Verklaring van Toepasselijkheid ISO27001:2017

Laposta B.V.

Eigenaar	Directie
Classificatie	OPENBAAR
Versie	2.0
Goedgekeurd op	26-01-2021

De Verklaring van Toepasselijkheid bevat de onderbouwing voor inclusie en exclusie van de Annex A controls.

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A.5.1.1 Beleidsregels voor informatiebeveiliging	**Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.**	JA	Risico Inventarisatie	Wettelijke en contractuele vereisten	Geïmplementeerd
A.5.1.2 Beoordeling van het informatiebeveiligingsbeleid	**Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	**Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.10.1.2 Sleutelbeheer	**Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.1.1 Fysieke beveiligingszone	**Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.1.2 Fysieke toegangsbeveiliging	**Beveiligde gebieden moeten worden beschermd doorpassende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.1.3 Kantoren, ruimten en faciliteiten beveiligen	**Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.1.4 Beschermen tegen bedreigingen van buitenaf	**Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.1.5 Werken in beveiligde gebieden	**Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.11.1.6 Laad- en loslocatie	**Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.11.2.1 Plaatsing en bescherming van apparatuur	**Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.11.2.2 Nutsvoorzieningen	**Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.11.2.3 Beveiliging van bekabeling	**Voeding- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A.11.2.4 Onderhoud van apparatuur	**Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.2.5 Verwijdering van bedrijfsmiddelen	**Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.**	JA	Best practice		Geïmplementeerd
A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	**Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.**	JA	Best practice		Geïmplementeerd
A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur	**Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.**	JA	Risico Inventarisatie		Geïmplementeerd
A.11.2.8 Onbeheerde gebruikersapparatuur	**Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.11.2.9 'Clear desk'- en 'clear screen'- beleid	**Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.12.1.1 Gedocumenteerde bedieningsprocedures	**Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.**	JA	Best practice		Geïmplementeerd
A.12.1.2 Wijzigingsbeheer	**Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, moeten worden beheerst.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.1.3 Capaciteitsbeheer	**Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.1.4 Scheiding van ontwikkel-, testen productieomgevingen	**Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.2.1 Beheersmaatregelen tegen malware	**Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.3.1 Back-up van informatie	**Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.4.1 Gebeurtenissen registreren	**Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.4.2 Beschermen van informatie in logbestanden	**Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.4.3 Logbestanden van beheerders en operators	**Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.4.4 Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	JA	Risico Inventarisatie		Geïmplementeerd
A.12.5.1 Software installeren op operationele systemen	**Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.**	JA	Risico Inventarisatie		Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A.12.6.1 Beheer van technische kwetsbaarheden	**Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt, aan te pakken.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.6.2 Beperkingen voor het installeren van software	**Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.13.1.1 Beheersmaatregelen voor netwerken	**Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.13.1.2 Beveiliging van netwerkdiensten	**Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.**	JA	Best practice		Geïmplementeerd
A.13.1.3 Scheiding in netwerken	**Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.**	JA	Risico Inventarisatie		Geïmplementeerd
A.13.2.1 Beleid en procedures voor informatietransport	**Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.**	JA	Risico Inventarisatie		Geïmplementeerd
A.13.2.2 Overeenkomsten over informatietransport	**Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.13.2.3 Elektronische berichten	**Informatie die is opgenomen in elektronische berichten, moet passend beschermd zijn.**	JA	Risico Inventarisatie		Geïmplementeerd
A.13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst	**Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.1.1 Analyse en specificatie van informatiebeveiligingseisen	**De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.1.2 Toepassingen op openbare netwerken beveiligen	**Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.1.3 Transacties van toepassingen beschermen	**Informatie die deel uitmaakt van transacties van toepassingen, moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.1 Beleid voor beveiligd ontwikkelen	**Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen	**Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.3 Technische beoordeling van toepassingen na wijzigingen besturingsplatform	**Als besturingsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.**	JA	Risico Inventarisatie		Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A.14.2.4 Beperkingen op wijzigingen aan softwarepakketten	**Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.5 Principes voor engineering van beveiligde systemen	**Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.6 Beveiligde ontwikkelomgeving	**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.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.7 Uitbestede softwareontwikkeling	**Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.8 Testen van systeembeveiliging	**Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.2.9 Systeemacceptatietests	**Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.**	JA	Risico Inventarisatie		Geïmplementeerd
A.14.3.1 Bescherming van testgegevens	**Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties	**Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	**Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.**	JA	Risico Inventarisatie		Geïmplementeerd
A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie	**Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.**	JA	Risico Inventarisatie		Geïmplementeerd 10. Uitbestedingsbeleid en leveranciersmanageme
A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	**Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditeren.**	JA	Risico Inventarisatie		Geïmplementeerd
A.15.2.2 Beheer van veranderingen in dienstverlening van leveranciers	**Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.16.1.1 Verantwoordelijkheden en procedures	**Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen	**Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	**Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie, moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.**	JA	Risico Inventarisatie		Geïmplementeerd
A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	**Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.**	JA	Risico Inventarisatie		Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A.16.1.5 Respons op informatiebeveiligingsincidenten	**Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.**	JA	Risico Inventarisatie		Geïmplementeerd
A.16.1.6 Lering uit informatiebeveiligingsincidenten	**Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.16.1.7 Verzamelen van bewijsmateriaal	**De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.17.1.1 Informatiebeveiligingscontinuïteit plannen	**De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.17.1.2 Informatiebeveiligingscontinuïteit implementeren	**De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.**	JA	Risico Inventarisatie		Geïmplementeerd
A.17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	**De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.**	JA	Risico Inventarisatie		Geïmplementeerd
A.17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	JA	Risico Inventarisatie		Geïmplementeerd
A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen	**Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.**	JA	Risico Inventarisatie		Geïmplementeerd
A.18.1.2 Intellectuele-eigendomsrechten	**Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectueleeigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.**	JA	Risico Inventarisatie	Wettelijke en contractuele vereisten	Geïmplementeerd
A.18.1.3 Beschermen van registraties	**Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.**	JA	Risico Inventarisatie	Wettelijke en contractuele vereisten	Geïmplementeerd
A.18.1.4 Privacy en bescherming van persoonsgegevens	**Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante weten regelgeving.**	JA	Risico Inventarisatie	Wettelijke en contractuele vereisten	Geïmplementeerd
A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	**Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.**	JA	Risico Inventarisatie	Wettelijke en contractuele vereisten	Geïmplementeerd
A.18.2.1 Onafhankelijke beoordeling van informatiebeveiliging	**De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging) moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A.18.2.2 Naleving van beveiligingsbeleid en -normen	**Leidinggevenden moeten 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.**	JA	Risico Inventarisatie	Wettelijke en contractuele vereisten	Geïmplementeerd
A.18.2.3 Beoordeling van technische naleving	**Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.**	JA	Risico Inventarisatie		Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	**Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A. 6.1.2 Scheiding van taken	**Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.**	JA	Risico Inventarisatie		Geïmplementeerd 03. Rollen en verantwoordelijkheden competenties
A. 6.1.3 Contact met overheidsinstanties	**Er moeten passende contacten met relevante overheidsinstanties worden onderhouden**	JA	Risico Inventarisatie		Geïmplementeerd 03. Rollen en verantwoordelijkheden competenties
A. 6.1.4 Contact met speciale belangengroepen	**Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 6.1.5 Informatiebeveiliging in projectbeheer	**Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A. 6.2.1 Beleid voor mobiele apparatuur	**Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 6.2.2 Telewerken	**Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 7.1.1 Screening	**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.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 7.1.2 Arbeidsvoorwaarden	**De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 7.2.1 Directieverantwoordelijkheden	**De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.**	JA	Risico Inventarisatie	Best practice	Geïmplementeerd
A. 7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	**Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 7.2.3 Disciplinaire procedure	**Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	**Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.1.1 Inventariseren van bedrijfsmiddelen	**Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.1.2 Eigendom van bedrijfsmiddelen	**Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, moeten een eigenaar hebben.**	JA	Risico Inventarisatie		Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A. 8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen	**Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.1.4 Teruggeven van bedrijfsmiddelen	**Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben, bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.2.1 Classificatie van informatie	**Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.2.2 Informatie labelen	**Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.2.3 Behandelen van bedrijfsmiddelen	**Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.3.1 Beheer van verwijderbare media	**Voor het beheren van verwijderbare media moeten in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.3.2 Verwijderen van media	**Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 8.3.3 Media fysiek overdragen	**Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.1.1 Beleid voor toegangsbeveiliging	**Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.1.2 Toegang tot netwerken en netwerkdiensten	**Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.2.1 Registratie en afmelden van gebruikers	**Een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.2.2 Gebruikers toegang verlenen	**Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.2.3 Beheren van speciale toegangsrechten	**Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerst.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.2.4 Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatieinformatie moet worden beheerst via een formeel beheersproces.	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.2.5 Beoordeling van toegangsrechten van gebruikers	**Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.2.6 Toegangsrechten intrekken of aanpassen	**De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.3.1 Geheime authenticatieinformatie gebruiken	**Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatieinformatie houden aan de praktijk van de organisatie.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.4.1 Beperking toegang tot informatie	**Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.**	JA	Risico Inventarisatie		Geïmplementeerd

Beheersmaatregelen	Vereiste	Toegepast	Reden	Aanvullende reden	Status
A. 9.4.2 Beveiligde inlogprocedures	**Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.4.3 Systeem voor wachtwoordbeheer	**Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.4.4 Speciale systeemhulpmiddelen gebruiken	**Het gebruik van systeem hulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.**	JA	Risico Inventarisatie		Geïmplementeerd
A. 9.4.5 Toegangsbeveiliging op programmabroncode	**Toegang tot de programmabroncode moet worden beperkt.**	JA	Risico Inventarisatie		Geïmplementeerd