SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.5 Informatie- beveiligingsbeleid	A.5.1.	Aansturing door de directie van de informatiebeveiliging	*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	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja	Ja	Beveiligingsinbreuken als gevolg van ontbreken van coördinatie vanuit de directie.	
	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	Ja	Medewerkers hebben onvoldoende aandacht voor het informatiebeveiligingsbeleid.	
tiebeveiliging	A. 6.1	Interne organisatie	*Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.*				

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.6. Organiseren van informat	A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	Ja	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	
	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	Ja	Wegnemen van bedrijfsmiddelen. Misbruik van bevoegdheden.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Ja	Ja	Misbruik van bevoegdheden.	
	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	Ja	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	
	A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Ja	Ja	Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten. Fouten als gevolg van wijzigingen in andere systemen.	
	A.6.2.	Mobiele apparatuur en telewerken	*Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.*				
	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	Ja	Verlies van mobiele apparatuur en opslagmedia	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties (thuiswerken) wordt bereikt, verwerkt of opgeslagen.	Ja	Ja	Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden. Aanvallen via onbeveiligde systemen.	
7. Veilig personeel	A.7.1.	Voorafgaand aan het dienstverband	*Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.*				
	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	Ja	Medewerkers hebben voldoende aandacht voor het informatiebeveiligingsbeleid. Misbruik van bevoegdheden	
	7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Ja	Medewerkers hebben voldoende aandacht voor het informatiebeveiligingsbeleid. Misbruik van bevoegdheden	
	A.7.2	Tijdens het dienstverband	*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	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	Ja	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Medewerkers hebben onvoldoende aandacht voor het informatiebeveiligingsbeleid	
	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	Ja	Beleid wordt niet gevolgd door ontbreken van sanctie	
	A.7.3	Beëindiging en wijziging van dienstverband	*Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.*				
	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	Ja	Onterecht hebben van rechten.	
A.8 Beheer van bedrijfsmiddelen	A.8.1.	Verantwoordelijkheid voor bedrijfsmiddelen	*Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.*				
	A.8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Ja	Ja	Wegnemen van bedrijfsmiddelen.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Ja	Ja	Wegnemen van bedrijfsmiddelen.	
	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	Ja	Systemen worden niet gebruikt waarvoor ze bedoeld zijn	
	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	Ja	Wegnemen van bedrijfsmiddelen.Onterecht hebben van rechten	
	A.8.2.	Informatieclassificatie	*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	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Ja	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	
	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	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.Onveilig versturen van gevoelige informatie.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	
	A.8.3	Behandelen van media	*Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.*				
	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	Ja	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering.	
	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	Ja	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering.	
	A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	Ja	Onveilig versturen van gevoelige informatie. Versturen van gevoelige informatie naar onjuiste persoon.	
veiliging	A.9.1	Bedrijfseisen voor toegangsbeveiliging	*Toegang tot informatie en informatieverwerkende faciliteiten beperken.*				

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.9 Toegangsbev	A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie	
	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	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie	
	A.9.2	Beheer van toegangsrechten van gebruikers	*Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.*				
	A.9.2.1	Registratie en uitschrijving van gebruikers	Een **formele** registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Ja	Misbruik van andermans identiteit. Onterecht hebben van rechten.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk. Onterecht hebben van rechten	
	A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Ja	Ja	Misbruik van bevoegdheden. Het niet hard kunnen maken van welke persoon over welk account beschikt.	
	A.9.2.4	Beheer van geheime authenticatie- informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Ja	Ja	Misbruik van andermans identiteit.	
	A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	Het niet hard kunnen maken van welke persoon over welk account beschikt. Onterecht hebben van rechten.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Onterecht hebben van rechten	
	A.9.3	Verantwoordelijkheden van gebruikers	*Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.*				
	A.9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Ja	Ja	Toegang tot informatie door slecht wachtwoordgebruik.	
	A.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	Ja	Onterecht hebben van rechten	
	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	Ja	Toegang tot informatie door slecht wachtwoordgebruik	
	A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	Ja	Toegang tot informatie door slecht wachtwoordgebruik	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Onterecht hebben van rechten.	
	A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	Ja	Ja	Onterecht hebben van rechten. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling	
A.10 Cryptografie	A.10.1	Cryptografische beheersmaatregelen	*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	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	Ja	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van gebruik van cryptografie	
	A.10.1.2	Sleutelbeheer		Ja	Ja	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van gebruik van cryptografie.	

SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.11 Fysieke beveiliging en beveiliging van de omgeving	A.11.1	Beveiligde gebieden	*Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.*				
	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	Ja	Ongeautoriseerde fysieke toegang	
	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	Ja	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk. Brand	
	A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja	Wegnemen van bedrijfsmiddelen. Ongeautoriseerde fysieke toegang.	
	A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja	Overstroming en wateroverlastBrand, Explosie, Rampen	
	A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja	SpotOnMedics heeft geen beveiligde gebieden.	
	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.	Nee	Nee	SpotOnMedics heeft geen laad en loslocatie	

SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.11.2	Apparatuur	*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	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	Ja	Toegang tot informatie door middel van afluisterapparatuur. Ongeautoriseerde fysieke toegang	
	A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja	Ja	Uitval van facilitaire middelen (gas, water, electra, airco).	
	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	Ja	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	
	A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja	Uitval van systemen door hardwarefouten.	
	A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja	Wegnemen van bedrijfsmiddelenToegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	
	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	Ja	Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering	
	A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja	Toegang tot informatie door onbeheerd achterlaten van werkplekken	
	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	Ja	Misbruik van andermans identiteitToegang tot informatie door onbeheerd achterlaten van werkplekken.	
A.12 Beveiliging bedrijfsvoering	A.12.1	Beveiliging bedrijfsvoering	*Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.*				
	A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja	Niet beschikbaar zijn van informatie of diensten vanuit derden.Kwijtraken van belangrijke kennis bij vertrek of niet beschikbaar zijn van medewerker	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Fouten als gevolg van wijzigingen in andere systemen.	
	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	Ja	Overbelasten van netwerkdiensten.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Uitval van systemen door softwarefouten.Uitval van systemen door configuratiefouten.	
	A.12.2	Bescherming tegen malware	*Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.*				
	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	Ja	Systemen raken besmet met malware.	
	A.12.3	Back-up	*Beschermen tegen het verlies van gegevens.*				

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Informatieverlies door verlopen van houdbaarheid van opslagwijze. Wegnemen van bedrijfsmiddelen. Systemen raken besmet met malware.	
	A.12.4	Verslaglegging en monitoren	*Gebeurtenissen vastleggen en bewijs verzamelen.*				
	A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja	Ja	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.	
	A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Ja	Het niet hard kunnen maken van welke persoon over welk account beschikt.	
	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	Ja	Het niet hard kunnen maken van welke persoon over welk account beschikt. Misbruik van bevoegdheden.	
	A.12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	Ja	Ja	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.12.5	Beheersing van operationele software	*De integriteit van operationele systemen waarborgen.*				
	A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Ja	Ja	Fouten als gevolg van wijzigingen in andere systemen	
	A.12.6	Beheer van technische kwetsbaarheden	*Benutting van technische kwetsbaarheden voorkomen.*				
	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	Ja	Systemen raken besmet met malware. Toegang tot informatie door misbruik van kwetsbaarheden in applicaties Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	
	A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Ja	Ja	Systemen raken besmet met malware. Informatieverlies door verlopen van houdbaarheid van opslagwijze.	
	A.12.7	Overwegingen betreffende audits van informatiesystemen	*De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.,*				

SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	
A.13 Communicatiebeveiliging	A.13.1	Beheer van netwerkbeveiliging	*De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.*				
	A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging. Aanvallen via onbeveiligde systemen	
	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	Ja	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging. Aanvallen via onbeveiligde systemen	
	A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	Ja	Systemen raken besmet met malware.Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	
	A.13.2	Informatietransport	*Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.*				

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie. Onveilig versturen van gevoelige informatie.	
	A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja	Onveilig versturen van gevoelige informatie.	
	A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	Ja	Ja	Versturen van gevoelige informatie naar onjuiste persoon	
	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	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.Misbruik van bevoegdheden	
nformatiesystemen	A.14.1	Beveiligingseisen voor informatiesystemen	*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.*				

SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.14 Acquisitie, ontwikkeling en onderhoud van in	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	Ja	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	
	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.	Ja	Ja	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud	
	A.14.1.3	Transacties van toepassingsdiensten 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.	Ja	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	
	A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	*Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.*				

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	
	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	Ja	Fouten als gevolg van wijzigingen in andere systemen.	
	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	Ja	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	
	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	Ja	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.Fouten als gevolg van wijzigingen in andere systemen.	
	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	Ja	Uitval van systemen door softwarefouten. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	
	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	Ja	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Ja	Ja	SpotOnMedics besteed vanaf eind 2020/2021 softwareontwikkeing uit.	
	A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Ja	Ja	Uitval van systemen door softwarefouten.Uitval van systemen door configuratiefouten.	
	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	Ja	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling. Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten	
	A.14.3	Testgegevens	*Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.*				
	A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	
A.15 Leveranciersrelaties	A.15.1	Informatiebeveiliging in leveranciersrelaties	*De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.*				
	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	Ja	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	
	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	Ja	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud. Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	
	A.15.2	Beheer van dienstverlening van leveranciers	*Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.*				
	A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Niet beschikbaar zijn van informatie of diensten vanuit derden.Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk.	
ebeveiligingsincidenten	A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	*Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.*				

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.16 Beheer van informatie	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	Ja	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	Ja	De gevolgen van incidenten worden onnodig groot, doordat deze niet tijdig gezien / opgepakt worden.	
	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	Ja	De gevolgen van incidenten worden onnodig groot, doordat deze niet tijdig gezien / opgepakt worden.	
	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	Ja	Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	
	A.16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	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	Ja	Herhaling van incidenten	
	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	Ja	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.Het niet hard kunnen maken van welke persoon over welk account beschikt.	
Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	A.17.1	Informatiebeveiligingscontinuïteit	*Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.*				
	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	Ja	Beveiligingsinbreuken als gevolg van ontbreken van coördinatie vanuit de directie. Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.Brand, Overstroming, Explosie, Rampen	
	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	Ja	ncidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken. Brand, Overstroming, Explosie, Rampen	

SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
A.17	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	Ja	Brand, Overstroming, Explosie, Rampen	
	A.17.2	Redundante componenten	*Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.*				
	A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	Overbelasten van netwerkdienstenNiet beschikbaar zijn van informatie of diensten vanuit derden	
A.18 Naleving	A.18.1	Naleving van wettelijke en contractuele eisen	*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	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	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van het bezoeken van dat land	

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.18.1.2	Intellectuele eigendomsrechten	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.	Ja	Ja	Tegen het bedrijf worden juridisch stappen genomen vanwege schenden van auteursrechten / IPR.	
	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	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	
	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 wet- en regelgeving.	Ja	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud.	
	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	Ja		

SpotOnMedics VVT v5.0 d.d. 4-8-2022

Onderwerp			Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Controlemaatregel
	A.18.2	Informatiebeveiligingsbeoordelingen	*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	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	Ja	Systemen worden niet gebruikt waarvoor ze bedoeld zijn. Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	
	A.18.2.2	Naleving van beveiligingsbeleid en -normen	Het management 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.	Ja	Ja	Systemen worden niet gebruikt waarvoor ze bedoeld zijn. Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	
	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	Ja	Systemen raken besmet met malware. Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	

G.J. van den Enden
15-9-2022