

Verklaring van Toepasselijkheid ISO/IEC 27001:2013

Datum:	11-11-2024
Auteur:	HumanCapitalCare B.V.
Versie:	3.0
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, Informatiebeveiliging en Privacy.

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, meest recente normen zoals gesteld in Certificatieschema Arbodiensten d.d. 9 november 2018, ISO/IEC 27001:2013, 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 27001:2013 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 11 november 2024 en ondertekend door de algemeen directeur, is opgesteld in het kader van de ISO/IEC 27001:2013.

Vastgesteld d.d. 11 november 2024,
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 27001:2013

Verklaring van Toepasselijkheid

		Van toepassing	Geïmplementeerd bij HumanCapitalCare	Geïmplementeerd d.m.v. uitbesteding aan IT&Care	Wet & Regelgeving	Best practice	Risico analyse	Toelichting:
A.5	Informatiebeveiligingsbeleid							
A.5.1	Aansturing door de directie van de informatiebeveiliging							
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ja	Ja	Ja			X	
A.5.1.2	Beoordeling van het Informatiebeveiligingsbeleid	Ja	Ja	Ja			X	
A.6	Organiseren van informatiebeveiliging							
A.6.1	Interne organisatie							
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja	Ja			X	
A.6.1.2	Scheiding van taken	Ja	Ja	Ja	X		X	
A.6.1.3	Contact met overheidsinstanties	Ja	Ja		X		X	
A.6.1.4	Contact met speciale belangengroepen	Ja	Ja	Ja			X	
A.6.1.5	Informatiebeveiliging in projectbeheer	Ja	Ja	Ja			X	
A.6.2	Mobiele apparatuur en telewerken							
A.6.2.1	Beleid voor mobiele apparatuur	Ja	Ja	Ja			X	
A.6.2.2	Telewerken	Ja	Ja	Ja			X	
A.7	Veilig personeel							
A.7.1	Voorafgaand aan het dienstverband							
A.7.1.1	Screening	Ja	Ja				X	
A.7.1.2	Arbeidsvoorwaarden	Ja	Ja		X		X	
A.7.2	Tijdens het dienstverband							
A.7.2.1	Directieverantwoordelijkheden	Ja	Ja		X		X	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja	Ja				X	
A.7.2.3	Disciplinaire procedure	Ja	Ja				X	
A.7.3	Beëindiging en wijziging dienstverband							
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja	Ja	Ja			X	

A.8	Beheer Bedrijfsmiddelen							
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen							
A.8.1.1	Inventariseren van bedrijfsmiddelen	Ja	Ja	Ja			X	
A.8.1.2	Eigendom van bedrijfsmiddelen	Ja	Ja	Ja			X	
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja	Ja	Ja	X		X	
A.8.1.4	Teruggeven van bedrijfsmiddelen	Ja	Ja	Ja			X	
A.8.2	Informatieclassificatie							
A.8.2.1	Classificatie van Informatie	Ja	Ja	Ja	X		X	
A.8.2.2	Informatie labelen	Ja	Ja	Ja	X		X	
A.8.2.3	Behandelen van bedrijfsmiddelen	Ja	Ja	Ja			X	
A.8.3	Behandelen van media							
A.8.3.1	Beheer van verwijderbare media	Ja	Ja	Ja			X	
A.8.3.2	Verwijderen van media	Ja	Ja	Ja			X	
A.8.3.3	Media fysiek overdragen	Ja	Ja	Ja			X	
A.9	Toegangsbeveiliging							
A.9.1	Bedrijfseisen voor toegangsbeveiliging							
A.9.1.1	Beleid voor toegangsbeveiliging	Ja	Ja	Ja			X	
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Ja	Ja	Ja			X	
A.9.2	Beheer van toegangsrechten van gebruikers							
A.9.2.1	Registratie en afmelden van gebruikers	Ja	Ja	Ja			X	
A.9.2.2	Gebruikers toegang verlenen	Ja	Ja	Ja			X	
A.9.2.3	Beheren van speciale toegangsrechten	Ja	Ja	Ja			X	
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Ja	Ja	Ja			X	
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Ja	Ja	Ja			X	
A.9.2.6	Toegangsrechten intrekken of aanpassen	Ja	Ja	Ja			X	
A.9.3	Verantwoordelijkheden van gebruikers							
A.9.3.1	Geheime authenticatie-informatie gebruiken	Ja	Ja	Ja			X	
A.9.4	Toegangsbeveiliging van systeem en toepassing							
A.9.4.1	Beperking toegang tot informatie	Ja	Ja	Ja			X	
A.9.4.2	Beveiligde inlogprocedures	Ja	Ja	Ja			X	
A.9.4.3	Systeem voor wachtwoordbeheer	Ja	Ja	Ja			X	
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Nee						HumanCapitalCare maakt geen gebruik van dergelijke middelen
A.9.4.5	Toegangsbeveiliging op programmabroncode	Nee						HumanCapitalCare ontwikkelt geen software

A.10	Cryptografie							
A.10.1	Cryptografische beheersmaatregelen							
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja	Ja	Ja	X		X	
A.10.1.2	Sleutelbeheer	Ja	Ja	Ja			X	
A.11	Fysieke beveiliging en beveiliging van de omgeving							
A.11.1	Beveiligde gebieden							
A.11.1.1	Fysieke beveiligingszone	Ja	Ja				X	
A.11.1.2	Fysieke toegangsbeveiliging	Ja	Ja				X	
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Ja	Ja				X	
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Ja	Ja				X	
A.11.1.5	Werken in beveiligde gebieden	Ja	Ja				X	
A.11.1.6	Laad- en loslocatie	Ja	Ja					
A.11.2	Apparatuur							
A.11.2.1	Plaatsing en bescherming van apparatuur	Ja	Ja				X	
A.11.2.2	Nutsvoorzieningen	Ja	Ja				X	
A.11.2.3	Beveiliging van bekabeling	Ja	Ja				X	
A.11.2.4	Onderhoud van apparatuur	Ja	Ja				X	
A.11.2.5	Verwijdering van bedrijfsmiddelen	Ja	Ja				X	
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Ja	Ja				X	
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Ja	Ja				X	
A.11.2.8	Onbeheerde gebruikersapparatuur	Ja	Ja				X	
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Ja	Ja				X	
A.12	Beveiliging bedrijfsvoering							
A.12.1	Bedieningsprocedures en verantwoordelijkheden							
A.12.1.1	Gedocumenteerde bedieningsprocedures	Ja	Ja	Ja			X	
A.12.1.2	Wijzigingsbeheer	Ja	Ja	Ja			X	
A.12.1.3	Capaciteitsbeheer	Ja	Ja	Ja			X	
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Nee						HumanCapitalCare ontwikkelt geen software
A.12.2	Bescherming tegen malware							
A.12.2.1	Beheersmaatregelen tegen malware	Ja	Ja	Ja	X		X	
A.12.3	Back-up							
A.12.3.1	Back-up van informatie	Ja	Ja	Ja			X	

A.12.4	Verslaglegging en monitoren							
A.12.4.1	Gebeurtenissen registreren	Ja	Ja	Ja	X		X	
A.12.4.2	Beschermen van informatie in logbestanden	Ja	Ja	Ja	X		X	
A.12.4.3	Logbestanden van beheerders en operators	Ja	Ja	Ja			X	
A.12.4.4	Kloksynchronisatie	Ja	Ja	Ja			X	
A.12.5	Beheersing van operationele software							
A.12.5.1	Software installeren op operationele systemen	Ja	Ja	Ja			X	
A.12.6	Beheer van technische kwetsbaarheden							
A.12.6.1	Beheer van technische kwetsbaarheden	Ja	Ja	Ja			X	
A.12.6.2	Beperkingen voor het installeren van software	Ja	Ja	Ja			X	
A.12.7	Overwegingen betreffende audits van informatiesystemen							
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Ja	Ja	Ja			X	
A.13	Communicatiebeveiliging							
A.13.1	Beheer van netwerkbeveiliging							
A.13.1.1	Beheersmaatregelen voor netwerken	Ja	Ja	Ja			X	
A.13.1.2	Beveiliging van netwerkdiensten	Ja	Ja	Ja			X	
A.13.1.3	Scheiding in netwerken	Ja	Ja	Ja			X	
A.13.2	Informatietransport							
A.13.2.1	Beleid en procedures voor informatietransport	Ja	Ja	Ja			X	
A.13.2.2	Overeenkomsten over informatietransport	Ja	Ja	Ja			X	
A.13.2.3	Elektronische berichten	Ja	Ja	Ja			X	
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja	Ja	Ja			X	
A.14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen							
A.14.1	Beveiligingseisen voor informatiesystemen							
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Ja	Ja	Ja			X	
A.14.1.2	Toepassingen op openbare netwerken beveiligen	Ja	Ja	Ja			X	
A.14.1.3	Transacties van toepassingen beschermen	Ja	Ja	Ja	X		X	

A.14.2	Beveiliging in ontwikkelings- en ondersteuningsprocessen							
A.14.2.1	Beleid voor beveiligd ontwikkelen	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.5	Principes voor engineering van beveiligde systemen	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.6	Beveiligde ontwikkelomgeving	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.7	Uitbestede software- ontwikkeling	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.8	Testen van systeembeveiliging	Nee						HumanCapitalCare ontwikkelt geen software
A.14.2.9	Systeemacceptatietests	Nee						HumanCapitalCare ontwikkelt geen software
A.14.3	Testgegevens							
A.14.3.1	Bescherming van testgegevens	Nee						HumanCapitalCare ontwikkelt geen software
A.15	Leveranciersrelaties							
A.15.1	Informatiebeveiliging in leveranciersrelaties							
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja	Ja	Ja			X	
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ja	Ja	Ja			X	
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Ja	Ja	Ja			X	
A.15.2	Beheer van dienstverlening van leveranciers							
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Ja	Ja	Ja			X	
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Ja	Ja	Ja			X	
A.16	Beheer van informatie-beveiligingsincidenten							
A.16.1	Rapportage van informatiebeveiligings-gebeurtenissen en verbeteringen							
A.16.1.1	Verantwoordelijkheden en procedures	Ja	Ja	Ja			X	
A.16.1.2	Rapportage van informatiebeveiligings-gebeurtenissen	Ja	Ja	Ja	X		X	
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Ja	Ja	Ja			X	

A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligings-gebeurtenissen	Ja	Ja	Ja			X	
A.16.1.5	Respons op informatiebeveiligingsincidenten	Ja	Ja	Ja	X		X	
A.16.1.6	Lering uit informatiebeveiligings-incidenten	Ja	Ja	Ja			X	
A.16.1.7	Verzamelen van bewijsmateriaal	Ja	Ja	Ja	X		X	
A.17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer							
A.17.1	Informatiebeveiligingscontinuïteit							
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	Ja	Ja	Ja			X	
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	Ja	Ja	Ja			X	
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja	Ja	Ja			X	
A.17.2	Redundante componenten							
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Ja	Ja	Ja			X	
A.18	Naleving							
A.18.1	Naleving van wettelijke en contractuele eisen							
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja	Ja	Ja	X		X	
A.18.1.2	Intellectuele eigendomsrechten	Ja	Ja	Ja	X		X	
A.18.1.3	Beschermen van registraties	Ja	Ja	Ja	X		X	
A.18.1.4	Privacy en bescherming van persoonsgegevens	Ja	Ja	Ja	X		X	
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja	Ja	Ja	X		X	
A.18.2	Informatiebeveiligings-beoordelingen							
A.18.2.1	Onafhankelijk beoordeling van informatiebeveiliging	Ja	Ja	Ja			X	
A.18.2.2	Naleving van beveiligingsbeleid en -normen	Ja	Ja	Ja			X	
A.18.2.3	Beoordeling van technische naleving	Ja	Ja	Ja			X	