A.5.1 Beleidsregels voor informatiebeveiliging	Beleidsregels voor cryptografie, Beleidsregels voor gebouwen, ruimten en werkplekken, Beleidsregels voor documenten, Beleidsregels voor softwaretoepassingen, Beleidsregels voor mobiele apparatuur, Beleidsregels voor back-up- en herstel van gegevens, Beleidsregels voor patch- en update, Beleidsregels voor leveranciers(diensten), Beleidsregels voor accounts en authenticatie, Beleidsregels voor rechten en permissies, Beleidsregels voor logging en monitoring, Implementeren van de beleidsregels ad.	Toepassing
A.5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen, verantwoordelijkheden en bevoegdheden	Toepassing
A.5.3 Functiescheiding	Rollen, verantwoordelijkheden en bevoegdheden	Toepassing
A.5.4 Managementverantwoordelijkheden	Rollen, verantwoordelijkheden en bevoegdheden Algemeen IB-beleid	Toepassing
A.5.5 Contact met overheidsinstanties	Overzicht contacten overheidsinstanties	Toepassing
A.5.6 Contact met speciale belangengroepen	Overzicht gespecialiseerde belangengroepen	Toepassing
A.5.7 Informatie en analyses over dreigingen	Overzicht informatiebeveiligingsdreigingen Risicobeoordeling Risicobehandeling (maatregelen) Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.8 Informatiebeveiliging in projectmanagement	Informatiebeveiliging in projectbeheer Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Overzicht relevante bedrijfsmiddelen	Toepassing
A.5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Beleidsregels voor cryptografie, Beleidsregels voor gebouwen, ruimten en werkplekken, Beleidsregels voor documenten Beleidsregels voor softwaretoepassingen Beleidsregels voor mobiele apparatuur, Beleidsregels voor back-up- en herstel van gegevens Beleidsregels voor patch- en update Beleidsregels voor leveranciers(diensten) Beleidsregels voor accounts en authenticatie Beleidsregels voor rechten en permissies Beleidsregels voor logging en monitoring Implementeren van de beleidsregels ad.	Toepassing
A.5.11 Retourneren van bedrijfsmiddelen	Uitgave en inname van bedrijfsmiddelen Personeelsmanagement	Toepassing
A.5.12 Classificeren van informatie	Informatieclassificatie en -labeling	Toepassing
A.5.13 Labelen van informatie	Informatieclassificatie en -labeling	Toepassing
A.5.14 Overdragen van informatie	Beleidsregels voor documenten Beleidsregels voor softwaretoepassingen Beleidsregels voor mobiele apparatuur Beleidsregels voor leveranciers(diensten)	Toepassing
A.5.15 Toegangsbeveiliging	Rollen, verantwoordelijkheden en bevoegdheden Beleidsregels voor accounts en authenticatie Beleidsregels voor rechten en permissies	Toepassing
A.5.16 Identiteitsbeheer	Beheer gebruikersaccounts Beleidsregels voor accounts en authenticatie Beleidsregels voor rechten en permissies	Toepassing

A.5.17 Authenticatie-informatie	Authenticatiebeheer Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.18 Toegangsrechten	Beheer fysieke en logische toegangsrechten tot bedrijfsmiddelen Beleidsregels voor accounts en authenticatie Beleidsregels voor rechten en permissies	Toepassing
A.5.19 Informatiebeveiliging in leveranciersrelaties	Overzicht relevante leveranciersdiensten Beleidsregels voor leveranciers(diensten) Bewaking en beoordeling leveranciersdiensten Screening en selectie van leveranciersdiensten Beëindiging van leveranciersdiensten Leverancierscontractering en -overeenkomsten Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.20 Adresseren van informatiebeveiliging in leveranciersovereen-komsten	Screening en selectie van leveranciersdiensten Leverancierscontractering en -overeenkomsten	Toepassing
A.5.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Beleidsregels voor leveranciers(diensten) Screening en selectie van leveranciersdiensten Leverancierscontractering en -overeenkomsten	Toepassing
A.5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Uitvoeren van de jaarlijkse leveranciersbeoordeling Beëindiging van leveranciersdiensten	Toepassing
A.5.23 Informatiebeveiliging voor het gebruik van clouddiensten	Beleidsregels voor leveranciers(diensten) Screening en selectie van leveranciersdiensten Leverancierscontractering en -overeenkomsten Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.24 Plannen en voorbereiden van het beheer van informatiebeveiligings-incidenten	Overzicht informatiebeveiligingsdreigingen Monitoren, beheren en oplossen van (beveiligings)incidenten	Toepassing
A.5.25 Beoordelen van en besluiten over informatiebeveiligings-gebeurtenissen	Monitoren, beheren en oplossen van (beveiligings)incidenten Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.26 Reageren op informatiebeveiligingsincidenten	Monitoren, beheren en oplossen van (beveiligings)incidenten Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.27 Leren van informatiebeveiligingsincidenten	Monitoren, beheren en oplossen van (beveiligings)incidenten Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.28 Verzamelen van bewijsmateriaal	Monitoren, beheren en oplossen van (beveiligings)incidenten Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.29 Informatiebeveiliging tijdens een verstoring	Beleidsregels voor back-up- en herstel van gegevens Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.30 ICT-gereedheid voor bedrijfscontinuïteit	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.5.31 Wettelijke, statutaire, regelgevende en contractuele eisen	Relevante wet-, en regelgeving en contractuele eisen Stakeholderanalyse Uitvoeren van de jaarlijkse leveranciersbeoordeling Directiebeoordeling	Toepassing
A.5.33 Beschermen van registraties	Beleidsregels voor logging en monitoring Monitoren, beheren en oplossen van (beveiligings)incidenten	Toepassing
A.5.34 Privacy en bescherming van persoonsgegevens	Relevante wet-, en regelgeving en contractuele eisen Stakeholderanalyse Bewustwordingssessies	Toepassing
A.5.35 Onafhankelijke beoordeling van informatiebeveiliging	Contextanalyse Relevante wet-, en regelgeving en contractuele eisen Stakeholderanalyse Toepassingsgebied voor managementsystemen Algemeen IB-beleid	Toepassing

A.5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	Relevante wet-, en regelgeving en contractuele eisen Stakeholderanalyse Verklaring van toepasselijkheid Contextanalyse	Toepassing
A.5.37 Gedocumenteerde bedieningsprocedures	Toegangsprocedure Beleidsregels voor documenten Beleidsregels voor accounts en authenticatie Rollen, verantwoordelijkheden en bevoegdheden, Informatieclassificatie en -labeling	Toepassing
A.6.1 Screening	Werving- en selectieprocedure Personeelsmanagement	Toepassing
A.6.2 Arbeidsovereenkomst	Competentiebeheer Werving- en selectieprocedure Bewustwordingssessies	Toepassing
A.6.3 Bewustwording van, opleiding en training in informatiebeveiliging	Bewustwordingssessies	Toepassing
A.6.4 Disciplinaire procedure	Competentiebeheer Personeelsmanagement	Toepassing
A.6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Personeelsmanagement	Toepassing
A.6.6 Vertrouwelijkheids- of geheimhoudingsover-eenkomsten	Personeelsmanagement Leverancierscontractering en -overeenkomsten	Toepassing
A.6.7 Werken op afstand	Personeelsmanagement Beleidsregels voor gebouwen, ruimten en werkplekken Beleidsregels voor mobiele apparatuur	Toepassing
A.6.8 Melden van informatiebeveiligingsgebeurtenissen	Personeelsmanagement Bewustwordingssessies Monitoren, beheren en oplossen van (beveiligings)incidenten	Toepassing
A.7.1 Fysieke beveiligingszones	Rollen, verantwoordelijkheden en bevoegdheden Toegangsprocedure Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.7.2 Fysieke toegangsbeveiliging	Toegangsprocedure Beleidsregels voor gebouwen, ruimten en werkplekken Beheer fysieke en logische toegangsrechten tot bedrijfsmiddelen	Toepassing
A.7.3 Beveiligen van kantoren, ruimten en faciliteiten	Beleidsregels voor gebouwen, ruimten en werkplekken Toegangsprocedure	Toepassing
A.7.4 Monitoren van de fysieke beveiliging	Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.7.5 Beschermen tegen fysieke en omgevingsdreigingen	Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.7.6 Werken in beveiligde zones	Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.7.7 'Clear desk' en 'clear screen'	Bewustwordingssessies	Toepassing
A.7.8 Plaatsen en beschermen van apparatuur	Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.7.10 Opslagmedia	Bewustwordingssessies Uitgave en inname van bedrijfsmiddelen	Toepassing
A.7.11 Nutsvoorzieningen	Uitvoeren van de jaarlijkse leveranciersbeoordeling Beleidsregels voor back-up- en herstel van gegevens	Toepassing
A.7.12 Beveiligen van bekabeling	Uitvoeren van de jaarlijkse leveranciersbeoordeling Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.7.13 Onderhoud van apparatuur	Overzicht relevante bedrijfsmiddelen Implementeren van de beleidsregels ad. Informatiebeveiliging	Toepassing
A.7.14 Veilig verwijderen of hergebruiken van apparatuur	Implementeren van de beleidsregels ad. Informatiebeveiliging	Toepassing

A.8.1 'User endpoint devices'	Beleidsregels voor mobiele apparatuur Overzicht relevante bedrijfsmiddelen	Toepassing
A.8.2 Speciale toegangsrechten	Algemeen IB-beleid Toegangsprocedure	Toepassing
A.8.3 Beperking toegang tot informatie	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.5 Beveiligde authenticatie	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.6 Capaciteitsbeheer	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.7 Bescherming tegen malware	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.8 Beheer van technische kwetsbaarheden	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.9 Configuratiebeheer	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.10 Wissen van informatie	Beleidsregels voor documenten	Toepassing
A.8.11 Maskeren van gegevens	Beleidsregels voor cryptografie Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.12 Voorkomen van gegevenslekken (data leakage prevention)	Bewustwordingssessies Informatiebeheer	Toepassing
A.8.13 Back-up van informatie	Beleidsregels voor back-up- en herstel van gegevens Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.14 Redundantie van informatieverwerkende faciliteiten	Monitoring en meting Beleidsregels voor logging en monitoring Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.15 Logging	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.16 Monitoren van activiteiten	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.17 Kloksynchronisatie	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.18 Gebruik van speciale systeemhulpmiddelen	Toegangsprocedure Bewustwordingssessies Beleidsregels voor gebouwen, ruimten en werkplekken	Toepassing
A.8.19 Installeren van software op operationele systemen	Beleidsregels voor softwaretoepassingen	Toepassing
A.8.20 Beveiliging netwerkcomponenten	Beleidsregels voor netwerkapparatuur en netwerken Beheer fysieke en logische toegangsrechten tot bedrijfsmiddelen	Toepassing
A.8.21 Beveiliging van netwerkdiensten	Netwerkscheiding Gescheiden netwerkapparatuur en netwerken	Toepassing
A.8.22 Netwerksegmentatie	Gescheiden netwerkapparatuur en netwerken	Toepassing
A.8.23 Toepassen van webfilters	De effectiviteit van de webfilters monitoren	Toepassing
A.8.24 Gebruik van cryptografie	Toepassen van encryptie Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.26 Toepassingsbeveiligingseisen	Overzicht relevante bedrijfsmiddelen	Toepassing
A.8.32 Wijzigingsbeheer	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
A.8.34 Bescherming van informatiesystemen tijdens audits	Uitvoeren van de jaarlijkse leveranciersbeoordeling	Toepassing
Titel	**Maatregelen**	**Verantwoording voor toepasselijkheid**

A.5.32 Intellectuele-eigendomsrechten		Niet van toepassing
A.7.9 Beveiligen van bedrijfsmiddelen buiten het terrein		Niet van toepassing
A.8.4 Toegangsbeveiliging op broncode		Niet van toepassing
A.8.25 Beveiligen tijdens de ontwikkelcyclus		Niet van toepassing
A.8.27 Veilige systeemarchitectuur en technische uitgangspunten		Niet van toepassing
A.8.28 Veilig coderen		Niet van toepassing
A.8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie		Niet van toepassing
A.8.30 Uitbestede systeemontwikkeling		Niet van toepassing
A.8.31 Scheiding van ontwikkel-, test- en productieomgevingen		Niet van toepassing
A.8.33 Testgegevens		Niet van toepassing