

Verklaring van Toepasselijkheid ISO/IEC 27001:2022

Datum:	22-5-2025
Auteur:	HumanCapitalCare B.V.
Versie:	4.0
Documenttype:	Verklaring van Toepasselijkheid
Classificatie:	Intern openbaar - normale persoonsgegevens
Distributie:	Medewerkers en klanten HumanCapitalCare
Eigenaar:	Algemeen directeur
Status:	Definitief

Inhoud

Inleiding.....	2
1. Scope.....	3
2. Verklaring van Toepasselijkheid.....	3

Inleiding

Verklaring van Toepasselijkheid

De directie is verantwoordelijk voor het vaststellen van het informatiebeveiligingsbeleid, dat onderdeel uitmaakt van het kwaliteitsbeleid van HumanCapitalCare. Bij de uitvoering en implementatie wordt de directie ondersteund door de afdeling Kwaliteit & Certificeringen.

Binnen het ondernemingsbeleid is het informatiebeveiligingsbeleid gericht op het bereiken van een zo optimaal mogelijke beveiliging van de informatie die aansluit op de eisen van de klanten en voldoet aan wet- en regelgeving. Het informatiebeveiligingsbeleid voldoet onder andere aan de vereiste normen zoals gesteld in Certificatieschema Arbodiensten d.d. 9 november 2018, ISO/IEC 27001:2022, NEN 7510:2017 en de Algemene Verordening Gegevensbescherming.

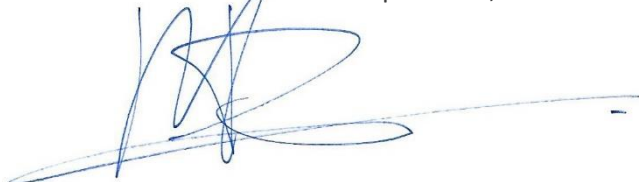
Alle medewerkers worden actief betrokken bij de invulling, implementatie, uitvoering en verbetering van het informatiebeveiligingsbeleid en worden tijdig geïnformeerd over aanpassingen of veranderingen in dit beleid.

Dit document omvat de Verklaring van Toepasselijkheid (VvT) ten behoeve van de certificering voor de ISO/IEC 27001:2022 standaard. De Verklaring van Toepasselijkheid bevat een omschrijving van de scope, toepassingsgebied en opsomming van de maatregelen waaraan voldaan moet worden en wordt, tenzij aangegeven dat maatregelen worden uitgesloten.

Directieverklaring

Deze Verklaring van Toepasselijkheid, die door de directie van HumanCapitalCare is vastgesteld op 22 mei 2025 en ondertekend door de algemeen directeur, is opgesteld in het kader van de ISO/IEC 27001:2022.

Vastgesteld d.d. 22 mei 2025 ,
namens de directie HumanCapitalCare,



M. Dekker
Algemeen Directeur

1. Scope

De scope betreft: alle organisatieonderdelen en processen die worden ingezet bij de dienstverlening op het gebied van arbeid, gezondheid en preventie, waarbij privacy en de beveiliging van persoonsgegevens gewaarborgd zijn.

HumanCapitalCare vertrouwt voor software-oplossingen op externe leveranciers, waardoor maatregelen met betrekking tot softwareontwikkeling zijn uitgesloten.

2. Verklaring van Toepasselijkheid

HumanCapitalCare houdt toezicht op de maatregelen die (deels) zijn uitbesteed aan IT&Care, die evenals HumanCapitalCare deel uit maakt van HumanTotalCare.

ISO/IEC 27001:2022

Verklaring van Toepasselijkheid

		Van toepassing	Geïmplementeerd bij HumanCapitalCare	Geïmplementeerd met uitbesteding aan IT&Care	Wet & Regelgeving	Best practice	Risico analyse	Toelichting:
A.5	Organisatorische beheersmaatregelen							
A.5.1	Beleidsregels voor informatiebeveiliging	Ja	Ja	√			X	
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja	√			X	
A.5.3	Functiescheiding	Ja	Ja	√	X		X	
A.5.4	Managementverantwoordelijkheden	Ja	Ja				X	
A.5.5	Contact met overheidsinstanties	Ja	Ja		X		X	
A.5.6	Contact met speciale belangengroepen	Ja	Ja	√			X	
A.5.7	Informatie en analyses over dreigingen	Ja	Ja	√			X	
A.5.8	Informatiebeveiliging in projectmanagement	Ja	Ja	√			X	
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Ja	Ja	√			X	
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Ja	Ja	√	X		X	
A.5.11	Retourneren van bedrijfsmiddelen	Ja	Ja	√			X	
A.5.12	Classificeren van informatie	Ja	Ja	√	X		X	
A.5.13	Labelen van informatie	Ja	Ja	√	X		X	
A.5.14	Overdragen van informatie	Ja	Ja	√			X	
A.5.15	Toegangsbeveiliging	Ja	Ja	√			X	
A.5.16	Identiteitsbeheer	Ja	Ja	√			X	

A.5.17	Authenticatie-informatie	Ja	Ja	√			X	
A.5.18	Toegangsrechten	Ja	Ja	√			X	
A.5.19	Informatiebeveiliging in leveranciersrelaties	Ja	Ja	√			X	
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Ja	Ja	√			X	
A.5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Ja	Ja	√			X	
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Ja	Ja	√			X	
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Ja	Ja	√			X	
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Ja	Ja	√			X	
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Ja	Ja	√			X	
A.5.26	Reageren op informatiebeveiligingsincidenten	Ja	Ja	√	X		X	
A.5.27	Leren van informatiebeveiligingsincidenten	Ja	Ja	√			X	
A.5.28	Verzamelen van bewijsmateriaal	Ja	Ja	√	X		X	
A.5.29	Informatiebeveiliging tijdens een verstoring	Ja	Ja	√			X	
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	Ja	Ja	√			X	
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Ja	Ja	√	X		X	
A.5.32	Intellectuele-eigendomsrechten	Ja	Ja	√	X		X	
A.5.33	Beschermen van registraties	Ja	Ja	√	X		X	
A.5.34	Privacy en bescherming van persoonsgegevens	Ja	Ja	√	X		X	
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	Ja	Ja	√			X	

A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Ja	Ja	√			X	
A.5.37	Gedocumenteerde bedieningsprocedures	Ja	Ja	√			X	

A.6	Mensgerichte beheersmaatregelen							
A.6.1	Screening	Ja	Ja				X	
A.6.2	Arbeidsovereenkomst	Ja	Ja				X	
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Ja	Ja				X	
A.6.4	Disciplinaire procedure	Ja	Ja				X	
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Ja	Ja	√			X	
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Ja	Ja	√			X	
A.6.7	Werken op afstand	Ja	Ja	√			X	
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	Ja	Ja	√			X	

A.7	Fysieke beheersmaatregelen							
A.7.1	Fysieke beveiligingszones	Ja	Ja				X	
A.7.2	Fysieke toegangsbeveiliging	Ja	Ja				X	
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Ja	Ja				X	
A.7.4	Monitoren van de fysieke beveiliging	Ja	Ja				X	
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Ja	Ja				X	
A.7.6	Werken in beveiligde zones	Ja	Ja				X	
A.7.7	'Clear desk' en 'clear screen'	Ja	Ja				X	
A.7.8	Plaatsen en beschermen van apparatuur	Ja	Ja				X	
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Ja	Ja	√			X	

A.7.10	Opslagmedia	Ja	Ja	√			X	
A.7.11	Nutsvoorzieningen	Ja	Ja	√			X	
A.7.12	Beveiligen van bekabeling	Ja	Ja	√			X	
A.7.13	Onderhoud van apparatuur	Ja	Ja	√			X	
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Ja	Ja	√			X	

A.8	Technologische beheersmaatregelen							
A.8.1	'User endpoint devices'	Ja	Ja	√			X	
A.8.2	Speciale toegangsrechten	Ja	Ja	√			X	
A.8.3	Beperking toegang tot informatie	Ja	Ja	√			X	
A.8.4	Toegangsbeveiliging op broncode	Nee						HumanCapitalCare ontwikkelt geen software
A.8.5	Beveiligde authenticatie	Ja	Ja	√			X	
A.8.6	Capaciteitsbeheer	Ja	Ja	√			X	
A.8.7	Bescherming tegen malware	Ja	Ja	√	X		X	
A.8.8	Beheer van technische kwetsbaarheden	Ja	Ja	√			X	
A.8.9	Configuratiebeheer	Ja	Ja	√			X	
A.8.10	Wissen van informatie	Ja	Ja	√			X	
A.8.11	Maskeren van gegevens	Nee						HumanCapitalCare ontwikkelt geen software
A.8.12	Voorkomen van gegevenslekken (data leakage prevention)	Ja	Ja	√			X	
A.8.13	Back-up van informatie	Ja	Ja	√			X	
A.8.14	Redundantie van informatieverwerkende faciliteiten	Ja	Ja	√			X	
A.8.15	Logging	Ja	Ja	√	X		X	
A.8.16	Monitoren van activiteiten	Ja	Ja	√			X	

A.8.17	Kloksynchronisatie	Ja	Ja	√			X	
A.8.18	Gebruik van speciale systeemhulpmiddelen	Ja	Ja	√			X	
A.8.19	Installeren van software op operationele systemen	Ja	Ja	√			X	
A.8.20	Beveiliging netwerkcomponenten	Ja	Ja	√			X	
A.8.21	Beveiliging van netwerkdiensten	Ja	Ja	√			X	
A.8.22	Netwerksegmentatie	Ja	Ja	√			X	
A.8.23	Toepassen van webfilters	Ja	Ja	√			X	
A.8.24	Gebruik van cryptografie	Ja	Ja	√	X		X	
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Nee						HumanCapitalCare ontwikkelt geen software
A.8.26	Toepassingsbeveiligingseisen	Ja	Ja	√	X		X	
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Nee						HumanCapitalCare ontwikkelt geen software
A.8.28	Veilig coderen	Nee						HumanCapitalCare ontwikkelt geen software
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Nee						HumanCapitalCare ontwikkelt geen software
A.8.30	Uitbestede systeemontwikkeling	Nee						HumanCapitalCare ontwikkelt geen software
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Nee						HumanCapitalCare ontwikkelt geen software
A.8.32	Wijzigingsbeheer	Ja	Ja	√			X	
A.8.33	Testgegevens	Nee						HumanCapitalCare ontwikkelt geen software
A.8.34	Bescherming van informatiesystemen tijdens audits	Ja	Ja	√			X	