Verklaring van Toepasselijkheid

Simac Techniek nv

NEN 7510-1+A1:2020

27-08-2024

Versie 2.0

Invoering

Dit document bevat de Verklaring van Toepasselijkheid ten behoeve van certificering voor de NEN 7510-1+A1:2020 normering. Het doel van dit document is om de juiste controles te identificeren die moeten worden geïmplementeerd om de bedreigingen tegen Simac en zijn bedrijfsprocessen te bewaken en te beheren. De beheersmaatregelen zijn geïdentificeerd op basis van de NEN 7510-1+A1:2020 standaard opgenomen beheersmaatregelen van de normering. Per beheersmaatregel is de toepasbaarheid weergegeven. Indien een beheersmaatregel niet van toepassing is, wordt hiervoor een toelichting gegeven.

Managementverklaring

De directie van Simac verklaart hierbij de in deze verklaring van toepasselijkheid genoemde maatregelen te bekrachtigen met betrekking tot de uitgevoerde risicoanalyses en aanvaardt het restrisico van niet genomen maatregelen.

Verklaring van Toepasselijkheid - NEN 7510-1+A1:2020

Legenda - Reden in scope	
Best practice	Beheersingsdoelstellingen en maatregelen die direct of indirect verband houden met verplichte beheersdoelstellingen en maatregelen in de NEN 7510-1+A1:2020 normering of die als best practices worden geaccepteerd.
Risico analyse	Beheersdoelstellingen en maatregelen die direct verband houden met een geïdentificeerd risico.
Wet- en regelgeving	Beheersdoelstellingen en maatregelen die direct verband houden met wet- en regelgeving.
Contract	Beheersdoelstellingen en maatregelen die direct verband houden met contractuele verplichtingen.

Beheerdoelstellingen en maatregelen			In scope	Geïmplementeerd	Uitbesteed	Reden (niet) in scope
ML.A.5	**Informatiebeveiligingsbeleid**					
ML.A.5.1	**Aansturing door de directie van de informatiebeveiliging**					
MK.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	Nee	Best practice
ML.A.5.1.1	Beleidsregels voor informatiebeveiliging	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice

ML.A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	ZORGSPECIFIEKE BEHEERSMAATREGEL Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	Ja	Ja	Nee	Best practice
ML.A.6	**Organiseren van informatiebeveiliging**					
ML.A.6.1	**Interne organisatie**					
MK.A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	Ja	Nee	Risico
ML.A.6.1.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen.	Ja	Ja	Nee	Risico
ML.A.6.1.1.2	Rollen en verantwoordelijkheden bij informatiebeveiliging (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Er behoort minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie.	Ja	Ja	Nee	Risico
ML.A.6.1.1.3	Rollen en verantwoordelijkheden bij informatiebeveiliging (3)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties behoren over een gezondheidsinformatiebeveiligingsmanagementforum (IBMF) te beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B3 en B4 van bijlage B (6. 1. 1). Het gezondheidsinformatiebeveiligingsforum behoort regelmatig, maandelijks of bijna maandelijks, te vergaderen. (Het is meestal het effectiefst als het forum vergadert op een tijdstip halverwege tussen twee vergaderingen van het bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.)	Ja	Ja	Nee	Risico
ML.A.6.1.1.4	Rollen en verantwoordelijkheden bij informatiebeveiliging (4)	ZORGSPECIFIEKE BEHEERSMAATREGEL Er behoort een formele verklaring van het toepassingsgebied te worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen.	Ja	Ja	Nee	Best practice
MK.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	Nee	Risico
ML.A.6.1.2	Scheiding van taken	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden	Ja	Ja	Nee	Risico

		om de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.				
MK.A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
MK.A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Ja	Ja	Nee	Best practice
ML.A.6.1.5	Informatiebeveiliging in projectbeheer	ZORGSPECIFIEKE BEHEERSMAATREGEL Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	Nee	Best practice
ML.A.6.2	**Mobiele apparatuur en telewerken**					
MK.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	Nee	Risico
MK.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	Ja	Nee	Best practice
ML.A.7	**Veilig personeel**					
ML.A.7.1	**Voorafgaand aan het dienstverband**					
MK.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	Ja	Nee	Best practice
ML.A.7.1.1.1	Screening (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties behoren minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie te verifiëren.	Ja	Ja	Nee	Best practice
ML.A.7.1.1.2	Screening (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband behoren een verificatie te omvatten van de toepasselijke kwalificaties voor zorgverleners indien er sprake is van accreditatie voor de	Nee	Nee	Nee	Er zijn geen personeelsleden in dienst waarop dit van toepassing kan zijn

		beroepsgroep op basis van die kwalificaties (bijv. artsen, verplegend personeel enz.).				
ML.A.7.1.1.3	Screening (3)	ZORGSPECIFIEKE BEHEERSMAATREGEL Als een persoon wordt ingehuurd voor een specifieke beveiligingsfunctie, behoort de organisatie zich ervan te vergewissen dat: de kandidaat over de nodige competentie beschikt om de beveiligingsfunctie te vervullen; de kandidaat de functie toevertrouwd kan worden, in het bijzonder als de functie cruciaal is voor de organisatie.	Ja	Ja	Nee	Best practice
MK.A.7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Ja	Nee	Best practice
ML.A.7.1.2	Arbeidsvoorwaarden	ZORGSPECIFIEKE BEHEERSMAATREGEL Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functieomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functieomschrijvingen worden vastgelegd. Er moet speciale aandacht worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz.	Ja	Ja	Nee	Best practice
ML.A.7.2	**Tijdens het dienstverband**					
MK.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	Nee	Risico
MK.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	Nee	Risico

ML.A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleiden -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derde-contractanten moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
ML.A.7.3	**Beëindiging en wijziging van dienstverband**					
MK.A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	Ja	Ja	Nee	Best practice
ML.A.8	**Beheer van bedrijfsmiddelen**					
ML.A.8.1	**Verantwoordelijkheid voor bedrijfsmiddelen**					
MK.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	Nee	Risico
ML.A.8.1.1.1	Inventariseren van bedrijfsmiddelen (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren verantwoording af te leggen over informatiebedrijfsmiddelen (d. w. z. een inventaris bij te houden van dergelijke bedrijfsmiddelen).	Ja	Ja	Nee	Risico
ML.A.8.1.1.2	Inventariseren van bedrijfsmiddelen (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren een eigenaar te hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8. 1. 2)	Ja	Ja	Nee	Risico
ML.A.8.1.1.3	Inventariseren van bedrijfsmiddelen (3)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren regels te hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	Ja	Nee	Risico

MK.A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Ja	Ja	Nee	Risico
MK.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	Nee	Best practice
MK.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	Nee	Best practice
ML.A.8.1.4	Teruggeven van bedrijfsmiddelen	ZORGSPECIFIEKE BEHEERSMAATREGEL Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	Ja	Ja	Nee	Best practice
ML.A.8.2	**Informatieclassificatie**					
MK.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	Nee	Risico
ML.A.8.2.1	Classificatie van informatie	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
ML.A.8.2.2	Informatie labelen	ZORGSPECIFIEKE BEHEERSMAATREGEL Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), en moeten papieren output als vertrouwelijk labelen als die output persoonlijke gezondheidsinformatie bevat.	Ja	Ja	Nee	Best practice
MK.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	Nee	Risico

ML.A.8.3	**Behandelen van media**					
MK.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	Nee	Risico
ML.A.8.3.1.1	Beheer van verwijderbare media (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Media die persoonlijke gezondheidsinformatie bevatten, behoren fysiek te worden beschermd of de gegevens ervan behoren versleuteld te worden.	Ja	Ja	Nee	Risico
ML.A.8.3.1.2	Beheer van verwijderbare media (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, behoren gemonitord te worden.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
ML.A.8.3.2	Verwijderen van media	ZORGSPECIFIEKE BEHEERSMAATREGEL Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Nee	Risico
MK.A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	Ja	Nee	Risico
ML.A.9	**Toegangsbeveiliging**					
ML.A.9.1	**Bedrijfseisen voor toegangsbeveiliging**					
MK.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	Nee	Risico
ML.A.9.1.1.1	Beleid voor toegangsbeveiliging (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de toegang tot dergelijke informatie te controleren. In het algemeen behoren de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie te beperken tot situaties: waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben; waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen.	Ja	Ja	Nee	Risico
ML.A.9.1.1.2	Beleid voor toegangsbeveiliging (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren een toegangscontrolebeleid te hebben waarmee de toegang tot deze gegevens wordt geregeld.	Ja	Ja	Nee	Risico

ML.A.9.1.1.3	Beleid voor toegangsbeveiliging (3)	ZORGSPECIFIEKE BEHEERSMAATREGEL Het beleid van de organisatie met betrekking tot toegangscontrole behoort te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol.	Ja	Ja	Nee	Risico
ML.A.9.1.1.4	Beleid voor toegangsbeveiliging (4)	ZORGSPECIFIEKE BEHEERSMAATREGEL Het toegangscontrolebeleid, als bestanddeel van het in 5. 1. 1 beschreven beleidskader voor informatiebeveiliging, behoort professionele, ethische, juridische en cliëntgerelateerde eisen te weerspiegelen en behoort de taken die worden uitgevoerd door zorgverleners en de workflow van de taak in aanmerking te nemen.	Ja	ja	Nee	Risico
ML.A.9.1.1.5	Beleid voor toegangsbeveiliging (5)	ZORGSPECIFIEKE BEHEERSMAATREGEL De organisatie behoort alle partijen te identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld en met deze partijen behoren contractuele afspraken over toegang en rechten te worden gemaakt, alvorens cliëntgegevens uit te wisselen.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
ML.A.9.2	**Beheer van toegangsrechten van gebruikers**					
MK.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	Nee	Risico
ML.A.9.2.1	Registratie en uitschrijving van gebruikers	ZORGSPECIFIEKE BEHEERSMAATREGEL De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikers- registratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
MK.A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Ja	Ja	Nee	Risico
MK.A.9.2.4	Beheer van geheime authenticatieinformatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Ja	Ja	Nee	Risico

MK.A.9.2.5	Beoordeling van toegangsrechten	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
ML.A.9.2.6	Toegangsrechten intrekken of aanpassen	ZORGSPECIFIEKE BEHEERSMAATREGEL Alle organisaties die persoonlijke gezondheidsinformatie verwerken, moeten voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaam- heden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	Ja	Ja	Nee	Risico
ML.A.9.3	**Gebruikersverantwoordelijkheden**					
MK.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	Nee	Risico
ML.A.9.4	**Toegangsbeveiliging van systeem en toepassing**					
MK.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	Nee	Risico
ML.A.9.4.1.1	Beperking toegang tot informatie (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden.	Ja	Ja	Nee	Risico
ML.A.9.4.1.2	Beperking toegang tot informatie (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie behoort geïsoleerd (en gescheiden) te worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	Nee	Risico
MK.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	Nee	Best practice
MK.A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	Ja	Nee	Risico

MK.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	Nee	Risico
MK.A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	Ja	Ja	Nee	Risico
ML.A.10	**Cryptografie**					
ML.A.10.1	**Cryptografische beheersmaatregelen**					
MK.A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja	Nee	Best practice
MK.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	Ja	Nee	Best practice
ML.A.11	**Fysieke beveiliging en beveiliging van de omgeving**					
ML.A.11.1	**Beveiligde gebieden**					
MK.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	Nee	Risico
ML.A.11.1.1	Fysieke beveiligingszone	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruikmaken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden moeten worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	Ja	Best practice
MK.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	Ja	Best practice
MK.A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja	Nee	Risico
MK.A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja	Nee	Best practice
MK.A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja	Nee	Best practice

MK.A.11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Ja	Ja	Nee	Risico
ML.A.11.2	**Apparatuur**					
MK.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	Nee	Risico
MK.A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja	Ja	Nee	Best practice
MK.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	Nee	Risico
MK.A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja	Ja	Nee	Best practice
MK.A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja	Nee	Best practice
ML.A.11.2.5	Verwijdering van bedrijfsmiddelen	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat die uitrusting, gegevens of software van de locatie wordt of worden verwijderd of erbinnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven.	Ja	Ja	Nee	Best practice
MK.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	Nee	Risico
ML.A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d. w. z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.).	Ja	Ja	Nee	Best practice

MK.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	Nee	Best practice
ML.A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Nee	Best practice
MK.A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
ML.A.12	**Beveiliging bedrijfsvoering**					
ML.A.12.1	**Bedieningsprocedures en verantwoordelijkheden**					
MK.A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
ML.A.12.1.2	Wijzigingsbeheer	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces beheersen om de gepaste beheersing van hosttoepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.	Ja	Ja	Nee	Best practice
MK.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	Nee	Risico
MK.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	Nee	Risico
ML.A.12.1.4.1	Scheiding van ontwikkel-, test- en productieomgevingen (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel) te scheiden van operationele	Ja	Ja	Nee	Risico

		omgevingen waar die gezondheidsinformatiesystemen gehost worden.				
ML.A.12.1.4.2	Scheiding van ontwikkel-, test- en productieomgevingen (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Er behoren regels voor het migreren van software van de ontwikkel- naar een operationele status te worden gedefinieerd en gedocumenteerd door de organisatie die de betreffende toepassing(en) host.	Ja	Ja	Nee	Risico
ML.A.12.2	**Bescherming tegen malware**					
MK.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	Nee	Best practice
ML.A.12.2.1	Beheersmaatregelen tegen malware	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en responsbeheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software en moeten passende bewustzijnstraining voor gebruikers implementeren.	Ja	Ja	Nee	Best practice
ML.A.12.3	**Back-up**					
MK.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	Nee	Best practice
ML.A.12.3.1.1	Back-up van informatie (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren back-ups te maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving op te slaan om te garanderen dat de informatie in de toekomst beschikbaar is.	Ja	Ja	Nee	Best practice
ML.A.12.3.1.2	Back-up van informatie (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Om de vertrouwelijkheid ervan te beschermen behoren er versleutelde back-ups te worden gemaakt van persoonlijke gezondheidsinformatie.	Ja	Ja	Nee	Best practice
ML.A.12.4	**Verslaglegging en monitoren**					
MK.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	Nee	Best practice
MK.A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Ja	Nee	Best practice
ML.A.12.4.2.1	Beschermen van informatie in logbestanden (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Auditverslagen behoren beveiligd te zijn en niet gemanipuleerd te kunnen worden.	Ja	Ja	Nee	Best practice

ML.A.12.4.2.2	Beschermen van informatie in logbestanden (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL De toegang tot hulpmiddelen voor audits van systemen en audittrajecten behoort te worden beveiligd om misbruik of compromittering te voorkomen.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
MK.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	Nee	Best practice
ML.A.12.4.4	Kloksynchronisatie	ZORGSPECIFIEKE BEHEERSMAATREGEL Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdssynchronisatiediensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	Ja	Ja	Nee	Best practice
ML.A.12.5	**Beheersing van operationele software**					
MK.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	Nee	Best practice
ML.A.12.6	**Beheer van technische kwetsbaarheden**					
MK.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	Nee	Risico
MK.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	Nee	Best practice
ML.A.12.7	**Overwegingen betreffende audits van informatiesystemen**					
MK.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	Nee	Best practice
ML.A.13	**Communicatiebeveiliging**					
ML.A.13.1	**Beheer van netwerkbeveiliging**					
MK.A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	Nee	Risico

MK.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	Nee	Risico
MK.A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	Ja	Nee	Risico
ML.A.13.2	**Informatietransport**					
MK.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	Nee	Best practice
MK.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	Nee	Best practice
MK.A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
ML.A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	Ja	Ja	Nee	Best practice
ML.A.14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**					
ML.A.14.1	**Beveiligingseisen voor informatiesystemen**					
MK.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	Nee	Best practice
ML.A.14.1.1.1.1	Zorgontvangers op unieke wijze identificeren (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren zeker te stellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem.	Ja	Ja	Nee	Best practice

ML.A.14.1.1.1.2	Zorgontvangers op unieke wijze identificeren (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren in staat te zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.	Ja	Ja	Nee	Best practice
ML.A.14.1.1.2	Validatie van outputgegevens	ZORGSPECIFIEKE BEHEERSMAATREGEL Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld	Ja	Ja	Nee	Best practice
MK.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	Nee	Risico
MK.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	Nee	Risico
ML.A.14.1.3.1.1	Openbaar beschikbare gezondheidsinformatie (1)	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd.	Nee	Nee	Nee	Simac verwerkt geen openbaar beschikbare gezondheidsinformatie
ML.A.14.1.3.1.2	Openbaar beschikbare gezondheidsinformatie (2)	De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen.	Nee	Nee	Nee	Simac verwerkt geen openbaar beschikbare gezondheidsinformatie
ML.A.14.1.3.1.3	Openbaar beschikbare gezondheidsinformatie (3)	De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie moet worden vermeld en de integriteit ervan behoort te worden beschermd.	Nee	Nee	Nee	Simac verwerkt geen openbaar beschikbare gezondheidsinformatie
ML.A.14.2	**Beveiliging in ontwikkelings- en ondersteunende processen**					
MK.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	Nee	Risico
MK.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	Nee	Risico

MK.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	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Best practice
MK.A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Nee	Nee	Nee	Er wordt geen software ontwilleking uitbesteed
MK.A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
ML.A.14.2.9.1	Systeemacceptatietests (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren acceptatiecriteria vast te stellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies.	Ja	Ja	Nee	Risico
ML.A.14.2.9.2	Systeemacceptatietests (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Voorafgaand aan acceptatie behoren ze (organisaties die persoonlijke gezondheidsinformatie verwerken) geschikte tests van het systeem uit te voeren.	Ja	Ja	Nee	Risico
ML.A.14.2.9.3	Systeemacceptatietests (3)	ZORGSPECIFIEKE BEHEERSMAATREGEL Klinische gebruikers moeten worden betrokken bij het testen van klinisch relevante systeemelementen.	Ja	Ja	Nee	Risico
ML.A.14.3	**Testgegevens**					
MK.A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja	Nee	Risico
ML.A.15	**Leveranciersrelaties**					
ML.A.15.1	**Informatiebeveiliging in leveranciersrelaties**					

MK.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	Nee	Risico
ML.A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die gezondheidsinformatie verwerken, moeten de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligings-beheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Risico
ML.A.15.2	**Beheer van dienstverlening van leveranciers**					
MK.A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
ML.A.16	**Beheer van informatiebeveiligingsincidenten**					
ML.A.16.1	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**					
MK.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	Nee	Best practice
MK.A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	Ja	Nee	Best practice

ML.A.16.1.2.1	Rapportage van informatiebeveiligingsgebeurtenissen (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vast te stellen: om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; om te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement; om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden. Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde openbaarmaking van persoonlijke gezondheidsinformatie of het niet langer beschikbaar zijn van gezondheidsinformatiesystemen waarbij dit niet beschikbaar zijn nadelige gevolgen heeft voor de zorg voor cliënten of bijdraagt aan nadelige klinische gebeurtenissen.	Ja	Ja	Nee	Best practice
ML.A.16.1.2.2	Rapportage van informatiebeveiligingsgebeurtenissen (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties behoren de cliënt altijd te informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt.	Ja	Ja	Nee	Best practice
ML.A.16.1.2.3	Rapportage van informatiebeveiligingsgebeurtenissen (3)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties behoren de cliënt op de hoogte te stellen als het niet beschikbaar zijn van gezondheidsinformatiesystemen negatieve gevolgen gehad kan hebben voor hun zorgverlening.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice
MK.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	Nee	Best practice
MK.A.16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Best practice

ML.A.17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**					
ML.A.17.1	**Informatiebeveiligingscontinuïteit**					
MK.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	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Best practice
ML.A.17.2	**Redundante componenten**					
MK.A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	Nee	Best practice
ML.A.18	**Naleving**					
ML.A.18.1	**Naleving van wettelijke en contractuele eisen**					
MK.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	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Risico
MK.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	Nee	Risico
ML.A.18.1.4.1	Privacy en bescherming van persoonsgegevens (1)	ZORGSPECIFIEKE BEHEERSMAATREGEL Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de geïnformeerde toestemming van cliënten te beheren.	Ja	Ja	Nee	Risico

ML.A.18.1.4.2	Privacy en bescherming van persoonsgegevens (2)	ZORGSPECIFIEKE BEHEERSMAATREGEL Waar mogelijk behoort geïnformeerde toestemming van cliënten te worden verkregen voordat persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.	Ja	Ja	Nee	Risico
MK.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	Nee	Best practice
ML.A.18.2	**Informatiebeveiligingsbeoordelingen**					
MK.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	Nee	Best practice
MK.A.18.2.2	Naleving van beveiligingsbeleid en -normen	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja	Nee	Best practice
MK.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	Nee	Best practice