

Verklaring van toepasselijkheid ISO 27001:2017 + A11:2020 NL NEN7510:2017 + A1:2020 NL Tribe Agency 8 maart 2023 versie 1.0		Van toepassing	Geïmplementeerd	Uitbesteed	Wet	Contract	Risico analyse	Reden uitsluiting
A.5	Informatiebeveiligingsbeleid							
A.5.1	Aansturing door de directie van de informatiebeveiliging	Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in						
	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden	Ja	Ja			X	
A.5.1.1	Zorgspecifieke beheersmaatregel: Beoordeling van het Informatiebeveiligingsbeleid	Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich	Ja	Ja			x	
A.5.1.2	Zorgspecifieke beheersmaatregel:	Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde	Ja	Ja			x	
A.6	Organiseren van informatiebeveiliging							
A.6.1	Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.						
	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	Organisaties moeten:	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	b) over een informatiebeveiligingsmanagementforum (IBMF) beschikken om te	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of	Ja	Ja			x	
A.6.1.1	Zorgspecifieke beheersmaatregel:	Er moet een formele verklaring van het toepassingsgebied worden geproduceerd	Ja	Ja			x	
	Scheiding van taken	Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om	Ja	Ja			x	
A.6.1.2	Zorgspecifieke beheersmaatregel:	Organisaties moeten, indien dit haalbaar is, plichten en	Ja	Ja				
A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden	Ja	Ja			x	
A.6.1.4	Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere	Ja	Ja			x	
	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het	Nee	Nee				
A.6.1.5	Zorgspecifieke beheersmaatregel:	Bij het management van projecten moet de patiëntveiligheid als projectrisico in						Tribe Agency heeft geen persoonlijke gezondheidsinformatie in projecten
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	Ja	Ja			x	
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden	Ja	Ja			x	
A.7	Veilig personeel							
A.7.1	Voorafgaand aan het dienstverband	Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.						
	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	Organisaties moeten minimaal de identiteit, het huidige adres en de vorige	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	Verificatiecontroles van de achtergrond van alle kandidaten voor een	Nee	Nee				Tribe Agency heeft geen zorgverleners in dienst.
A.7.1.1	Zorgspecifieke beheersmaatregel:	Als een persoon wordt ingehuurd voor een specifieke beveiligingsrol, moet de	Nee	Nee				Tribe Agency maakt geen gebruik van ingehuurde capaciteit voor specifieke beveiligingsrollen.
	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van	Ja	Ja			x	
A.7.1.2	Zorgspecifieke beheersmaatregel:	Er moet speciale aandacht worden besteed aan de rollen en	Nee	Nee				Tribe Agency maakt geen gebruik van inhuur tijdelijk personeel (Stagiaires, tijdelijk personeel)
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	Ja	Ja			x	
	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Alle medewerkers van de organisatie en, voor zover relevant, contractanten	Ja	Ja			x	
	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten	Ja	Ja				
A.7.2.2	Zorgspecifieke beheersmaatregel:	Werknemers van de organisatie en, waar relevant, derde-contractanten moeten	Ja	Ja				
A.7.2.3	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te	Ja	Ja			x	
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.						
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van	Ja	Ja			x	
A.8	Beheer van bedrijfsmiddelen							
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.						
	Inventariseren van bedrijfsmiddelen	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en	Ja	Ja			x	
	Zorgspecifieke beheersmaatregelen:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten:	Ja	Ja			x	
	Zorgspecifieke beheersmaatregelen:	b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie	Ja	Ja			x	
A.8.1.1	Zorgspecifieke beheersmaatregelen:	c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die	Ja	Ja			x	
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, moeten een	Ja	Ja			x	
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die	Ja	Ja			x	
	Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de	Ja	Ja			x	
A.8.1.4	Zorgspecifieke beheersmaatregel:	Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband,	Ja	Ja			x	
A.8.2	Informatieclassificatie	Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.						
	Classificatie van Informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen,	Ja	Ja			x	
A.8.2.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke	Ja	Ja				
	Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden	Ja	Ja			x	

A.12.1	Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.								
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld	Ja	Ja					x	
	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende	Ja	Ja					x	
A.12.1.2	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de	Ja	Ja					x	
A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten	Ja	Ja					x	
	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het	Ja	Ja					x	
A.12.1.4	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten	Ja	Ja					x	
A.12.2	Bescherming tegen Malware	Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn								
	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie,	Ja	Ja					x	
A.12.2.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste	Ja	Ja					x	
A.12.3	Back-up	Beschermen tegen het verlies van gegevens.								
	Back-up van informatie	Regelmatig moeten back-upkopieën van informatie, software en	Ja	Ja					x	
A.12.3.1	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups	Nee							Tribe Agency verwerkt geen gezondheidsinformatie
A.12.4	Verslaglegging en monitoren	Gebeurtenissen vastleggen en bewijs verzamelen.								
A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en	Ja	Ja					x	
	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen	Ja	Ja					x	
A.12.4.2	Zorgspecifieke beheersmaatregel:	Auditverslagen moeten beveiligd zijn en mogen niet gemanipuleerd kunnen	Ja	Ja					x	
A.12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en	Ja	Ja					x	
	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een	Ja	Ja					x	
A.12.4.4	Zorgspecifieke beheersmaatregel:	Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg	Nee							Tribe Agency heeft geen kloksynchronisatie voor de gezondheidszorg.
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	Ja	Ja					x	
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	Ja	Ja					x	
A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden	Ja	Ja					x	
A.12.7	Overwegingen betreffende audits van informatiesystemen	De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.								
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich	Ja	Ja					x	
A.13	Communicatiebeveiliging									
A.13.1	Beheer van netwerkbeveiliging	De bescherming van informatie in netwerken en de ondersteunende								
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en	Ja	Ja					x	
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle	Ja	Ja					x	
A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken	Ja	Ja					x	
A.13.2	Informatietransport	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een								
A.13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten	Ja	Ja					x	
A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van	Ja	Ja			x	x		
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten, moet passend beschermd	Ja	Ja					x	
	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de	Ja	Ja			x	x		
A.13.2.4	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten	Nee	Nee						Tribe Agency verwerkt geen gezondheidsinformatie
A.14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen									
A.14.1	Beveiligingseisen voor informatiesystemen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van								
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging moeten worden	Ja	Ja					x	
A.14.1.1.1	Zorgontvangers op unieke wijze identificeren Zorgspecifieke	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie	Nee	Nee						Tribe Agency verwerkt geen gezondheidsinformatie
A.14.1.1.2	Validatie van outputgegevens Zorgspecifieke beheersmaatregel	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie	Nee	Nee						Tribe Agency verwerkt geen gezondheidsinformatie
A.14.1.2	Toepassingen op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare	Ja	Ja					x	
A.14.1.3	Transacties van toepassingen beschermen	Informatie die deel uitmaakt van transacties van toepassingen, moet worden	Ja	Ja					x	
A.14.1.3.1	Openbaar beschikbare	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke	Nee						x	Tribe Agency verwerkt geen (openbare) gezondheidsinformatie
A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd								
A.14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden	Ja	Ja					x	
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten	Ja	Ja					x	
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bes	Als besturingsplatform zijn veranderd, moeten bedrijfskritische toepassingen	Ja	Ja					x	
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot	Ja	Ja					x	
A.14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden	Ja	Ja					x	
A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend	Ja	Ja					x	
A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden	Nee							Tribe Agency maakt geen gebruik van uitbestede softwareontwikkeling
A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Ja	Ja					x	
	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten	Ja	Ja					x	
A.14.2.9	Zorgspecifieke beheersmaatregel:	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten	Nee							Tribe Agency verwerkt geen gezondheidsinformatie
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					x	
A.15.1	Informatiebeveiliging in leveranciersrelaties	De bescherming waarborgen van bedrijfsmiddelen van de organisatie die								
	Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen	Ja	Ja					x	
A.15.1.1	Zorgspecifieke beheersmaatregel:	Organisaties die gezondheidsinformatie verwerken moeten de risico's in verband	Nee	Ja					x	Tribe Agency verwerkt geen gezondheidsinformatie

A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomst	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en	Ja	Ja			x	x		
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben	Ja	Ja				x		
A.15.2	Beheer van dienstverlening van leveranciers	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in								
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisatie moeten regelmatig de dienstverlening van leveranciers monitoren,	Ja	Ja				x		
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers met inbegrip van handhaving	Ja	Ja				x		
A.16	Beheer van informatie-beveiligingsincidenten									
A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van								
A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om	Ja	Ja				x		
A.16.1.2	Rapportage van informatiebeveiligings-gebeurtenissen Zorgspecifieke beheersmaatregel:	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste	Ja	Ja				x		
		Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten	Ja	Ja				x		
		Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde	Ja	Ja					x	
		Organisaties moeten de cliënt altijd informeren als er per ongeluk persoonlijke	Ja	Ja					x	
		Organisaties moeten de cliënt op de hoogte stellen als het niet beschikbaar zijn	Ja	Ja					x	
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen	Ja	Ja				x		
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiliging	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet	Ja	Ja				x		
A.16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in	Ja	Ja				x		
A.16.1.6	Lering uit informatiebeveiligingsincidenten	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op	Ja	Ja				x		
A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren,	Ja	Ja				x		
A.17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer									
A.17.1	Informatiebeveiligingscontinuïteit	Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het								
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	De organisatie moet haar eisen voor informatiebeveiliging en voor continuïteit van	Ja	Ja				x		
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen,	Ja	Ja				x		
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit	Ja	Ja				x		
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	Ja	Ja			x	x		
A.18	Naleving									
A.18.1	Naleving van wettelijke en contractuele eisen	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of								
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak	Ja	Ja			x	x		
A.18.1.2	Intellectuele-eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met	Ja	Ja			x	x		
A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende,	Ja	Ja			x	x		
A.18.1.4	Privacy en bescherming van persoonsgegevens Zorgspecifieke beheersmaatregel:	Privacy en bescherming van persoonsgegevens moeten, voor zover van	Ja	Ja			x	x		
		Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de	Nee	Nee					Tribe Agency kan geen geïnformeerde toestemming van cliënt verkrijgen omdat onze klant de zorgverlener is en niet de cliënt.	
		Waar mogelijk moet geïnformeerde toestemming van cliënten worden verkregen	Nee	Nee					Tribe Agency kan geen geïnformeerde toestemming van cliënt verkrijgen omdat onze klant de zorgverlener is en niet de cliënt.	
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in	Ja	Ja			x	x		
A.18.2	Informatiebeveiligingsbeoordelingen	Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in								
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van	Ja	Ja				x		
A.18.2.2	Naleving van beveiligingsbeleid en	Leidinggevend moeten regelmatig de naleving van de informatieverwerking en -	Ja	Ja			x	x		
A.18.2.3	Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de	Ja	Ja			x	x		