

SpotOnMedics VVT v7.0 d.d. 31-3-2024

Legenda

WE = Wettelijke eis

CE = Contractuele eis

BP/BR = Best Practise / Business Requirement (kenmerkend voor onze business)

RA = Result of Risk Assessment (uit risicobeoordeling)

Onderwerp		Beheersmaatregel	Geselecteerd	Geïmplementeerd	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel
5	5.1	Beleidsregels voor informatiebeveiliging	Ja	Ja	Beveiligingsinbreuken als gevolg van ontbreken van coördinatie vanuit de directie. Medewerkers hebben onvoldoende aandacht voor het informatiebeveiligingsbeleid.	41 54
	5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevend.	41 43 120
	5.3	Functiescheiding	Ja	Ja	Wegnemen van bedrijfsmiddelen. Misbruik van bevoegdheden.	43 121
	5.4	Managementverantwoordelijkheden	Ja	Ja	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevend.	32 122
	5.5	Contact met overheidsinstanties	Ja	Ja	Misbruik van bevoegdheden.	123
	5.6	Contact met speciale belangengroepen	Ja	Ja	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	123
	5.7	Informatie en analyses over dreigingen	Ja	Ja	Mogelijk onvolledige of onnauwkeurige informatie gebruikt bij het beoordelen van de dreigingen waarmee SpotOnMedics wordt geconfronteerd.	113 124
	5.8	Informatiebeveiliging in projectmanagement	Ja	Ja	- Uitval van systemen door softwarefouten. - Uitval van systemen door configuratiefouten. - Fouten als gevolg van wijzigingen in andere systemen. - Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	8 55 63 t/m 69 83 125
	5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Ja	Ja	Wegnemen van bedrijfsmiddelen.	18 62 126
	5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Ja	Ja	- Systemen worden niet gebruikt waarvoor ze bedoeld zijn - Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	2 9 16 19 20 126
	5.11	Retourneren van bedrijfsmiddelen	Ja	Ja	Wegnemen van bedrijfsmiddelen. Onterecht hebben van rechten	13 18 126

5. Organisatorische beheersmaatregelen	5.12	Classificeren van informatie	Informatie behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Ja	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	3 15 42 127
	5.13	Labelen van informatie	Om informatie te labelen behoort een passende reeks procedures te 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.	42 127
	5.14	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Ja	- Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie. - Onveilig versturen van gevoelige informatie. - Versturen van gevoelige informatie naar onjuiste persoon	8 27 31 38 40
	5.15	Toegangsbeveiliging	Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja	Ja	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie	21 34
	5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	Ja	Ja	Misbruik van andermans identiteit. Onterecht hebben van rechten.	23 39
	5.17	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerd door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja	Ja	- Misbruik van andermans identiteit - Toegang tot informatie door slecht wachtwoordgebruik.	21 35
	5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja	Ja	- Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk. - Onterecht hebben van rechten - Het niet hard kunnen maken van welke persoon over welk account beschikt. - Onterecht hebben van rechten. - Onterecht hebben van rechten	13 18 21 23 28 34 39
	5.19	Informatiebeveiliging in leveranciersrelaties	Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	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.	22 25 33
	5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	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.	22
	5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er behoren processen en procedures te worden bepaald en geïmplementeerd om de informatie- beveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	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.	22
	5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	Ja	Ja	- Toegang tot informatie door misbruik van kwetsbaarheden in applicaties. - Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging. - 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.	25 36
	5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.	Ja	Ja	Het risico op datalekken neemt toe. Het kan leiden tot het verlies of de ongeoorloofde toegang tot gevoelige informatie, wat kan resulteren in reputatieschade, juridische gevolgen en financiële verliezen.	129

5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Ja	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	42 60 61 70 95
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Ja	Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	60 61
5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	60 61
5.27	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Ja	Herhaling van incidenten	60 61
5.28	Verzamelen van bewijsmateriaal	De organisatie behoort procedures vast te stellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	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.	60 61
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	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. - "Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken. - Brand, Overstroming, Explosie, Rampen"	22 24 33
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja	Ja	SpotonMedics kan niet voldoen aan de doelstellingen van de organisatie door een verstoring	130
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, behoren te worden geïdentificeerd, 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	36 44 45 88
5.32	Intellectuele-eigendomsrechten	De organisatie behoort passende procedures te implementeren om intellectuele-eigendomsrechten te beschermen.	Ja	Ja	Tegen het bedrijf worden juridisch stappen genomen vanwege schenden van auteursrechten / IPR.	36
5.33	Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	3 7 36 38 44
5.34	Privacy en bescherming van persoonsgegevens	De organisatie behoort de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen.	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.	21 25 36 38 44 89
5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te 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.	45 96 97

	5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.	Ja	Ja	- Systemen worden niet gebruikt waarvoor ze bedoeld zijn. Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevendenden. - Systemen raken besmet met malware. Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	27 45
	5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Ja	Ja	Niet beschikbaar zijn van informatie of diensten vanuit derden. Kwijtraken van belangrijke kennis bij vertrek of niet beschikbaar zijn van medewerker	4 12 17 32 38
6. Mensgericht beheersmaatregelen	6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband behoort te worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfs-eisen, 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	32
	6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Ja	Medewerkers hebben voldoende aandacht voor het informatiebeveiligingsbeleid. Misbruik van bevoegdheden	131
	6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	Ja	Ja	Medewerkers hebben onvoldoende aandacht voor het informatiebeveiligingsbeleid	10 12 17 19 20 28 32 70
	6.4	Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja	Ja	Beleid wordt niet gevolgd door ontbreken van sanctie	31 38
	6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	Ja	Onterecht hebben van rechten.	13 18 23 39 147
	6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie. Misbruik van bevoegdheden	31 38
	6.7	Werken op afstand	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja	Ja	Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden. Aanvallen via onbeveiligde systemen.	19
	6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja	Ja	De gevolgen van incidenten worden onnodig groot, doordat deze niet tijdig gezien / opgepakt worden.	42 60 61
	7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja	Ja	Ongeautoriseerde fysieke toegang	1 50 52

7. Fysieke beheersmaatregelen	7.2	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Ja	Ja	- Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk. Brand - SpotOnMedics heeft geen laad en loslocatie	1 13 37 90 t/m 93 112 114
	7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.	Ja	Ja	Wegnemen van bedrijfsmiddelen. Ongeautoriseerde fysieke toegang.	1 37 50 52 90 t/m 93 108 112 114
	7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.	Ja	Ja	Diefstal, toegang tot informatie door onbevoegden (B, V)	37
	7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, te worden ontworpen en geïmplementeerd.	Ja	Ja	Overstroming en wateroverlast Brand, Explosie, Rampen	37 111 112 114
	7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Ja	Ja	SpotOnMedics heeft geen beveiligde gebieden.	37
	7.7	'Clear desk' en 'clear screen'	Er behoren 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten te worden gedefinieerd en op passende wijze te worden afgedwongen.	Ja	Ja	Misbruik van andermans identiteit Toegang tot informatie door onbeheerd achterlaten van werkplekken.	14 15 20 59
	7.8	Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd.	Ja	Ja	Toegang tot informatie door middel van afuisterapparatuur. Ongeautoriseerde fysieke toegang	15
	7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.	Ja	Ja	Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	9 57 59
	7.10	Opslagmedia	Opslagmedia behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanterings-eisen van de organisatie.	Ja	Ja	- Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering. - Onveilig versturen van gevoelige informatie. Versturen van gevoelige informatie naar onjuiste persoon. - Wegnemen van bedrijfsmiddelen Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	16 20 56 57 59
	7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Ja	Uitval van facilitaire middelen (gas, water, electra, airco).	15 59
	7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Ja	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	15 59
	7.13	Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja	Ja	Uitval van systemen door hardwarefouten.	15 59
7.14	Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja	Ja	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering	14 59	

8.1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.	Ja	Ja	- Verlies van mobiele apparatuur en opslagmedia - Toegang tot informatie door onbeheerd achterlaten van werkplekken	1 2 9 14 37 59 86 87
8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten behoort te worden beperkt en beheerd.	Ja	Ja	Misbruik van bevoegdheden. Het niet hard kunnen maken van welke persoon over welk account beschikt.	35
8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja	Onterecht hebben van rechten	21 28 34
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd.	Ja	Ja	Onterecht hebben van rechten. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling	21
8.5	Beveiligde authenticatie	Er behoren beveiligde authenticatietechnologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja	Toegang tot informatie door slecht wachtwoordgebruik	42
8.6	Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Ja	Overbelasten van netwerkdiensten.	4
8.7	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja	Ja	Systemen raken besmet met malware.	27 28
8.8	Beheer van technische kwetsbaarheden	Er behoort informatie te worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behorende passende maatregelen te worden getroffen.	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. - Systemen raken besmet met malware. Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	27
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Ja	Kans op beveiligingsincidenten neemt toe	132 143
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer vereist is.	Ja	Ja	Ongewenste openbaarmaking van gevoelige informatie, grotere kans op datalekken	21 133
8.11	Maskeren van gegevens	Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Ja	Ongewenste openbaarmaking van gevoelige informatie, grotere kans op datalekken	21 134 144
8.12	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Ja	Ongewenste openbaarmaking van gevoelige informatie, grotere kans op datalekken	135
8.13	Back-up van informatie	Back-ups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups	Ja	Ja	Informatieverlies door verlopen van houdbaarheid van opslagwijze. Wegnemen van bedrijfsmiddelen. Systemen raken besmet met malware.	3 24
8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	Overbelasten van netwerkdiensten Niet beschikbaar zijn van informatie of diensten vanuit derden	22 24 25 33

8. Technologische beheersmaatregelen	8.15	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	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. - Het niet hard kunnen maken van welke persoon over welk account beschikt. Misbruik van bevoegdheden.	145
	8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Ja	Toename van gegevenslekken, wanneer monitoren niet naar behoren wordt uitgevoerd	136
	8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja	Ja	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.	17
	8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	Ja	Ja	Onterecht hebben van rechten.	21
	8.19	Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Ja	- Fouten als gevolg van wijzigingen in andere systemen - Systemen raken besmet met malware. Informatieverlies door verlopen van houdbaarheid van opslagwijze.	17 27 94 99
	8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, 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	27
	8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningsseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Ja	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging. Aanvallen via onbeveiligde systemen	137
	8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.	Ja	Ja	Systemen raken besmet met malware. Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	34
	8.23	Toepassen van webfilters	De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Ja	Zonder webfilters hebben gebruikers onbeperkte toegang tot het volledige spectrum van internetinhoud, inclusief potentieel schadelijke websites die malware, virussen of phishingaanvallen kunnen bevatten. Dit verhoogt het risico op infectie van systemen en gegevensverlies.	138 146
	8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Ja	Ja	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van gebruik van cryptografie	27 74 98
	8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.	Ja	Ja	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	11
	8.26	Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Ja	- Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud - Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	8
	8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja	Ja	Uitval van systemen door softwarefouten. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	11
	8.28	Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling	Ja	Ja	Slecht gecodeerde applicaties kunnen het risico op datalekken vergroten, waarbij gevoelige informatie per ongeluk wordt blootgesteld als gevolg van programmeerfouten.	139

8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja	Ja	- Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten. - Onvoldoende aandacht voor beveiliging bij softwareontwikkeling. Uitval van systemen door softwarefouten of door configuratiefouten	11
8.30	Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.	Ja	Ja	SpotOnMedics besteed vanaf eind 2020/2021 softwareontwikkeling uit.	140
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	Ja	Ja	- Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten. - Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.en	4 11 55
8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	Ja	Ja	- Fouten als gevolg van wijzigingen in andere systemen. - Toegang tot informatie door misbruik van kwetsbaarheden in applicaties. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling. - Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.Fouten als gevolg van wijzigingen in andere systemen.	4 8 11
8.33	Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	Ja	Ja	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	5 25
8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Ja	Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	27