

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A	Organisatorische beheersmaatregelen	Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie				
					WR	CE	BR	RA	
A.5	Organisatorische beheersmaatregelen	Organisatorische beheersmaatregelen							
A.5.1	Beleidsregels voor informatiebeveiliging	Beleidsregels voor informatiebeveiliging Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	Ja			■	■		
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja			■	■		
A.5.3	Functiescheiding	Functiescheiding Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja			■		■	
A.5.4	Managementverantwoordelijkheden	Managementverantwoordelijkheden Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	Ja			■		■	
A.5.5	Contact met overheidsinstanties	Contact met overheidsinstanties De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja			■		■	
A.5.6	Contact met speciale belangengroepen	Contact met speciale belangengroepen De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja					■	
A.5.7	Threat intelligence (informatie en analyse over dreigingen)	Informatie en analyses over dreigingen Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja				■	■	■
A.5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging in projectmanagement Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja					■	

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A	Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
				WR	CE	BR	RA
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja				■	
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen 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 moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja			■	■	■
A.5.11	Retourneren van bedrijfsmiddelen Retourneren van bedrijfsmiddelen Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja				■	■
A.5.12	Classificeren van informatie Classificeren van informatie Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Ja				■	
A.5.13	Labelen van informatie Labelen van informatie Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Nee	Vanuit de risicoanalyse is niet gebleken dat maatregelen noodzakelijk zijn om de (bedrijfs)informatie te labelen				
A.5.14	Overdragen van informatie Overdragen van informatie Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Ja			■	■	■
A.5.15	Toegangsbeveiliging Toegangsbeveiliging Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja				■	■
A.5.16	Identiteitsbeheer Identiteitsbeheer De volledige levenscyclus van identiteiten moet worden beheerd.	Ja				■	

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A		Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
					WR	CE	BR	RA
A.5.17	Beheren van authenticatie-informatie	Authenticatie-informatie De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja			■	■	■
A.5.18	Toegangsrechten	Toegangsrechten Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja			■	■	■
A.5.19	Informatiebeveiliging in leveranciersrelaties	Informatiebeveiliging in leveranciersrelaties Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	Ja					■
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Adresseren van informatiebeveiliging in leveranciersovereenkomsten Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja			■	■	■
A.5.21	Beheren van informatiebeveiliging in de ICT-keten	Beheren van informatiebeveiliging in de ICT-toeleveringsketen Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	Ja					■
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja					■
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Informatiebeveiliging voor het gebruik van clouddiensten Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja			■	■	■

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A		Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie				
					WR	CE	BR	RA	
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Plannen en voorbereiden van het beheer van informatiebeveiligings-incidenten De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie-beveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja				■		
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja				■		
A.5.26	Reageren op informatiebeveiligingsincidenten	Reageren op informatiebeveiligingsincidenten Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja			■	■	■	
A.5.27	Leren van informatiebeveiligingsincidenten	Leren van informatiebeveiligingsincidenten Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja			■	■		
A.5.28	Verzamelen van bewijsmateriaal	Verzamelen van bewijsmateriaal De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja			■	■		
A.5.29	Informatiebeveiliging tijdens een verstoring	Informatiebeveiliging tijdens een verstoring De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja				■		
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	ICT-gereedheid voor bedrijfscontinuïteit De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoel-stellingen en ICT-continuïteitseisen.	Ja				■	■	
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	Ja			■	■	■	■

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A	Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
				WR	CE	BR	RA
A.5.32	Intellectuele-eigendomsrechten De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	Ja		■		■	
A.5.33	Beschermen van registraties Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja		■		■	
A.5.34	Privacy en bescherming van persoonsgegevens De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	Ja		■	■	■	■
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja			■	■	
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 moet regelmatig worden beoordeeld.	Ja		■	■	■	■
A.5.37	Gedocumenteerde bedieningsprocedures Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja				■	

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A	Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
				WR	CE	BR	RA
A.6	Mensgerichte beheersmaatregelen						
A.6.1	Screening	Nee	Er vindt geen screening plaats. Mensen moeten binnen het (kleine) team passen. Wel wordt een VOG verlangd. Deze wordt getoond en niet opgeslagen in het dossier.				
A.6.2	Arbeidsovereenkomst	Ja		■	■	■	
A.6.3	Bewustwording, opleiding en training in informatiebeveiliging	Ja			■	■	■
A.6.4	Disciplinaire procedure	Ja		■	■	■	■
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Ja			■	■	■

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A		Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
					WR	CE	BR	RA
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja			■	■	■
A.6.7	Werken op afstand	Werken op afstand Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja				■	■
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	Melden van informatiebeveiligingsgebeurtenissen De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings-gebeurtenissen tijdig via passende kanalen kan melden.	Ja			■	■	
A.7	Fysieke beheersmaatregelen	Fysieke beheersmaatregelen						
A.7.1	Fysieke beveiligingszones	Fysieke beveiligingszones Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja			■	■	
A.7.2	Fysieke toegangsbeveiliging	Fysieke toegangsbeveiliging Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Ja			■	■	
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Beveiligen van kantoren, ruimten en faciliteiten Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja			■	■	■
A.7.4	Monitoren van de fysieke beveiliging	Monitoren van de fysieke beveiliging Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja			■	■	■
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Beschermen tegen fysieke en omgevingsdreigingen Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	Ja			■	■	■
A.7.6	Werken in beveiligde zones	Werken in beveiligde zones Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Nee	Output4You beschikt niet/ werkt niet met/ in beveiligde zones				

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A		Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
					WR	CE	BR	RA
A.7.7	'Clear desk' en 'clear screen'	'Clear desk' en 'clear screen' Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	Ja				■	■
A.7.8	Plaatsen en beschermen van apparatuur	Plaatsen en beschermen van apparatuur Apparatuur moet veilig worden geplaatst en beschermd.	Ja					■
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Beveiligen van bedrijfsmiddelen buiten het terrein Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja			■		■
A.7.10	Opslagmedia	Opslagmedia Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja					■ ■
A.7.11	Nutsvoorzieningen	Nutsvoorzieningen Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja				■	■
A.7.12	Beveiligen van bekabeling	Beveiligen van bekabeling Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja				■	■
A.7.13	Onderhoud van apparatuur	Onderhoud van apparatuur Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja				■	■ ■
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Veilig verwijderen of hergebruiken van apparatuur Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja				■	■ ■

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A	Technologische beheersmaatregelen	Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
					WR	CE	BR	RA
A.8	Technologische beheersmaatregelen	Technologische beheersmaatregelen						
A.8.1	'User endpoint devices'	User endpoint devices' Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja			■	■	
A.8.2	Speciale toegangsrechten	Speciale toegangsrechten Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja			■	■	
A.8.3	Beperking toegang tot informatie	Beperking toegang tot informatie De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja			■	■	
A.8.4	Toegangsbeveiliging op broncode	Toegangsbeveiliging op broncode Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja					■
A.8.5	Beveiligde authenticatie	Beveiligde authenticatie Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja			■	■	■
A.8.6	Capaciteitsbeheer	Capaciteitsbeheer Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja			■	■	
A.8.7	Bescherming tegen malware	Bescherming tegen malware Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja			■	■	■
A.8.8	Beheer van technische kwetsbaarheden	Beheer van technische kwetsbaarheden Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.	Ja			■	■	■
A.8.9	Configuratiebeheer	Configuratiebeheer Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja				■	■

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A	Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
				WR	CE	BR	RA
A.8.10	Wissen van informatie Wissen van informatie In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja		■		■	■
A.8.11	Maskeren van gegevens Maskeren van gegevens Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Nee	Standaard vindt maskering op wachtwoorden plaats. Vanuit de risicoanalyse is niet gebleken dat aanvullende maskering noodzakelijk is.				
A.8.12	Voorkomen van gegevenslekken (Data leakage prevention) Voorkomen van gegevenslekken (data leakage prevention) Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja			■	■	■
A.8.13	Back-up van informatie Back-up van informatie Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja		■	■	■	
A.8.14	Redundantie van informatieverwerkende faciliteiten Redundantie van informatieverwerkende faciliteiten Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja			■	■	■
A.8.15	Logging Logging Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja			■	■	■
A.8.16	Monitoren van activiteiten Monitoren van activiteiten Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja			■	■	■
A.8.17	Kloksynchronisatie Kloksynchronisatie De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja				■	

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A		Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
					WR	CE	BR	RA
A.8.18	Gebruik van speciale systeemhulpmiddelen	Gebruik van speciale systeemhulpmiddelen Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja				■	
A.8.19	Installeren van software op operationele systemen	Installeren van software op operationele systemen Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja				■	■
A.8.20	Beveiliging netwerkcomponenten	Beveiliging netwerkcomponenten Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja			■	■	
A.8.21	Beveiliging van netwerkdiensten	Beveiliging van netwerkdiensten Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja			■	■	■
A.8.22	Netwerksegmentatie	Netwerksegmentatie Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja			■	■	■
A.8.23	Toepassen van webfilters	Toepassen van webfilters De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja				■	■
A.8.24	Gebruik van cryptografie	Gebruik van cryptografie Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja			■		■
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Beveiligen tijdens de ontwikkelcyclus Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja					■
A.8.26	Toepassingsbeveiligingseisen	Toepassingsbeveiligingseisen Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja					■

Verklaring van Toepasselijkheid ISO27001:2022

v1.1 van 19-03-2026

Index: **WR:** Wet- en Regelgeving, **CE:** Contractuele Eis, **BR:** Business Requirements, **RA:** Risico Analyse

Nummer	Toepasselijkheid van maatregelen ISO 27001:2022 Bijlage A		Geselecteerd & geïmplementeerd Ja / Nee	Onderbouwing indien niet geselecteerd	Reden van selectie			
					WR	CE	BR	RA
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Veilige systeemarchitectuur en technische uitgangspunten Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja				■	
A.8.28	Veilig coderen	Veilig coderen Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja				■	
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Testen van de beveiliging tijdens ontwikkeling en acceptatie Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja				■	
A.8.30	Uitbestede systeemontwikkeling	Uitbestede systeemontwikkeling De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Output4you heeft geen software ontwikkeling uitbesteed en maakt uitsluiten gebruik van Commercial Of The Shelve (COTS) software				
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Scheiding van ontwikkel-, test- en productieomgevingen Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja				■	
A.8.32	Wijzigingsbeheer	Wijzigingsbeheer Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja			■	■	■
A.8.33	Testgegevens	Testgegevens Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja				■	
A.8.34	Bescherming van informatiesystemen tijdens audits	Bescherming van informatiesystemen tijdens audits Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja				■	