ISO/IEC 27001:2017 en NEN 7510-1:2017 maatregelen | versie 1.0			
Clause	**Sectie**	**Naam**	**Van toepassing**
5 Informatiebeveiligingsbeleid	5.1	Aansturing door de directie van de informatiebeveiliging	
	5.1.1	Beleidsregels voor informatiebeveiliging	Ja
	5.1.2	Beoordeling van het informatiebeveiligingsbeleid	Ja
6 Organiseren van informatiebeveiliging	6.1	Interne organisatie	
	6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja
	6.1.2	Scheiding van taken	Ja
	6.1.3	Contact met overheidsinstanties	Ja
	6.1.4	Contact met speciale belangengroepen	Ja
	6.1.5	Informatiebeveiliging in projectbeheer	Ja
	6.2	Mobiele apparatuur en telewerken	
	6.2.1	Beleid voor mobiele apparatuur	Ja
	6.2.2	Telewerken	Ja
7 Veilig personeel	7.1	Voorafgaand aan het dienstverband	
	7.1.1	Screening	Ja
	7.1.2	Arbeidsvoorwaarden	Ja
	7.2	Tijdens het dienstverband	
	7.2.1	Directieverantwoordelijkheden	Ja
	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja
	7.2.3	Disciplinaire procedure	Ja
	7.3	Beëindiging en wijziging van dienstverband	
	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja
8 Beheer van bedrijfsmiddelen	8.1	Verantwoordelijkheid voor bedrijfsmiddelen	
	8.1.1	Inventariseren van bedrijfsmiddelen	Ja
	8.1.2	Eigendom van bedrijfsmiddelen	Ja
	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja
	8.1.4	Teruggeven van bedrijfsmiddelen	Ja
	8.2	Informatieclassificatie	
	8.2.1	Classificatie van informatie	Ja
	8.2.2	Informatie labelen	Ja
	8.2.3	Behandelen van bedrijfsmiddelen	Ja
	8.3	Behandelen van media	
	8.3.1	Beheer van verwijderbare media	Ja
	8.3.2	Verwijderen van media	Ja
	8.3.3	Media fysiek overdragen	Ja
	9.1	Bedrijfseisen voor toegangsbeveiliging	
	9.1.1	Beleid voor toegangsbeveiliging	Ja
	9.1.2	Toegang tot netwerken en netwerkdiensten	Ja

9 Toegangsbeveiliging	9.2	Beheer van toegangsrechten van gebruikers	
	9.2.1	Registratie en afmelden van gebruikers	Ja
	9.2.2	Gebruikers toegang verlenen	Ja
	9.2.3	Beheren van speciale toegangsrechten	Ja
	9.2.4	Beheer van geheime authenticatieinformatie van gebruikers	Ja
	9.2.5	Beoordeling van toegangsrechten van gebruikers	Ja
	9.2.6	Toegangsrechten intrekken of aanpassen	Ja
	9.3	Verantwoordelijkheden van gebruikers	
	9.3.1	Geheime authenticatie-informatie gebruiken	Ja
	9.4	Toegangsbeveiliging van systeem en toepassing	
	9.4.1	Beperking toegang tot informatie	Ja
	9.4.2	Beveiligde inlogprocedures	Ja
	9.4.3	Systeem voor wachtwoordbeheer	Ja
	9.4.4	Speciale systeemhulpmiddelen gebruiken	Ja
	9.4.5	Toegangsbeveiliging op programmabroncode	Ja
10 Cryptografie	10.1	Cryptografische beheersmaatregelen	
	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja
	10.1.2	Sleutelbeheer	Ja
11 Fysieke beveiliging en beveiliging van de omgeving	11.1	Beveiligde gebieden	
	11.1.1	Fysieke beveiligingszone	Ja
	11.1.2	Fysieke toegangsbeveiliging	Ja
	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Ja
	11.1.4	Bescherming tegen bedreigingen van buitenaf	Ja
	11.1.5	Werken in beveiligde gebieden	Ja
	11.1.6	Laad- en loslocatie	Ja
	11.2	Apparatuur	
	11.2.1	Plaatsing en bescherming van apparatuur	Ja
	11.2.2	Nutsvoorzieningen	Ja
	11.2.3	Beveiliging van bekabeling	Ja
	11.2.4	Onderhoud van apparatuur	Ja
	11.2.5	Verwijdering van bedrijfsmiddelen	Ja
	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Ja
	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Ja
	11.2.8	Onbeheerde gebruikersapparatuur	Ja
	11.2.9	‘Clear desk’- en ‘clear screen’-beleid	Ja
	12.1	Bedieningsprocedures en verantwoordelijkheden	
	12.1.1	Gedocumenteerde bedieningsprocedures	Ja
	12.1.2	Wijzigingsbeheer	Ja
	12.1.3	Capaciteitsbeheer	Ja
	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ja

12 Beveiliging bedrijfsvoering	12.2	Bescherming tegen malware	
	12.2.1	Beheersmaatregelen tegen malware	Ja
	12.3	Back-up	
	12.3.1	Back-up van informatie	Ja
	12.4	Verslaglegging en monitoren	
	12.4.1	Gebeurtenissen registreren	Ja
	12.4.2	Beschermen van informatie in logbestanden	Ja
	12.4.3	Logbestanden van beheerders en operators	Ja
	12.4.4	Kloksynchronisatie	Ja
	12.5	Beheersing van operationele software	
	12.5.1	Software installeren op operationele systemen	Ja
	12.6	Beheer van technische kwetsbaarheden	
	12.6.1	Beheer van technische kwetsbaarheden	Ja
	12.6.2	Beperkingen voor het installeren van software	Ja
	12.7	Overwegingen betreffende audits van informatiesystemen	
	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Ja
13 Communicatiebeveiliging	13.1	Beheer van netwerkbeveiliging	
	13.1.1	Beheersmaatregelen voor netwerken	Ja
	13.1.2	Beveiliging van netwerkdiensten	Ja
	13.1.3	Scheiding in netwerken	Ja
	13.2	Informatietransport	
	13.2.1	Beleid en procedures voor informatietransport	Ja
	13.2.2	Overeenkomsten over informatietransport	Ja
	13.2.3	Elektronische berichten	Ja
	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen	14.1	Beveiligingseisen voor informatiesystemen	
	14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Ja
	14.1.2	Toepassingen op openbare netwerken beveiligen	Ja
	14.1.3	Transacties van toepassingen beschermen	Ja
	14.2	Beveiliging in ontwikkelings- en ondersteunende processen	
	14.2.1	Beleid voor beveiligd ontwikkelen	Ja
	14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Ja
	14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Ja
	14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Ja
	14.2.5	Principes voor engineering van beveiligde systemen	Ja
	14.2.6	Beveiligde ontwikkelomgeving	Ja
	14.2.7	Uitbestede softwareontwikkeling	Ja
	14.2.8	Testen van systeembeveiliging	Ja
	14.2.9	Systeemacceptatietests	Ja
	14.3	Testgegevens	
	14.3.1	Bescherming van testgegevens	Ja

15 Leveranciersrelaties	15.1	Informatiebeveiliging in leveranciersrelaties	
	15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja
	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ja
	15.1.3	Toeleveringsketen van informatieen communicatietechnologie	Ja
	15.2	Beheer van dienstverlening van leveranciers	
	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Ja
	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Ja
16 Beheer van informatiebeveiligingsincidenten	16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	
	16.1.1	Verantwoordelijkheden en procedures	Ja
	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Ja
	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Ja
	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Ja
	16.1.5	Respons op informatiebeveiligingsincidenten	Ja
	16.1.6	Lering uit informatiebeveiligingsincidenten	Ja
	16.1.7	Verzamelen van bewijsmateriaal	Ja
17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	17.1	Informatiebeveiligingscontinuïteit	
	17.1.1	Informatiebeveiligingscontinuïteit plannen	Ja
	17.1.2	Informatiebeveiligingscontinuïteit implementeren	Ja
	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja
	17.2	Redundante componenten	
	17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Ja
18 Naleving	18.1	Naleving van wettelijke en contractuele eisen	
	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja
	18.1.2	Intellectuele-eigendomsrechten	Ja
	18.1.3	Beschermen van registraties	Ja
	18.1.4	Privacy en bescherming van persoonsgegevens	Ja
	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja
	18.2	Informatiebeveiligingsbeoordelingen	
	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	Ja
	18.2.2	Naleving van beveiligingsbeleid en -normen	Ja
	18.2.3	Beoordeling van technische naleving	Ja