Verklaring van toepasselijkheid 2022

Norm	Beheersmaatregel	VvT	Impl.	Wet	Contract	RA/BP	Onderbouwing uitsluiting
A.05.1.1	Ten behoeve van IB moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	j	j		x	x	
A.05.1.2	Het beleid voor IB moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	j	j			x	
A.06.1.1	Alle verantwoordelijkheden bij IB moeten worden gedefinieerd en toegewezen.	j	j			x	
A.06.1.2	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	j	j			x	
A.06.1.3	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	j	j	x		x	
A.06.1.4	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	j	j			x	
A.06.1.5	IB moet aan de orde komen in projectbeheer, ongeacht het soort project.	j	j		x	x	
A.06.2.1	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	j	j	x		x	
A.06.2.2	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	j	j		x		
A.07.1.1	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	j	j			x	
A.07.1.2	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor IB en die van de organisatie vermelden.	j	j	x		x	
A.07.2.1	De directie moet van alle medewerkers en contractanten eisen dat ze IB toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	j	j			x	
A.07.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten	j	j	x	x	x	
A.07.2.3	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te	j	j	x			
A.07.3.1	Verantwoordelijkheden en taken met betrekking tot IB die van kracht blijven na	j	j	x	x	x	
A.08.1.1	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende	j	j	x		x	
A.08.1.2	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een	j	j			x	
A.08.1.3	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die	j	j	x		x	
A.08.1.4	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de	j	j			x	
A.08.2.1	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen,	j	j	x		x	
A.08.2.2	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld	j	j		x	x	
A.08.2.3	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld	j	j			x	
A.08.3.1	Voor het beheren van verwijderbare media moeten procedures worden	j	j		x	x	
A.08.3.2	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet	j	j		x	x	
A.08.3.3	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde	j	j		x	x	
A.09.1.1	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en	j	j		x	x	
A.09.1.2	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten	j	j		x	x	
A.09.2.1	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd	j	j		x	x	
A.09.2.2	Een formele gebruikerstoegangsverleningsprocedure moet worden	j	j		x	x	
A.09.2.3	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden	j	j		x	x	
A.09.2.4	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een	j	j		x		
A.09.2.5	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig	j	j		x	x	
A.09.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie	j	j		x	x	
A.09.3.1	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime	j	j		x	x	
A.09.4.1	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in	j	j		x	x	
A.09.4.2	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	j	j		x	x	
A.09.4.3	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden	j	j		x	x	
A.09.4.4	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen	j	j		x	x	
A.09.4.5	Toegang tot de programmabroncode moet worden beperkt.	j	j			x	
A.10.1.1	Ter bescherming van informatie moet een beleid voor het gebruik van	j	j	x	x	x	
A.10.1.2	Met betrekking tot het gebruik, de bescherming en de levensduur van	j	j		x	x	
A.11.1.1	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te	j	j		x	x	
A.11.1.2	Beveiligde gebieden moeten worden beschermd door passende	j	j		x		
A.11.1.3	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen	j	j		x	x	
A.11.1.4	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke	j	j		x	x	
A.11.1.5	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en	j	j		x	x	
A.11.1.6	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde	j	j		x	x	Simplicate heeft geen laad- en los locatie
A.11.2.1	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen	j	j		x	x	
A.11.2.2	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	j	j	x		x	
A.11.2.3	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die	j	j		x	x	
A.11.2.4	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en	j	j			x	
A.11.2.5	Apparatuur, informatie en software mogen niet van de locatie worden	j	j		x	x	
A.11.2.6	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd,	j	j		x	x	
A.11.2.7	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden	j	j		x	x	
A.11.2.8	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende	j	j		x	x	
A.11.2.9	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare	j	j		x	x	
A.12.1.1	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld	j	j			x	
A.12.1.2	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende	j	j		x	x	
A.12.1.3	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten	j	j		x	x	
A.12.1.4	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het	j	j			x	
A.12.2.1	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie,	j	j		x	x	
A.12.3.1	Regelmatig moeten back-upkopieën van informatie, software en	j	j		x	x	
A.12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en IB-	j	j	x		x	
A.12.4.2	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen	j	j		x	x	
A.12.4.3	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en	j	j		x	x	
A.12.4.4	De klokken van alle relevante informatieverwerkende systemen binnen een	j	j				
A.12.5.1	Om het op operationele systemen installeren van software te beheersen moeten	j	j			x	

Verklaring van toepasselijkheid 2022

Norm	Beheersmaatregel	VvT	Impl.	Wet	Contract	RA/BP	Onderbouwing uitsluiting
A.12.6.1	Informatie over technische kwetsbaarheden van informatiesystemen die worden	j	j		x	x	
A.12.6.2	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	j	j	x		x	
A.12.7.1	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich	j	j	x	x	x	
A.13.1.1	Netwerken moeten worden beheerd en beheerst om informatie in systemen en	j	j			x	
A.13.1.2	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle	j	j		x	x	
A.13.1.3	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken	j	j		x		
A.13.2.1	Ter bescherming van het informatietransport, dat via alle soorten	j	j	x		x	
A.13.2.2	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van	j	j		x		
A.13.2.3	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	j	j		x	x	
A.13.2.4	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de	j	j		x		
A.14.1.1	De eisen die verband houden met IB moeten worden opgenomen in de eisen voor	j	j	x		x	
A.14.1.2	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare	j	j			x	
A.14.1.3	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden	j	j			x	
A.14.2.1	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld	j	j			x	
A.14.2.2	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	j	j		x		
A.14.2.3	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen	j	j	x		x	
A.14.2.4	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot	j	j	x		x	
A.14.2.5	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld,	j	j	x		x	
A.14.2.6	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	j	j			x	
A.14.2.7	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden	j	j			x	
A.14.2.8	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	j	j			x	
A.14.2.9	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma'	j	j		x	x	
A.14.3.1	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	j	j			x	
A.15.1.1	Met de leverancier moeten de IB-eisen om risico's te verlagen die verband houden	j	j			x	
A.15.1.2	Alle relevante IB-eisen moeten worden vastgesteld en overeengekomen met elke	j	j		x	x	
A.15.1.3	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben	j	j		x	x	
A.15.2.1	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren,	j	j			x	
A.15.2.2	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving	j	j			x	
A.16.1.1	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een	j	j	x		x	
A.16.1.2	IB-gebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus					x	
A.16.1.3	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen	j	j			x	
A.16.1.4	IB-gebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of	j	j			x	
A.16.1.5	Op IB-incidenten moet worden gereageerd in overeenstemming met de	j	j			x	
A.16.1.6	Kennis die is verkregen door IB-incidenten te analyseren en op te lossen moet	j	j			x	
A.16.1.7	De organisatie moet procedures definiëren en toepassen voor het identificeren,	j	j	x		x	
A.17.1.1	De organisatie moet haar eisen voor IB en voor de continuïteit van het IB-beheer in	j	j		x	x	
A.17.1.2	De organisatie moet processen, procedures en beheersmaatregelen vaststellen,	j	j		x	x	
A.17.1.3	De organisatie moet de ten behoeve van IB-continuïteit vastgestelde en	j	j		x	x	
A.17.2.1	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden	j	j		x	x	
A.18.1.1	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak	j	j	x		x	
A.18.1.2	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met	j	j	x		x	
A.18.1.3	Registraties moeten in overeenstemming met wettelijke, regelgevende,	j	j	x		x	
A.18.1.4	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	j	j	x	x	x	
A.18.1.5	Cryptografische beheersmaatregelen moeten worden toegepast in	j	j		x	x	
A.18.2.1	De aanpak van de organisatie ten aanzien van het beheer van IB en de	j	j			x	
A.18.2.2	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	j	j			x	
A.18.2.3	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de	j	j			x	