



Certificate ISMS-K103628/01

Issued	2020-07-13	Replaces	7247/1-NL
Valid until	2023-07-13	First issued	2020-07-13

ISO/IEC 27001

Kiwa has determined that the information security management system applied by

Decos Information Solutions

and its implementation comply with ISO/IEC 27001:2017 and the Statement of Applicability version 1.3 dated May 1st 2019 for the scope:

All development, sales, implementation, hosting and maintenance of software within Decos Information Solutions, including supporting facilities from Decos Technology Group.

Ron Scheepers
Kiwa

*This certificate consists of 1 page.
Publication of this certificate is allowed.*

CERTIFICATE

19/1190619

Kiwa Nederland B.V.
Sir Winston Churchillaan 273
Postbus 70
NL-2280 AB RIJSWIJK
Tel. +31 88 998 44 00
Fax +31 88 998 44 20
info@kiwa.nl
www.kiwa.nl

Company
Decos Software Engineering B.V.
Huygensstraat 30
NL-2201 DK NOORDWIJK ZH
Tel. +31 88-3326700
info@decos.com
www.decos.com
KVK 28054540

Tradename
Decos Information Solutions

Datum van beoordeling		1 mei 2019	Toepasselijk	Status
Reference	Domain / Section	Control	J/N	
A.5 Informatiebeveiligingsbeleid				
A.5.1 Aansturing door de directie van de informatiebeveiliging				
Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.				
A.5.1.1	Beleidsregels voor informatiebeveiliging	<i>Beheersmaatregel</i> Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	J	Gereed
A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	<i>Beheersmaatregel</i> 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.	J	Gereed
A.6 Organiseren van informatiebeveiliging				
A.6.1 Interne organisatie				
Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.				
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	<i>Beheersmaatregel</i> Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	J	Gereed
A.6.1.2	Scheiding van taken	<i>Beheersmaatregel</i> 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	Gereed
A.6.1.3	Contact met overheidsinstanties	<i>Beheersmaatregel</i> Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	J	Gereed
A.6.1.4	Contact met speciale belangengroepen	<i>Beheersmaatregel</i> Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	J	Gereed
A.6.1.5	Informatiebeveiliging in projectbeheer	<i>Beheersmaatregel</i> Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	J	Gereed
A.6.2 Mobiele apparatuur en telewerken				
Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.				
A.6.2.1	Beleid voor mobiele apparatuur	<i>Beheersmaatregel</i> Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	J	Gereed
A.6.2.2	Telewerken	<i>Beheersmaatregel</i> Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	J	Gereed
A.7 Veilig personeel				
A.7.1 Voorafgaand aan het dienstverband				
Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.				
A.7.1.1	Screening	<i>Beheersmaatregel</i> 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	Gereed
A.7.1.2	Arbeidsvoorwaarden	<i>Beheersmaatregel</i> De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	J	Gereed
A.7.2 Tijdens het dienstverband				
Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.				
A.7.2.1	Directieverantwoordelijkheden	<i>Beheersmaatregel</i>		

		De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	J	Gereed
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	<i>Beheersmaatregel</i> 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.	J	Gereed
A.7.2.3	Disciplinaire procedure	<i>Beheersmaatregel</i> Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	J	Gereed
A.7.3 Beëindiging en wijziging van dienstverband				
Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.				
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	<i>Beheersmaatregel</i> 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.	J	Gereed
A.8 Beheer van bedrijfsmiddelen				
A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen				
Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.				
A.8.1.1	Inventariseren van bedrijfsmiddelen	<i>Beheersmaatregel</i> Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	J	Gereed
A.8.1.2	Eigendom van bedrijfsmiddelen	<i>Beheersmaatregel</i> Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	J	Gereed
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	<i>Beheersmaatregel</i> Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	J	Gereed
A.8.1.4	Teruggeven van bedrijfsmiddelen	<i>Beheersmaatregel</i> 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.	J	Gereed
A.8.2 Informatieclassificatie				
Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.				
A.8.2.1	Classificatie van informatie	<i>Beheersmaatregel</i> Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	J	Gereed
A.8.2.2	Informatie labelen	<i>Beheersmaatregel</i> Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	J	Gereed
A.8.2.3	Behandelen van bedrijfsmiddelen	<i>Beheersmaatregel</i> Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	J	Gereed
A.8.3 Behandelen van media				
Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.				
A.8.3.1	Beheer van verwijderbare media	<i>Beheersmaatregel</i> Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	J	Gereed
A.8.3.2	Verwijderen van media	<i>Beheersmaatregel</i> Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures	J	Gereed

A.8.3.3	Media fysiek overdragen	<i>Beheersmaatregel</i> Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	J	Gereed
A.9 Toegangsbeveiliging				
A.9.1 Bedrijfseisen voor toegangsbeveiliging				
Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.				
A.9.1.1	Beleid voor toegangsbeveiliging	<i>Beheersmaatregel</i> Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	J	Gereed
A.9.1.2	Toegang tot netwerken en netwerkdiensten	<i>Beheersmaatregel</i> Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	J	Gereed
A.9.2 Beheer van toegangsrechten van gebruikers				
Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.				
A.9.2.1	Registratie en uitschrijving van gebruikers	<i>Beheersmaatregel</i> Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	J	Gereed
A.9.2.2	Gebruikers toegang verlenen	<i>Beheersmaatregel</i> 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.	J	Gereed
A.9.2.3	Beheren van speciale toegangsrechten	<i>Beheersmaatregel</i> Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	J	Gereed
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	<i>Beheersmaatregel</i> Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	J	Gereed
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	<i>Beheersmaatregel</i> Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	J	Gereed
A.9.2.6	Toegangsrechten intrekken of aanpassen	<i>Beheersmaatregel</i> 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.	J	Gereed
A.9.3 Gebruikersverantwoordelijkheden				
Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.				
A.9.3.1	Geheime authenticatie-informatie gebruiken	<i>Beheersmaatregel</i> Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	J	Gereed
A.9.4 Toegangsbeveiliging van systeem en toepassing				
Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.				
A.9.4.1	Beperking toegang tot informatie	<i>Beheersmaatregel</i> Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	J	Gereed
A.9.4.2	Beveiligde inlogprocedures	<i>Beheersmaatregel</i> Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	J	Gereed
A.9.4.3	Systeem voor wachtwoordbeheer	<i>Beheersmaatregel</i> Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	J	Gereed
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	<i>Beheersmaatregel</i> Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	J	Gereed
A.9.4.5	Toegangsbeveiliging op programmabroncode	<i>Beheersmaatregel</i> Toegang tot de programmabroncode moet worden beperkt.	J	Gereed
A.10 Cryptografie				
A.10.1 Cryptografische beheersmaatregelen				
Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.				

A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	<i>Beheersmaatregel</i> Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	J	Gereed
A.10.1.2	Sleutelbeheer	<i>Beheersmaatregel</i> Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	J	Gereed
A.11 Fysieke beveiliging en beveiliging van de omgeving				
A.11.1 Beveiligde gebieden				
Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.				
A.11.1.1	Fysieke beveiligingszone	<i>Beheersmaatregel</i> Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	J	Gereed
A.11.1.2	Fysieke toegangsbeveiliging	<i>Beheersmaatregel</i> Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	J	Gereed
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	<i>Beheersmaatregel</i> Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	J	Gereed
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	<i>Beheersmaatregel</i> Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	J	Gereed
A.11.1.5	Werken in beveiligde gebieden	<i>Beheersmaatregel</i> Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	N	Niet van toepassing
A.11.1.6	Laad- en loslocatie	<i>Beheersmaatregel</i> 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.	J	Gereed
A.11.2 Apparatuur				
Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.				
A.11.2.1	Plaatsing en bescherming van apparatuur	<i>Beheersmaatregel</i> Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	J	Gereed
A.11.2.2	Nutsvoorzieningen	<i>Beheersmaatregel</i> Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	J	Gereed
A.11.2.3	Beveiliging van bekabeling	<i>Beheersmaatregel</i> Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	J	Gereed
A.11.2.4	Onderhoud van apparatuur	<i>Beheersmaatregel</i> Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	J	Gereed
A.11.2.5	Verwijdering van bedrijfsmiddelen	<i>Beheersmaatregel</i> Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	J	Gereed
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	<i>Beheersmaatregel</i> 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.	J	Gereed
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	<i>Beheersmaatregel</i> 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 veilig zijn overschreven.	J	Gereed
A.11.2.8	Onbeheerde gebruikersapparatuur	<i>Beheersmaatregel</i> Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	J	Gereed
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	<i>Beheersmaatregel</i>		

		Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	J	Gereed
A.12 Beveiliging bedrijfsvoering				
A.12.1 Bedieningsprocedures en verantwoordelijkheden				
Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.				
A.12.1.1	Gedocumenteerde bedieningsprocedures	<i>Beheersmaatregel</i> Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	J	Gereed
A.12.1.2	Wijzigingsbeheer	<i>Beheersmaatregel</i> Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	J	Gereed
A.12.1.3	Capaciteitsbeheer	<i>Beheersmaatregel</i> Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	J	Gereed
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	<i>Beheersmaatregel</i> Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	J	Gereed
A.12.2 Bescherming tegen malware				
Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.				
A.12.2.1	Beheersmaatregelen tegen malware	<i>Beheersmaatregel</i> Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	J	Gereed
A.12.3 Back-up				
Doelstelling: Beschermen tegen het verlies van gegevens.				
A.12.3.1	Back-up van informatie	<i>Beheersmaatregel</i> Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	J	Gereed
A.12.4 Verslaglegging en monitoren				
Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.				
A.12.4.1	Gebeurtenissen registreren	<i>Beheersmaatregel</i> Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	J	Gereed
A.12.4.2	Beschermen van informatie in logbestanden	<i>Beheersmaatregel</i> Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	J	Gereed
A.12.4.3	Logbestanden van beheerders en operators	<i>Beheersmaatregel</i> Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	J	Gereed
A.12.4.4	Kloksynchronisatie	<i>Beheersmaatregel</i> De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	J	Gereed
A.12.5 Beheersing van operationele software				
Doelstelling: De integriteit van operationele systemen waarborgen.				
A.12.5.1	Software installeren op operationele systemen	<i>Beheersmaatregel</i> Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	J	Gereed
A.12.6 Beheer van technische kwetsbaarheden				
Doelstelling: Benutting van technische kwetsbaarheden voorkomen.				
A.12.6.1	Beheer van technische kwetsbaarheden	<i>Beheersmaatregel</i> 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.	J	Gereed
A.12.6.2	Beperkingen voor het installeren van software	<i>Beheersmaatregel</i> Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	J	Gereed
A.12.7 Overwegingen betreffende audits van informatiesystemen				

Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.				
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	<i>Beheersmaatregel</i> Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	J	Gereed
A.13 Communicatiebeveiliging				
A.13.1 Beheer van netwerkbeveiliging				
Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.				
A.13.1.1	Beheersmaatregelen voor netwerken	<i>Beheersmaatregel</i> Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	J	Gereed
A.13.1.2	Beveiliging van netwerkdiensten	<i>Beheersmaatregel</i> 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.	J	Gereed
A.13.1.3	Scheiding in netwerken	<i>Beheersmaatregel</i> Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	J	Gereed
A.13.2 Informatietransport				
Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.				
A.13.2.1	Beleid en procedures voor informatietransport	<i>Beheersmaatregel</i> Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	J	Gereed
A.13.2.2	Overeenkomsten over informatietransport	<i>Beheersmaatregel</i> Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	J	Gereed
A.13.2.3	Elektronische berichten	<i>Beheersmaatregel</i> Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	J	Gereed
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	<i>Beheersmaatregel</i> 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.	J	Gereed
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen				
A.14.1 Beveiligingseisen voor informatiesystemen				
Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.				
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	<i>Beheersmaatregel</i> De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	J	Gereed
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	<i>Beheersmaatregel</i> 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.	J	Gereed
A.14.1.3	Transacties van toepassingsdiensten beschermen	<i>Beheersmaatregel</i> Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelelen.	J	Gereed
A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen				
Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.				
A.14.2.1	Beleid voor beveiligd ontwikkelen	<i>Beheersmaatregel</i> Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	J	Gereed
A.14.2.2	Procedures voor wijzigingsbeheer	<i>Beheersmaatregel</i>		

	met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	J	Gereed
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	<i>Beheersmaatregel</i> Als bedieningsplatforms 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.	J	Gereed
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	<i>Beheersmaatregel</i> Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	J	Gereed
A.14.2.5	Principes voor engineering van beveiligde systemen	<i>Beheersmaatregel</i> Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	J	Gereed
A.14.2.6	Beveiligde ontwikkelomgeving	<i>Beheersmaatregel</i> 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	Gereed
A.14.2.7	Uitbestede softwareontwikkeling	<i>Beheersmaatregel</i> Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	J	Gereed
A.14.2.8	Testen van systeembeveiliging	<i>Beheersmaatregel</i> Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	J	Gereed
A.14.2.9	Systeemacceptatietests	<i>Beheersmaatregel</i> Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	J	Gereed
A.14.3 Testgegevens				
Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.				
A.14.3.1	Bescherming van testgegevens	<i>Beheersmaatregel</i> Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	J	Gereed
A.15 Leveranciersrelaties				
A.15.1 Informatiebeveiliging in leveranciersrelaties				
Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.				
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	<i>Beheersmaatregel</i> 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.	J	Gereed
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	<i>Beheersmaatregel</i> 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.	J	Gereed
A.15.1.3	Toelevingsketen van informatie- en communicatietechnologie	<i>Beheersmaatregel</i> Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toelevingsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	J	Gereed
A.15.2 Beheer van dienstverlening van leveranciers				
Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.				
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	<i>Beheersmaatregel</i> Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	J	Gereed
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	<i>Beheersmaatregel</i> 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.	J	Gereed
A.16 Beheer van informatiebeveiligingsincidenten				
A.16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen				

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.				
A.16.1.1	Verantwoordelijkheden en procedures	<i>Beheersmaatregel</i> Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	J	Gereed
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	<i>Beheersmaatregel</i> Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	J	Gereed
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	<i>Beheersmaatregel</i> 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.	J	Gereed
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	<i>Beheersmaatregel</i> Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	J	Gereed
A.16.1.5	Respons op informatiebeveiligingsincidenten	<i>Beheersmaatregel</i> Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	J	Gereed
A.16.1.6	Lering uit informatiebeveiligingsincidenten	<i>Beheersmaatregel</i> 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.	J	Gereed
A.16.1.7	Verzamelen van bewijsmateriaal	<i>Beheersmaatregel</i> De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	J	Gereed
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer				
A.17.1 Informatiebeveiligingscontinuïteit				
Doelstelling: Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.				
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	<i>Beheersmaatregel</i> De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	J	Gereed
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	<i>Beheersmaatregel</i> 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.	J	Gereed
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	<i>Beheersmaatregel</i> 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.	J	Gereed
A.17.2 Redundante componenten				
Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.				
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	<i>Beheersmaatregel</i> Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	J	Gereed
A.18 Naleving				
A.18.1 Naleving van wettelijke en contractuele eisen				
Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.				
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	<i>Beheersmaatregel</i> 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.	J	Gereed
A.18.1.2	Intellectuele eigendomsrechten	<i>Beheersmaatregel</i> Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele- eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	J	Gereed

A.18.1.3	Beschermen van registraties	<i>Beheersmaatregel</i> Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	J	Gereed
A.18.1.4	Privacy en bescherming van persoonsgegevens	<i>Beheersmaatregel</i> Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	J	Gereed
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	<i>Beheersmaatregel</i> Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	J	Gereed
A.18.2 Informatiebeveiligingsbeoordelingen				
Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.				
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	<i>Beheersmaatregel</i> 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.	J	Gereed
A.18.2.2	Naleving van beveiligingsbeleid en -normen	<i>Beheersmaatregel</i> 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	Gereed
A.18.2.3	Beoordeling van technische naleving	<i>Beheersmaatregel</i> Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	J	Gereed