Verklaring van toepasselijkheid | ISO/IEC 27001:2022

Organisatie:	Parantion Groep B.V.| Scorion
Beheerder/Eigenaar:	Directie
Datum:	26-3-2025
Classificatie:	Publiek
Geldigheidsperiode:	26-03-2025 tot 06-10-2028

Document historie

Versie	Status	Toelichting	Auteur	Datum
1.1	Definitief	Verklaring van toepasselijkheid ISO27001:2022	Directie	26-03-2025

1. Inleiding

Dit document omvat de Verklaring van Toepasselijkheid (VVT) ten behoeve van de certificering voor de ISO27001-standaard. Het doel van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Parantion Groep B.V.| Scorion en bedrijfsprocessen te controleren en te managen.

De van toepassing zijnde beheersmaatregelen zijn geïdentificeerd op basis van de beheersmaatregelen benoemd in de ISO 27002:2022. Indien een beheersmaatregel niet van toepassing is, wordt hiervoor een verklaring gegeven.

De organisatie heeft geïnvesteerd in het opzetten van een robuust Informatiebeveiligingsmanagementsysteem (ISMS), waarbij de richtlijnen en controles uit de ISO/IEC 27002-norm zijn toegepast en geïmplementeerd om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen.

2. Directieverklaring

De Directie van Parantion Groep B.V. | Scorion verklaart hierbij de in deze VVT vermelde maatregelen bekrachtigd in relatie tot de uitgevoerde risicoanalyses en accepteert het restrisico van eventuele niet genomen maatregelen.

Deventer, 26 maart 2025

Roel Smabers CEO

3. Scope

Informatiebeveiliging gerelateerd aan het ontwikkelen, adviseren, implementeren en het leveren van ondersteuning op het SaaS platform voor portfoliomanagement, persoonlijke ontwikkeling en assessment toepassingen.

4. Verklaring van toepasselijkheid

4.1 Van toepassing zijnde maatregelen

Maatregel nr.	Maatregel omschrijving	Reden van toepassing	Geïmplementeerd
5	**Organisatorische beheersmaatregelen**		
5.1	Beleidsregels voor informatiebeveiliging	Baseline	Ja
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Baseline	Ja
5.3	Functiescheiding	Baseline	Ja
5.4	Managementverantwoordelijkheden	Baseline	Ja
5.5	Contact met overheidsinstanties	Baseline	Ja
5.6	Contact met speciale belangengroepen	Baseline	Ja
5.7	Informatie en analyses over dreigingen	Risicoanalyse	Ja
5.8	Informatiebeveiliging in projectmanagement	Risicoanalyse	Ja

5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Risicoanalyse	Ja
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Risicoanalyse	Ja
5.11	Retourneren van bedrijfsmiddelen	Risicoanalyse	Ja
5.12	Classificatie van informatie	Risicoanalyse	Ja
5.13	Labelen van informatie	Risicoanalyse	Ja
5.14	Overdragen van informatie	Risicoanalyse	Ja
5.15	Toegangsbeveiliging	Baseline	Ja
5.16	Identiteitsbeheer	Risicoanalyse	Ja
5.17	Authenticatie-informatie	Risicoanalyse	Ja
5.18	Toegangsrechten	Risicoanalyse	Ja
5.19	Informatiebeveiliging in leveranciersrelaties	Risicoanalyse	Ja
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Risicoanalyse	Ja
5.21	Beheer van informatiebeveiliging in de ICT-toeleveringsketen	Baseline	Ja
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Risicoanalyse	Ja
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Risicoanalyse	Ja
5.24	Planning en voorbereiding van het beheer van informatiebeveiligingsincidenten	Baseline	Ja
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Baseline	Ja
5.26	Reageren op informatiebeveiligingsincidenten	Baseline	Ja
5.27	Leren van informatiebeveiligingsincidenten	Risicoanalyse	Ja
5.28	Verzameling van bewijsmateriaal	Risicoanalyse	Ja
5.29	Informatiebeveiliging tijdens een verstoring	Risicoanalyse	Ja
5.30	ICT-gereedheid voor bedrijfscontinuïteit	Baseline	Ja
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Baseline	Ja
5.32	Intellectuele eigendomsrechten	Wet en regelgeving	Ja
5.33	Beschermen van registraties	Wet en regelgeving	Ja
5.34	Privacy en bescherming van persoonsgegevens	Wet en regelgeving	Ja
5.35	Onafhankelijke beoordeling van informatiebeveiliging	Risicoanalyse	Ja
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Wet en regelgeving	Ja
5.37	Gedocumenteerde bedieningsprocedures	Risicoanalyse	Ja
6	**Mensgerichte beheersmaatregelen**		
6.1	Screening	Risicoanalyse	Ja
6.2	Arbeidsovereenkomst	Baseline	Ja
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Risicoanalyse	Ja
6.4	Disciplinair procedure	Risicoanalyse	Ja

6.5	Verantwoordelijkheden na beëindiging of wijziging van dienstverband	Risicoanalyse	Ja
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Risicoanalyse	Ja
6.7	Werken op afstand	Risicoanalyse	Ja
6.8	Melden van informatiebeveiligingsgebeurtenissen	Risicoanalyse	Ja
7	**Fysieke beheersmaatregelen**		
7.1	Fysieke beveiligingszones	Risicoanalyse	Ja
7.2	Fysieke toegangsbeveiliging	Risicoanalyse	Ja
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Risicoanalyse	Ja
7.4	Monitoring van de fysieke beveiliging	Risicoanalyse	Ja
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Risicoanalyse	Ja
7.6	Werken in beveiligde zones	Risicoanalyse	Ja
7.7	‘Clear desk’, ‘clear screen’	Risicoanalyse	Ja
7.8	Plaatsing en bescherming van apparatuur	Risicoanalyse	Ja
7.9	Beveiliging van bedrijfsmiddelen buiten het terrein	Risicoanalyse	Ja
7.10	Opslagmedia	Risicoanalyse	Ja
7.11	Nutssystemen	Risicoanalyse	Ja
7.12	Beveiligen van bekabeling	Risicoanalyse	Ja
7.13	Onderhoud van apparatuur	Risicoanalyse	Ja
7.14	Veilig verwijderen of hergebruiken van apparatuur	Risicoanalyse	Ja
8	**Technologische beheersmaatregelen**		
8.1	‘user endpoint devices’	Risicoanalyse	Ja
8.2	Speciale toegangsrechten	Risicoanalyse	Ja
8.3	Beperking toegang tot informatie	Risicoanalyse	Ja
8.4	Toegangsbeveiliging op broncode	Risicoanalyse	Ja
8.5	Beveiligde authenticatie	Risicoanalyse	Ja
8.6	Capaciteitsbeheer	Risicoanalyse	Ja
8.7	Bescherming tegen malware	Risicoanalyse	Ja
8.8	Beheer van technische kwetsbaarheden	Risicoanalyse	Ja
8.9	Configuratiebeheer	Risicoanalyse	Ja
8.10	Wissen van informatie	Risicoanalyse	Ja
8.11	Maskeren van gegevens	Risicoanalyse	Ja
8.12	Voorkomen van gegevenslekken (data leakage prevention)	Risicoanalyse	Ja
8.13	Back-up van informatie	Risicoanalyse	Ja
8.14	Redundantie van informatieverwerkende faciliteiten	Risicoanalyse	Ja
8.15	Logging	Risicoanalyse	Ja
8.16	Monitoren van activiteiten	Risicoanalyse	Ja
8.17	Kloksynchronisatie	Risicoanalyse	Ja
8.18	Gebruik van speciale systeemhulpmiddelen	Risicoanalyse	Ja
8.19	Installeren van software op operationele systemen	Risicoanalyse	Ja
8.20	Beveiliging van netwerkcomponenten	Risicoanalyse	Ja

8.21	Beveiliging van netwerkdiensten	Risicoanalyse	Ja
8.22	Netwerk segmentatie	Risicoanalyse	Ja
8.23	Toepassen van webfilters	Risicoanalyse	Ja
8.24	Gebruik van cryptografie	Risicoanalyse	Ja
8.25	Beveiligen tijdens de ontwikkelcyclus	Risicoanalyse	Ja
8.26	Toepassingsbeveiligingsvereisten	Risicoanalyse	Ja
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Risicoanalyse	Ja
8.28	Veilig coderen	Risicoanalyse	Ja
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Risicoanalyse	Ja
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Risicoanalyse	Ja
8.32	Wijzigingsbeheer	Risicoanalyse	Ja
8.33	Testgegevens	Risicoanalyse	Ja
8.34	Bescherming van informatiesystemen tijdens audits	Baseline	Ja

4.2. Niet van toepassing zijnde maatregelen

Maatregel nr.	Maatregel omschrijving	Reden niet van toepassing	Geïmplementeerd
8	**Technische maatregelen**		
8.30	Uitbestede systeemontwikkeling	Scorion besteedt de ontwikkeling van programmatuur niet uit. Zij doet de ontwikkeling van haar applicaties binnen de organisatie zelf.	Nee

5. Conclusie

De organisatie heeft de noodzakelijke maatregelen geïmplementeerd in overeenstemming met de **ISO/IEC 27002:2022**-norm en voldoet daarmee aan de vereisten voor informatiebeveiliging. Het ISMS wordt regelmatig geëvalueerd en verbeterd om ervoor te zorgen dat de beveiligingsmaatregelen effectief blijven in het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie