

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](mailto:info@prosoftware.nl)  
[www.prosoftware.nl](http://www.prosoftware.nl)

## **Verklaring van Toepasselijkheid ISO 27001:2013**

## Inhoud

1. Inleiding.....	3
2. Directieverklaring .....	3
3. Scope .....	3
4. Beheersmaatregelen .....	4

## 1. Inleiding

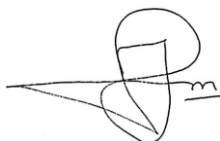
Dit document omvat de Verklaring van Toepasselijkheid ten behoeve van de certificering voor de ISO 27001 standaard. De doelstelling van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Prosoftware en haar bedrijfsprocessen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

De beheersmaatregelen zijn geïdentificeerd op basis van de ISO 27001:2013 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, 13 december 2018



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	Wet- en regelgeving	Klantcontract	Risicoanalyse	Reden voor uitsluiting
<b>A. 5</b>	<b>Informatiebeveiligingsbeleid</b>						
A. 5.1.1	Beleidsregels voor informatiebeveiliging	Ja	Ja			X	
A. 5.1.2	Beoordeling van het informatiebeveiligingsbeleid	Ja	Ja			X	
<b>A. 6</b>	<b>Organiseren van informatiebeveiliging</b>						
A. 6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja			X	
A. 6.1.2	Scheiding van taken	Ja	Ja			X	
A. 6.1.3	Contact met overheidsinstanties	Ja	Ja	X		X	
A. 6.1.4	Contact met speciale belangengroepen	Ja	Ja			X	
A. 6.1.5	Informatiebeveiliging in projectbeheer	Ja	Ja			X	
A. 6.2.1	Beleid voor mobiele apparatuur	Ja	Ja			X	
A. 6.2.2	Telewerken	Ja	Ja			X	
<b>A. 7</b>	<b>Veilig personeel</b>						
A. 7.1.1	Screening	Ja	Ja			X	
A. 7.1.2	Arbeidsvoorwaarden	Ja	Ja			X	
A. 7.2.1	Directieverantwoordelijkheden	Ja	Ja			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. 7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja	Ja			X	
<b>A. 8</b>	<b>Beheer van bedrijfsmiddelen</b>						
A. 8.1.1	Inventariseren van bedrijfsmiddelen	Ja	Ja			X	
A. 8.1.2	Eigendom van bedrijfsmiddelen	Ja	Ja			X	
A. 8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja	Ja			X	
A. 8.1.4	Teruggeven van bedrijfsmiddelen	Ja	Ja			X	
A. 8.2.1	Classificatie van informatie	Ja	Ja			X	
A. 8.2.2	Informatie labelen	Ja	Ja			X	
A. 8.2.3	Behandelen van bedrijfsmiddelen	Ja	Ja			X	
A. 8.3.1	Beheer van verwijderbare media	Ja	Ja			X	
A. 8.3.2	Verwijderen van media	Ja	Ja			X	
A. 8.3.3	Media fysiek overdragen	Ja	Ja			X	
<b>A. 9</b>	<b>Toegangsbeveiliging</b>						
A. 9.1.1	Beleid voor toegangsbeveiliging	Ja	Ja			X	
A. 9.1.2	Toegang tot netwerken en netwerkdiensten	Ja	Ja			X	
A. 9.2.1	Registratie en afmelden van gebruikers	Ja	Ja			X	
A. 9.2.2	Gebruikers toegang verlenen	Ja	Ja			X	
A. 9.2.3	Beheren van speciale toegangsrechten	Ja	Ja			X	
A. 9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Ja	Ja			X	

Beheersmaatregelen		Van toepassing	Geïmplementeerd	Wet- en regelgeving	Klantcontract	Risicoanalyse	Reden voor uitsluiting
A. 9.2.5	Beoordeling van toegangsrechten van gebruikers	Ja	Ja			X	
A. 9.2.6	Toegangsrechten intrekken of aanpassen	Ja	Ja			X	
A. 9.3.1	Geheime authenticatie-informatie gebruiken	Ja	Ja			X	
A. 9.4.1	Beperking toegang tot informatie	Ja	Ja			X	
A. 9.4.2	Beveiligde inlogprocedures	Ja	Ja			X	
A. 9.4.3	Systeem voor wachtwoordbeheer	Ja	Ja			X	
A. 9.4.4	Speciale systeemhulpmiddelen gebruiken	Ja	Ja			X	
A. 9.4.5	Toegangsbeveiliging op programmabroncode	Ja	Ja			X	
<b>A. 10</b>	<b>Cryptografie</b>						
A. 10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja	Ja			X	
A. 10.1.2	Sleutelbeheer	Ja	Ja			X	
<b>A. 11</b>	<b>Fysieke beveiliging en beveiliging van de omgeving</b>						
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			X	
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		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	
<b>A. 12</b>	<b>Beveiliging bedrijfsvoering</b>						
A. 12.1.1	Gedocumenteerde bedieningsprocedures	Ja	Ja			X	
A. 12.1.2	Wijzigingsbeheer	Ja	Ja			X	
A. 12.1.3	Capaciteitsbeheer	Ja	Ja			X	
A. 12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ja	Ja			X	
A. 12.2.1	Beheersmaatregelen tegen malware	Ja	Ja			X	
A. 12.3.1	Back-up van informatie	Ja	Ja			X	
A. 12.4.1	Gebeurtenissen, incidenten registreren	Ja	Ja			X	
A. 12.4.2	Beschermen van informatie in logbestanden	Ja	Ja			X	

Beheersmaatregelen		Van toepassing	Geïmplementeerd	Wet- en regelgeving	Klantcontract	Risicoanalyse	Reden voor uitsluiting
A. 12.4.3	Logbestanden van beheerders en operators	Ja	Ja			x	
A. 12.4.4	Kloksynchronisatie	Ja	Ja			x	
A. 12.5.1	Software installeren op operationele systemen	Ja	Ja			x	
A. 12.6.1	Beheer van technische kwetsbaarheden	Ja	Ja			x	
A. 12.6.2	Beperkingen voor het installeren van software	Ja	Ja			x	
A. 12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Ja	Ja			x	
<b>A. 13</b>	<b>Communicatiebeveiliging</b>						
A. 13.1.1	Beheersmaatregelen voor netwerken	Ja	Ja			x	
A. 13.1.2	Beveiliging van netwerkdiensten	Ja	Ja			x	
A. 13.1.3	Scheiding in netwerken	Ja	Ja			x	
A. 13.2.1	Beleid en procedures voor informatietransport	Ja	Ja			x	
A. 13.2.2	Overeenkomsten over informatietransport	Ja	Ja			x	
A. 13.2.3	Elektronische berichten	Ja	Ja			x	
A. 13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja	Ja		x	x	
<b>A. 14</b>	<b>Acquisitie (inkoop), ontwikkeling en onderhoud van informatiesystemen</b>						
A. 14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Ja	Ja			x	
A. 14.1.2	Toepassingen op openbare netwerken beveiligen	Ja	Ja			x	
A. 14.1.3	Transacties van toepassingen beschermen	Ja	Ja			x	
A. 14.2.1	Beleid voor beveiligd ontwikkelen	Ja	Ja			x	
A. 14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Ja	Ja			x	
A. 14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Ja	Ja			x	
A. 14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Ja	Ja			x	
A. 14.2.5	Principes voor engineering van beveiligde systemen	Ja	Ja			x	
A. 14.2.6	Beveiligde ontwikkelomgeving	Ja	Ja			x	
A. 14.2.7	Uitbestede softwareontwikkeling	Nee	Nee				Prosoftware besteedt software-ontwikkeling niet uit.
A. 14.2.8	Testen van systeembeveiliging	Ja	Ja			x	
A. 14.2.9	Systeemacceptatietests	Ja	Ja			x	
A. 14.3.1	Bescherming van testgegevens	Ja	Ja			x	
<b>A. 15</b>	<b>Leveranciersrelaties</b>						
A. 15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja	Ja			x	

Beheersmaatregelen		Van toepassing	Geïmplementeerd	Wet- en regelgeving	Klantcontract	Risicoanalyse	Reden voor uitsluiting
A. 15.1.2	Opnemen van beveiligingsaspecten in leverancierovereenkomsten	Ja	Ja			X	
A. 15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Ja	Ja			X	
A. 15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Ja	Ja			X	
A. 15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Ja	Ja			X	
<b>A. 16</b>	<b>Beheer van informatiebeveiligingsincidenten</b>						
A. 16.1.1	Verantwoordelijkheden en procedures	Ja	Ja			X	
A. 16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Ja	Ja			X	
A. 16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Ja	Ja			X	
A. 16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Ja	Ja			X	
A. 16.1.5	Respons op informatiebeveiligingsincidenten	Ja	Ja			X	
A. 16.1.6	Lering uit informatiebeveiligingsincidenten	Ja	Ja			X	
A. 16.1.7	Verzamelen van bewijsmateriaal	Ja	Ja			X	
<b>A. 17</b>	<b>Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer</b>						
A. 17.1.1	Informatiebeveiligingscontinuïteit plannen	Ja	Ja			X	
A. 17.1.2	Informatiebeveiligingscontinuïteit implementeren	Ja	Ja			X	
A. 17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja	Ja			X	
A. 17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	Ja	Ja			X	
<b>A. 18</b>	<b>Naleving</b>						
A. 18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja	Ja	X		X	
A. 18.1.2	Intellectuele-eigendomsrechten	Ja	Ja	X		X	
A. 18.1.3	Beschermen van registraties	Ja	Ja	X		X	
A. 18.1.4	Privacy en bescherming van persoonsgegevens	Ja	Ja	X	X	X	
A. 18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja	Ja			X	
A. 18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	Ja	Ja			X	
A. 18.2.2	Naleving van beveiligingsbeleid en -normen	Ja	Ja			X	
A. 18.2.3	Beoordeling van technische naleving	Ja	Ja			X	