Avinty Holding B.V.
Verklaring van Toepasselijkheid
ISO 27001: 2017 + A11:2020
Versie 1.0
28-03-2023
(Publiek)

ACTIVATIE VERKLARING VAN TOEPASSELIJKHEID

Voor u ligt de definitieve ISO 27001 Verklaring van Toepasselijkheid (VVT) van Avinty Holding B.V. welke betrekking heeft op haar gelieerde ondernemingen.

Scope

Informatiebeveiliging gerelateerd aan het ontwikkelen, onderhouden, leveren van (geïntegreerde) zorgsystemen en diensten als consultancy en support voor zowel de zorgprofessional (gebruiker) als de patiënt/ cliënt (eindgebruiker). Waarbij Koppeltaal een onderdeel uitmaakt van het ISMS. Het hosten van de data is uitbesteed aan externe datacenters.

De volgende Avinty dochterondernemingen zijn onderdeel van deze scope:

- **Avinty GGZ**
  Actief in de Geestelijke Gezondheidszorg (GGZ) met het Elektronisch Patiënten Dossier USER ter ondersteuning van het zorgproces.
- **Avinty Jeugd & Gehandicaptenzorg**
  Het Elektronisch Cliënten Dossier (ECD) voor de Gehandicaptenzorg en de Jeugdzorg.
- **Avinty Karify**
  Karify verbindt gebruikers en professionals via eHealth interventies, veilige communicatie, informatie-uitwisseling en online inzage.
- **Avinty Revalidatie**
  Reflex het Elektronisch Patiënten Dossier (EPD) dat zich richt op de multidisciplinaire revalidatiezorg.
  Zij committeren zich allen aan deze verklaring van toepasselijkheid.

Doelgroep

Deze VVT is bestemd voor alle werknemers van Avinty Holding B.V., klanten en andere Avinty stakeholders en haar stakeholders. Het gehanteerde Information Security Management System (ISMS) is van toepassing op de bedrijfsprocessen.

Verantwoordelijkheden

De reikwijdte van de VVT is vastgesteld in samenspraak met het directieteam. Met het ondertekenen is het de verantwoordelijkheid van de directie om de maatregelen te treffen die noodzakelijkerwijs volgen uit het ISMS. Toetsing van het ISO 27001 ISMS vindt plaats door geaccrediteerde certificatie instelling. Om het ISMS doeltreffend en efficiënt te houden treft de organisatie jaarlijks de nodige maatregelen en acties met de benodigde resources

Ondertekend namens het directieteam van Avinty Holding B.V.		
Naam	Joris Tukkers	*Handtekening*
Functie	CFRO	
Plaats	Oldenzaal	
Datum	28-03-2023	

MET DE ONDERTEKENING ACTIVEERT EN BORGT AVINTY HOLDING B.V. HET NORMENKADER ALS VOLGT:

Toelichting normenkader

De Avinty Groep beschikt over een risicoanalyse waarin alle beheersmaatregelen zijn opgenomen en gecontroleerd. Op basis van deze risicoanalyse is vastgesteld dat de normeisen in onderstaande tabel van toepassing zijn voor Avinty. De tabel beschrijft naast de beheersmaatregelen ook de context die op de eis van toepassing is binnen Avinty, als het gaat om:

- Uitbestede controls;
- Beleid;
- Wet- & regelgeving;
- Contractueel;
- Risicoanalyse

Er zijn *geen* beheersmaatregelen uitgesloten.

A5	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Informatiebeveiligingsbeleid								
5.1 Aansturing door de directie van de informatiebeveiliging								
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	X			X	
A.5.1.2	Beoordelen 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				X	

A6	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Organiseren van informatiebeveiliging								
6.1 Interne organisatie								
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	X			X	
A.6.1.2	Scheiding van taken	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.	Ja	X			X	
A.6.1.3	Contact met overheidsinstanties	Er behoren passende contacten met relevante	Ja			X	X	

		overheidsinstanties worden onderhouden.						
A.6.1.4	Contact met speciale belangengroepen	Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	Ja	X			X	
A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Ja	X			X	
6.2 Mobiele apparaten en telewerken								
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	X			X	
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	Ja	X			X	

A7	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Veilig personeel								
7.1 Voorafgaand aan het dienstverband								
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		X		X	
A.7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun	Ja		X	X	X	

		verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.						
7.2 Tijdens het dienstverband								
A.7.2.1	Directieverant-woordelijkheden	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		X		X	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiligi ng	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	X			X	
7.3 Beëindiging en wijziging van dienstverband								
A.7.2.3	Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Ja				X	
A.7.3.1	Beëindiging of wijziging van verantwoordelijkh eden 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	X			X	

A8	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Beheer van bedrijfsmiddelen								
8.1 Verantwoordelijkheden voor bedrijfsmiddelen								
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	X			X	
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Ja	X		X	X	
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	X		X	X	
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	X		X	X	
8.2 Informatieclassificatie								
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	X			X	

A.8.2.2	Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatie-schema dat is vastgesteld door de organisatie.	Ja	X			X	
A.8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatie-schema dat is vastgesteld door de organisatie.	Ja	X	X		X	
8.3 Behandelen van media								
A.8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	X			X	
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	X			X	
A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	X			X	

A9	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Toegangsbeveiliging								
9.1 Bedrijfsvereisten voor toegangscontrole								
A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld	Ja	X			X	

		op basis van bedrijfs- en informatiebeveiligings-eisen.						
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	X			X	
9.2 Beheer van toegangsrechten van gebruikers								
A.9.2.1	Registratie en uitschrijving van gebruikers	Een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	X			X	
A.9.2.2	Gebruikers toegang verlenen	Een formele gebruikerstoegangs-verleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Ja	X			X	
A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Ja	X			X	
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Ja	X			X	
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Ja	X			X	
A.9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie-verwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Ja	X			X	
9.3 Verantwoordelijkheden van gebruikers								
A.9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden	Ja	X	X	X	X	

		aan de praktijk van de organisatie.						

9.4 Toegangsbeveiliging van systeem en toepassing								
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Ja	X			X	
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	X		X	X	
A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	X		X	X	
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja				X	
A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	Ja	X			X	

A10	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Cryptografie								
10.1 Cryptografische beheersmaatregelen								
A.10.1.1	Beleid inzake het gebruik van cryptografische	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische	Ja	X		X	X	

	beheersmaatregelen	beheersmaatregelen worden ontwikkeld en 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	X			X	

A11	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Fysieke beveiliging en beveiliging van de omgeving								
11.1 Beveiligde gebieden								
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	X			X	
A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	X		X	X	
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	X		X	X	
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	X			X	
A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	X			X	
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	Ja			X	X	

		informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.						
A.11.2 Beveiliging van apparatuur								
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		X		X	
A.11.2.2	Nutsvoorzieningen	Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja		X		X	
A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	X			X	
A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	X			X	
A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	X	X	X	X	
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	X	X		X	
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 veilig zijn overschreven.	Ja	X	X		X	

A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	X			X	
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	X			X	

A12	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Beveiliging bedrijfsvoering								
A.12.1 Bedieningsprocedures en verantwoordelijkheden								
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja		X		X	
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	X			X	
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	X		X	X	
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	X			X	
A.12.2 Bescherming tegen malware								
A.12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd,	Ja	X			X	

		in combinatie met een passend bewustzijn van gebruikers.						
A.12.3 Back-up								
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	X		X	X	
12.4 Verslaglegging en monitoren								
A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja		X	X	X	
A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja		X	X	X	
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		X	X	X	
A.12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	Ja	X	X	X	X	
12.5 Beheersing van operationele programmatuur								
A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd	Ja	X			X	
12.6 Beheer van technische kwetsbaarheden								
A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden	Ja	X				

		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.						
A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Ja	X		X		

12.7 Overwegingen bij audits van informatiesystemen								
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			X			

A13	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Communicatiebeveiliging								
13.1 Beheer van netwerkbeveiliging								
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	X			X	
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligings-mechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomstenbetreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Ja	X			X	
A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	X			X	
13.2 Informatietransport								

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	X		X	X	
A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	X		X	X	
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	Ja	X		X	X	
A.13.2.4	Vertrouwelijkheids- of geheimhoudings-overeenkomst	Eisen voor vertrouwelijkheids- of geheimhoudings-overeenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Ja	X		X	X	

A14	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Acquisitie, ontwikkeling en onderhoud van informatiesytemen								
14.1 Beveiligingseisen voor informatiesystemen								
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	X			X	
A.14.1.2	Toepassingsdiensten 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.				X	X	

A.14.1.3	Transacties van toepassingsdienst en beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.		X		X	X	

14.2 Beveiliging in ontwikkelings- en ondersteunende processen								
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	X	X	X	X	
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 controleprocedures voor wijzigingsbeheer.	Ja	X	X	X	X	
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	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.	Ja	X	X	X	X	
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	X			X	
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	X	X	X	X	

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	X	X		X	
A.14.2.7	Uitbestede software-ontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Ja	X		X	X	

A.14.2.8	Testen van systeembeveiliging	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Ja	X	X	X	X	
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	X	X	X	X	
14.3 Testgegevens								
A14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	X	X	X	X	

A15	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Leveranciersrelaties								
15.1 Informatiebeveiliging in leveranciersrelaties								
A.15.1.1	Informatiebeveiligings- beleid 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	Ja	X		X	X	

		overeengekomen en gedocumenteerd.						
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten	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	X		X	X	

A15.1.3	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		X	X	X	
15.2 Beheer van dienstverlening van leveranciers								
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	X	X		X	
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	X	X		X	

A16	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Beheer van informatiebeveiligingsincidenten								
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen								
A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle doeltreffende en ordelijke respons op informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	Ja	X	X		X	
A.16.1.2	Rapportage van informatiebeveiligings-gebeurtenissen	Informatiebeveiligings-gebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	X	X	X	X	
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	X	X	X	X	
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligings-gebeurtenissen	Informatiebeveiliging-gebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	X	X		X	
A.16.1.5	Respons op informatiebeveiligings-incidenten	Op informatiebeveiligings-incidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	X	X		X	

A.16.1.6	Lering uit informatiebeveiligings-incidenten	Kennis die is verkregen door informatiebeveiliging-incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja	X	X		X	
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	X	X	X	X	

A17	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer								
17.1 Informatiebeveiligingscontinuïteit								
A.17.1.1	Informatiebeveiligings- continuïteit plannen	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligings-beheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Ja	X		X	X	
A.17.1.2	Informatiebeveiliging-continuïteit 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	X		X	X	
A.17.1.3	Informatiebeveiliging-continuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligings continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig	Ja	X		X	X	

		verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.							
17.2 Redundante componenten									
A.17.2.1	Beschikbaarheid van informatie-verwerkende faciliteiten	Informatieverwerkende faciliteitenmoeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja		X		X	X	

A18	Paragraaf	Beheersmaatregel	Geïmplementeerd?	Beleid	Wet	Contract	Risicoanalyse	Toelichting
Naleving								
18.1 Compliance met juridische standaarden								
A.18.1.1	Identificatie van toepasbare wet- en regelgeving	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	X	X	X	X	
A.18.1.2	Intellectueel eigendom rechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele- eigendomsrechten en het gebruik van eigendomssoftware-producten te waarborgen moeten passende procedures worden geïmplementeerd.	Ja	X	X	X	X	
A.18.1.3	Bescherming van records	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	X	X	X	X	
A.18.1.4	Privacy en bescherming van persoonlijke data	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Ja	X	X	X	X	
A.18.1.5	Beheersmaatregel van cryptografische controls	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	X		X	X	

18.2 Informatie veiligheid reviews								
A.18.2.1	Onafhankelijke review van informatieveiligheid	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheers doelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	Ja	X		X	X	
A.18.2.2	Compliance met beleid en standaarden	Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	X		X	X	
A.18.2.3	Technische compliance review	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Ja	X		X	X	