beheer van informatiebeveiligingsincidenten
bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer	7510-2 12.3 Back-up - volledig 7510-2 16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen - gedeeltelijke dekking van crisis- en continuïteitsbeheer 7510-2 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer - gedeeltelijke dekking crisis- en continuïteitsbeheer 7510-2 12.1.2 Wijzigingsbeheer - gedeeltelijke dekking crisis- en continuïteitsbeheer
de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners	7510-2 14.2.7 Uitbestede softwareontwikkeling 7510-2 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie
beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden	7510-2 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 7510-2 12.6 Beheer van technische kwetsbaarheden
beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen	7510-1 6.1 Maatregelen om risico's te beperken en kansen te benutten
basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging	7510-2 bevat legio maatregelen, een groot deel waarvan als basispraktijken zouden kunnen worden bestempeld
beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie	7510-2 10 Cryptografie
beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa	7510-2 7 Veilig personeel 7510-2 8 Beheer van bedrijfsmiddelen 7510-2 9 Toegangsbeveiliging
wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit	7510-2 9.4.1 Beperking toegang tot informatie (MFA) 7510-2 9 Toegangsbeveiliging Het tweede gedeelte (spraak, video, tekst) wordt niet in zoveel specifieke woorden gecovered in de 7510. Een deel kan je nog zien onder: 7510-2 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie