ISO/IEC 27001:2023

Verklaring van Toepasselijkheid

Gepubliceerd op | 17-02-2025
Versie | 5.0
Gepubliceerd door | Frank Schonewille

Scope

Informatiebeveiliging gerelateerd aan het leveren van het Vcare cloud telefonieplatform voor de zorgsector in overeenstemming met de Verklaring van Toepasselijkheid versie 5.0 17 februari 2025.

#	Titel	Beheersmaatregel	S	R	B	W	C	Status	Toelichting
A.5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoren te worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd	√	√				Gerealiseerd	

		aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld. *Doel: De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management overeenkomstig de bedrijfseisen en de eisen van wet- en regelgeving, statutaire en contractuele eisen bewerkstelligen.*							
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie. *Doel: Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.*	√	√				Gerealiseerd	
A.5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.	√	√				Gerealiseerd	

		Doel: Het risico op fraude, fouten en het omzeilen van beheersmaatregelen voor informatiebeveiliging verminderen.							
A.5.4	Managementverantwoordelijkheden	Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie. *Doel: Bewerkstelligen dat het management zijn rol bij informatiebeveiliging begrijpt en maatregelen neemt om ervoor te zorgen dat al het personeel zich bewust is van zijn verantwoordelijkheden op het gebied van informatiebeveiliging en deze ook nakomt.*	√	√				Gerealiseerd	
A.5.5	Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden. *Doel: Een passende stroom van informatie met betrekking tot informatiebeveiliging tussen de organisatie en relevante juridische, regelgevende en toezichthoudende instanties bewerkstelligen.*	√	√		√		Gerealiseerd	
A.5.6	Contact met speciale belangengroepen	De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.	√	√				Gerealiseerd	

		Doel: Een passende stroom van informatie met betrekking tot informatiebeveiliging bewerkstelligen.							
A.5.7	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren. *Doel: Bewustwording bieden van de mogelijke dreigingen voor de organisatie zodat de passende mitigerende maatregelen kunnen worden getroffen.*	√	√				Gerealiseerd	
A.5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement. *Doel: Ervoor zorgen dat informatiebeveiligingsrisico's binnen projecten en te leveren producten en diensten gedurende de gehele levenscyclus van het project op doeltreffende wijze binnen het projectmanagement worden aangepakt.*	√	√			√	Gerealiseerd	
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er behoort een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, te worden opgesteld en onderhouden.	√	√			√	Gerealiseerd	

		Doel: De informatie en andere gerelateerde bedrijfsmiddelen van de organisatie identificeren om de informatiebeveiliging ervan te behouden en passend eigenaarschap toe te wijzen.							
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden vastgesteld, gedocumenteerd en geïmplementeerd. *Doel: Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.*	√	√			√	Gerealiseerd	
A.5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren. *Doel: Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun*	√	√			√	Gerealiseerd	

		dienstverband, contract of overeenkomst te retourneren.							
A.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 belanghebbenden. *Doel: 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.*	√	√				Gerealiseerd	
A.5.13	Labelen van informatie	Om informatie te labelen behoort een passende reeks procedures te worden vastgesteld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. *Doel: 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.*	√	√				Gerealiseerd	
A.5.14	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.	√	√			√	Gerealiseerd	

		Doel: 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.							
A.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. *Doel: 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.*	√	√				Gerealiseerd	
A.5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd. *Doel: De unieke identificatie van personen en systemen die toegang hebben tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, en een juiste toewijzing van toegangsrechten mogelijk maken.*	√	√			√	Gerealiseerd	
A.5.17	Beheren van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het	√	√				Gerealiseerd	

		informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt. *Doel: De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.*							
A.5.18	Toegangsrechten	Toegangsrechten met betrekking tot 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. *Doel: 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.*	√	√			√	Gerealiseerd	
A.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 beheren.	√	√			√	Gerealiseerd	

		Doel: 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.							
A.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. *Doel: Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.*	√	√			√	Gerealiseerd	
A.5.21	Beheren van informatiebeveiliging in de ICT-keten	Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren. *Doel: Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.*	√	√		√	√	Gerealiseerd	
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	√	√			√	Gerealiseerd	

		Doel: De organisatie behoort de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.							
A.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. *Doel: Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.*	√	√				Gerealiseerd	
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiliging sincidenten	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. *Doel: De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door*	√	√				Gerealiseerd	

		processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.							
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten. *Doel: Doeltreffende categorisering en prioritering van informatiebeveiligingsgebeurtenissen bewerkstelligen.*	√	√				Gerealiseerd	
A.5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. *Doel: Een doelmatige en doeltreffende reactie op informatiebeveiligingsincidenten bewerkstelligen.*	√	√				Gerealiseerd	
A.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. *Doel: De waarschijnlijkheid of de gevolgen van toekomstige incidenten verminderen.*	√	√				Gerealiseerd	

A.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. *Doel: In het kader van disciplinaire en gerechtelijke stappen consistent en doeltreffend beheer bewerkstelligen van bewijsmateriaal in verband met informatiebeveiligingsincidenten.*	√	√				Gerealiseerd	
A.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. *Doel: De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.*	√	√			√	Gerealiseerd	
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen. *Doel: De beschikbaarheid van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie tijdens een verstoring waarborgen.*	√	√				Gerealiseerd	
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Eisen van wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de	√	√		√	√	Gerealiseerd	

		organisatie om aan deze eisen te voldoen behoren te worden vastgesteld, gedocumenteerd en actueel gehouden. *Doel: De naleving bewerkstelligen van wettelijke, statutaire, regelgevende en contractuele eisen in verband met informatiebeveiliging.*							
A.5.32	Intellectuele-eigendomsrechten	De organisatie behoort passende procedures te implementeren om intellectuele eigendomsrechten te beschermen. *Doel: De naleving bewerkstelligen van eisen van wet- en regelgeving, statutaire en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van gepatenteerde producten.*	√	√		√	√	Gerealiseerd	
A.5.33	Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave. *Doel: De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen, alsmede gemeenschaps- of maatschappelijke verwachtingen, met betrekking tot de bescherming en beschikbaarheid van registraties.*	√	√		√	√	Gerealiseerd	
A.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	√	√		√	√	Gerealiseerd	

		wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen. *Doel: De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot de informatiebeveiligingsaspecten voor de bescherming van persoonsgegevens.*							
A.5.35	Onafhankelijke review 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. *Doel: Waarborgen dat de organisatie continu een geschikte, toereikende en doeltreffende aanpak voor het beheer van informatiebeveiliging hanteert.*	√	√				Gerealiseerd	
A.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. *Doel: Bewerkstelligen dat informatiebeveiliging in overeenstemming met het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en normen van*	√	√				Gerealiseerd	

		de organisatie wordt geïmplementeerd en uitgevoerd.							
A.5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft. *Doel: De correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.*	√	√				Gerealiseerd	
A.6.1	Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie 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, voorschriften en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's. *Doel: Bewerkstelligen dat al het personeel in aanmerking komt en geschikt is voor de functies waarvoor zij worden overwogen en dat zij hiervoor gedurende hun dienstverband in aanmerking blijven komen en geschikt blijven.*	√	√				Gerealiseerd	

A.6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging. *Doel: Bewerkstelligen dat personeel begrijpt wat hun verantwoordelijkheden zijn op het gebied van informatiebeveiliging voor de rollen waarvoor zij mogelijk in aanmerking komen.*	√	√			√	Gerealiseerd	
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passend(e) bewustwording van, opleiding, training en bijscholing in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen. *Doel: Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.*	√	√				Gerealiseerd	
A.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.	√	√			√	Gerealiseerd	

		Doel: Bewerkstelligen dat personeel en andere relevante belanghebbenden de gevolgen begrijpen van schending van het informatiebeveiligingsbeleid, personeel en andere relevante belanghebbenden ervan weerhouden zich schuldig te maken aan een schending, en personeel en andere relevante belanghebbenden die zich schuldig hebben gemaakt aan een schending op de juiste manier aanpakken.							
A.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. *Doel: De belangen van de organisatie beschermen als onderdeel van de wijzigings- of beëindigingsprocedure van dienstverband of contracten.*	√	√			√	Gerealiseerd	
A.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.	√	√			√	Gerealiseerd	

		Doel: De vertrouwelijkheid van informatie waartoe personeel of externe partijen toegang hebben handhaven.							
A.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. *Doel: De beveiliging van informatie waarborgen wanneer personeel op afstand werkt.*	√	√			√	Gerealiseerd	
A.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. *Doel: Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen die door personeel kunnen worden geïdentificeerd.*	√	√				Gerealiseerd	
A.7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.	√	√			√	Gerealiseerd	

		Doel: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie voorkomen.							
A.7.2	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangscontroles en toegangspunten. *Doel: Bewerkstelligen dat er alleen bevoegde fysieke toegang tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie plaatsvindt.*	√	√			√	Gerealiseerd	
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd. *Doel: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie in kantoren, ruimten en faciliteiten voorkomen.*	√	√				Gerealiseerd	
A.7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang. *Doel: Onbevoegde fysieke toegang detecteren en ontmoedigen.*	√	√				Gerealiseerd	

A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, te worden ontworpen en geïmplementeerd. *Doel: De gevolgen van gebeurtenissen die voortvloeien uit fysieke en omgevingsdreigingen, voorkomen of beperken.*	√	√		√	Gerealiseerd	
A.7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd. *Doel: Informatie en andere gerelateerde bedrijfsmiddelen in beveiligde zones beschermen tegen schade en onbevoegde verstoring door personeel dat in deze zones aan het werk is.*	√	√				Gerealiseerd	
A.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 ten uitvoer worden gebracht. *Doel: De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen*	√	√				Gerealiseerd	

		tijdens en buiten de gebruikelijke werkuren beperken.							
A.7.8	Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd. *Doel: De risico's op fysieke en omgevingsdreigingen en op toegang door onbevoegden en schade beperken.*	√	√				Gerealiseerd	
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd. *Doel: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen buiten het gebouw en/of terrein en onderbreking van de bedrijfsvoering van de organisatie voorkomen.*	√	√				Gerealiseerd	
A.7.10	Opslagmedia	Opslagmedia behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie. *Doel: Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.*	√	√				Gerealiseerd	
A.7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en	√	√				Gerealiseerd	

		andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen. *Doel: Verlies, schade of compromittering van informatie en andere gerelateerde bedrijfsmiddelen of onderbreking van de bedrijfsvoering van de organisatie vanwege verstoring en ontregeling van ondersteunende nutsvoorzieningen voorkomen.*							
A.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. *Doel: Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie in verband met voedings- en communicatiekabels voorkomen.*	√	√		√		Gerealiseerd	
A.7.13	Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.	√	√				Gerealiseerd	

		Doel: Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie door gebrekkig onderhoud voorkomen.							
A.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. *Doel: Het lekken van informatie via af te voeren of te hergebruiken apparatuur voorkomen.*	√	√				Gerealiseerd	
A.8.1	Gebruikersapparatuur	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd. *Doel: Informatie beschermen tegen de risico's als gevolg van het gebruik van 'user endpoint devices'.*	√	√			√	Gerealiseerd	
A.8.2	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd. *Doel: Bewerkstelligen dat alleen bevoegde gebruikers, softwarecomponenten en diensten speciale toegangsrechten krijgen.*	√	√				Gerealiseerd	

A.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. *Doel: De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging*	√	√				Gerealiseerd	
A.8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd. *Doel: Voorkomen dat er ongeoorloofde functionaliteit wordt geïntroduceerd, vermijden dat onbedoelde of kwaadwillige wijzigingen plaatsvinden en de vertrouwelijkheid behouden van waardevol intellectueel eigendom.*	√	√				Gerealiseerd	
A.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 of aanvullende beleid inzake toegangsbeveiliging.	√	√				Gerealiseerd	

		Doel: Bewerkstelligen dat een gebruiker of een entiteit veilig wordt geauthenticeerd wanneer toegang tot systemen, toepassingen en diensten wordt verleend.							
A.8.6	Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen. *Doel: De vereiste capaciteit van informatieverwerkende faciliteiten, personeel, kantoren en andere faciliteiten waarborgen.*	√	√				Gerealiseerd	
A.8.7	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn. *Doel: Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.*	√	√				Gerealiseerd	
A.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. *Doel: Misbruik van technische kwetsbaarheden voorkomen.*	√	√			√	Gerealiseerd	

A.8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld. *Doel: Garanderen dat hardware, software, diensten en netwerken correct met de vereiste beveiligingsinstellingen functioneren en de configuratie niet door ongeautoriseerde of onjuiste wijzigingen wordt gewijzigd.*	√	√				Gerealiseerd	
A.8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer nodig is. *Doel: Onnodige openbaarmaking van gevoelige informatie voorkomen en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voor het wissen van informatie voldoen.*	√	√				Gerealiseerd	
A.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.	√	√				Gerealiseerd	

		Doel: De openbaarmaking van gevoelige informatie met inbegrip van persoonsgegevens beperken en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voldoen.							
A.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. *Doel: Om de ongeoorloofde openbaarmaking en extractie van informatie door personen of systemen te detecteren en te voorkomen.*	√	√				Gerealiseerd	
A.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. *Doel: Herstel mogelijk maken na verlies van gegevens of systemen.*	√	√				Gerealiseerd	
A.8.14	Redundantie van informatieverwerken de faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. *Doel: De ononderbroken werking van informatieverwerkende faciliteiten waarborgen.*	√	√			√	Gerealiseerd	

A.8.15	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd te worden geproduceerd, opgeslagen, beschermd en geanalyseerd. *Doel: Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen leiden en onderzoeken ondersteunen.*	√	√				Gerealiseerd	
A.8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te evalueren. *Doel: Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.*	√	√				Gerealiseerd	
A.8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen. *Doel: De correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere*	√	√				Gerealiseerd	

		geregistreerde gegevens mogelijk maken en onderzoeken bij informatiebeveiligingsincidenten ondersteunen.							
A.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. *Doel: Bewerkstelligen dat het gebruik van systeemhulpmiddelen geen schade toebrengt aan systeem- en toepassingsbeheersmaatregelen voor informatiebeveiliging.*	√	√				Gerealiseerd	
A.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. *Doel: De integriteit van operationele systemen garanderen en voorkomen dat misbruik wordt gemaakt van technische kwetsbaarheden.*	√	√				Gerealiseerd	
A.8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen. *Doel: Informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten*	√	√				Gerealiseerd	

		beschermen tegen compromittering via het netwerk.							
A.8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord. *Doel: De beveiliging bij het gebruik van netwerkdiensten waarborgen.*	√	√		√	√	Gerealiseerd	
A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd. *Doel: Het netwerk opsplitsen met beveiligingsgrenzen en het verkeer ertussen op basis van de bedrijfsbehoeften beheersen.*	√	√				Gerealiseerd	
A.8.23	Toepassen van webfilters	De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken. *Doel: Systemen beschermen om te voorkomen dat ze door malware worden gecompromitteerd en om toegang tot ongeoorloofde internetbronnen te voorkomen.*	√	√				Gerealiseerd	
A.8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van	√	√				Gerealiseerd	

		cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd. *Doel: Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.*							
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast. *Doel: Bewerkstelligen dat informatiebeveiliging binnen de veilige ontwikkelcyclus van software en systemen wordt ontworpen en geïmplementeerd.*	√	√				Gerealiseerd	
A.8.26	Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen. *Doel: Garanderen dat alle informatiebeveiligingseisen zijn geïdentificeerd en meegenomen bij het ontwikkelen of aanschaffen van toepassingen.*	√	√			√	Gerealiseerd	

A.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. *Doel: Waarborgen dat informatiesystemen veilig worden ontworpen, geïmplementeerd en beheerd binnen de ontwikkelingslevenscyclus.*	√	√				Gerealiseerd	
A.8.28	Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling. *Doel: Waarborgen dat veilige software wordt geschreven waardoor het aantal potentiële informatiebeveiligingskwetsbaarheden in de software wordt beperkt.*	√	√				Gerealiseerd	
A.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. *Doel: Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.*	√	√			√	Gerealiseerd	
A.8.30	Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.						Niet van toepassing	Vcare besteedt geen ontwikkeling uit.

		Doel: Garanderen dat de door de organisatie vereiste informatiebeveiligingsmaatregelen bij uitbestede systeemontwikkeling worden geïmplementeerd.							
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd. *Doel: De productieomgeving en de gegevens beschermen tegen compromittering door ontwikkel- en testactiviteiten.*	√	√				Gerealiseerd	
A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer. *Doel: De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.*	√	√				Gerealiseerd	
A.8.33	Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd. *Doel: De relevantie van het testen en de bescherming van operationele gegevens die voor het testen worden gebruikt, waarborgen.*	√	√				Gerealiseerd	
A.8.34	Bescherming van informatiesystemen tijdens audits	Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld behoren te worden gepland en	√	√				Gerealiseerd	

		overeengekomen tussen de tester en het verantwoordelijke management. *Doel: De impact van audittests en andere auditactiviteiten op operationele systemen en bedrijfsprocessen tot een minimum beperken.*							