ProSoftware©
ontzorgt de zorg

Kamerlingh Onnesweg 61
3316 GK Dordrecht
Tel: 078 711 21 04
Fax: 084 223 92 53
IBAN: NL42INGB0004295394
BIC: INGBNL2A
BTW: NL8176.20.746.B01
KvK: 24 35 75 40

info@prosoftware.nl
www.prosoftware.nl

Verklaring van Toepasselijkheid
ISO 27001:2022

ProSoftware©
ontzorgt de zorg

Inhoud

1. Inleiding

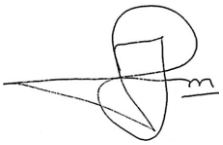
Dit document omvat de Verklaring van Toepasselijkheid ten behoeve van de certificering voor de ISO 27001 standaard. De doelstelling van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Prosoftware en haar bedrijfsprocessen te controleren en te managen.

De beheersmaatregelen zijn geïdentificeerd op basis van de ISO 27001:2022 standaard opgenomen beheersmaatregelen van de norm. Per beheersmaatregel wordt de toepasselijkheid weergegeven. Indien een beheersmaatregel niet van toepassing is, wordt hiervoor een verklaring gegeven.

2. Directieverklaring

De Directie van Prosoftware verklaart hierbij de in deze Verklaring van Toepasselijkheid vermelde maatregelen bekrachtigd in relatie tot de uitgevoerde risicoanalyses en accepteert het restrisico van niet genomen maatregelen.

Dordrecht, 30-09-2025



J. Langendam

3. Scope

Het ontwikkelen, leveren, hosten en ondersteunen van software voor de zorgsector, waaronder software voor het uitvoeren van klanttevredenheidsonderzoeken.

4. Beheersmaatregelen

Beheersmaatregelen		Van toepassing	Geïmplementeerd	Risicoanalyse	Wet- en regelgeving	Overeenkomst	Good practice	Reden voor uitsluiting
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				
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				
A. 5.11	Retourneren van bedrijfsmiddelen	Ja	Ja	x				
A. 5.12	Classificeren van informatie	Ja	Ja	x				
A. 5.13	Labelen van informatie	Ja	Ja	x				
A. 5.14	Overdragen van informatie	Ja	Ja	x				
A. 5.15	Toegangsbeveiliging	Ja	Ja	x		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				
A. 5.27	Leren van informatiebeveiligingsincidenten	Ja	Ja	x				
A. 5.28	Verzamelen van bewijsmateriaal	Ja	Ja	x				
A. 5.29	Informatiebeveiliging tijdens een verstoring	Ja	Ja	x				
A. 5.30	ICT-gereedheid voor bedrijfscontinuiteit	Ja	Ja	x				

Beheersmaatregelen		Van toepassing	Geïmplementeerd	Risicoanalyse	Wet- en regelgeving	Overeenkomst	Good practice	Reden voor uitsluiting
A. 5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Ja	Ja	x				
A. 5.32	Intellectuele- eigendomsrechten	Ja	Ja		x			
A. 5.33	Beschermen van registraties	Ja	Ja	x				
A. 5.34	Privacy en bescherming van persoonsgegevens	Ja	Ja	x	x	x		
A. 5.35	Onafhankelijke beoordeling van informatiebeveiliging	Ja	Ja	x		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		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 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 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 clearn 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				

Beheersmaatregelen		Van toepassing	Geïmplementeerd	Risicoanalyse	Wet- en regelgeving	Overeenkomst	Good practice	Reden voor uitsluiting
A. 8.2	Speciale toegangsrechten	Ja	Ja	x				
A. 8.3	Beperking toegang tot informatie	Ja	Ja	x				
A. 8.4	Toegangsbeveiliging op broncode	Ja	Ja	x				
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		x		
A. 8.9	Configuratiebeheer	Ja	Ja	x				
A. 8.10	Wissen van informatie	Ja	Ja	x		x		
A. 8.11	Maskeren van gegevens	Ja	Ja				x	
A. 8.12	Voorkomen van gegevenslekker	Ja	Ja	x				
A. 8.13	Back-up van informatie	Ja	Ja	x		x		
A. 8.14	Redundantie van informatieverwerkende faciliteiten	Ja	Ja	x		x		
A. 8.15	Logging	Ja	Ja	x				
A. 8.16	Monitoren van activiteiten	Ja	Ja	x		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		x		
A. 8.22	Netwerksegmentatie	Ja	Ja	x				
A. 8.23	Toepassen van webfilters	Ja	Ja	x		x		
A. 8.24	Gebruik van cryptografie	Ja	Ja	x		x		
A. 8.25	Beveiligen tijdens ontwikkelcyclus	Ja	Ja	x				
A. 8.26	Toepassingsbeveiligingseisen	Ja	Ja	x				
A. 8.27	Veilige systeemarchitectuur en technische uitgangspunten	Ja	Ja	x		x		
A. 8.28	Veilig coderen	Ja	Ja	x				
A. 8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Ja	Ja	x				
A. 8.30	Uitbestede systeemontwikkeling	Ja	Ja	x				
A. 8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ja	Ja	x				
A. 8.32	Wijzigingsbeheer	Ja	Ja	x				
A. 8.33	Testgegevens	Ja	Ja	x				
A. 8.34	Bescherming van informatiesystemen tijdens audits	Ja	Ja				x	