Verklaring van Toepasselijkheid

Parantion Groep B.V.

ISO27001:2017

Document index

Auteur	Parantion Groep B.V.
Document naam	Verklaring van Toepasselijkheid_ISO_Directie_v4.3_juli2022_Openbaar.docx
Datum	20 juli 2022
Distributie	Openbaar

Inhoudsopgave

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. en bedrijfsprocessen te controleren en te managen.

De van toepassing zijnde beheersmaatregelen zijn geïdentificeerd op basis van de beheersmaatregelen benoemd in de ISO 27001 norm Annex 1. Voor de van toepassing zijnde beheersmaatregel wordt verwezen naar de gedefinieerde ISO27002 'best practices' richtlijnen welke specifiek zijn gemaakt voor toepassing in Parantion Groep B.V. bedrijfsprocessen. Indien een beheersmaatregel niet van toepassing is, wordt hiervoor een verklaring gegeven.

2. Directieverklaring

De Directie van Parantion Groep B.V. 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, 20 juli 2022

Roel Smabers

3. Scope

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

4. Verklaring van toepasselijkheid

De VVT is weergegeven in de volgende tabel met de volgende kolommen: 1. De nummer van de beheersmaatregel; 2. De naam van de beheersmaatregel.

4.1. Van toepassing zijnde maatregelen

Maatregel nr.	Maatregel omschrijving	Reden van toepassing	Geïmplementeerd
A.5 Informatiebeveiligingsbeleid			
A.05.01.01	Beleidsregels voor informatiebeveiliging	Baseline	Ja
A.05.01.02	Beoordeling van het informatiebeveiligingsbeleid	Baseline	Ja
A.6 Organiseren van informatiebeveiliging			
A.06.01.01	Rollen en verantwoordelijkheden voor informatiebeveiliging	Baseline	Ja
A.06.01.02	Scheiding van taken	Baseline	Ja
A.06.01.03	Contact met overheidsinstanties	Baseline	Ja
A.06.01.04	Contact met speciale belangengroepen	Baseline	Ja
A.06.01.05	Informatiebeveiliging in projectbeheer	Risicoanalyse	Ja
A.06.02.01	Beleid voor mobiele apparatuur	Risicoanalyse	Ja
A.06.02.02	Telewerken	Risicoanalyse	Ja
A.7 Veilig Personeel			
A.07.01.01	Screening	Risicoanalyse	Ja
A.07.01.02	Arbeidsvoorwaarden	Baseline	Ja
A.07.02.01	Directieverantwoordelijkheden	Baseline	Ja
A.07.02.02	Bewustzijn, opleiding en training ten behoeve van informatiebeveiliging	Risicoanalyse	Ja
A.07.02.03	Disciplinaire procedure	Risicoanalyse	Ja
A.07.03.01	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Risicoanalyse	Ja
A.8 Beheer van bedrijfsmiddelen			
A.08.01.01	Inventarisatie van bedrijfsmiddelen	Risicoanalyse	Ja
A.08.01.02	Eigendom van bedrijfsmiddelen	Risicoanalyse	Ja
A.08.01.03	Aanvaardbaar gebruik van bedrijfsmiddelen	Risicoanalyse	Ja

A.08.01.04	Teruggeven van bedrijfsmiddelen	Risicoanalyse	Ja
A.08.02.01	Classificatie van informatie	Risicoanalyse	Ja
A.08.02.02	Informatie labelen	Risicoanalyse	Ja
A.08.02.03	Behandelen van bedrijfsmiddelen	Risicoanalyse	Ja
A.08.03.01	Beheer van verwijderbare media	Risicoanalyse	Ja
A.08.03.02	Verwijderen van media	Risicoanalyse	Ja
A.08.03.03	Media fysiek overdragen	Risicoanalyse	Ja
A.9 Toegangsbeveiliging			
A.09.01.01	Beleid voor toegangsbeveiliging	Baseline	Ja
A.09.01.02	Toegang tot netwerken en netwerkdiensten	Risicoanalyse	Ja
A.09.02.01	Registratie en uitschrijving van gebruikers	Risicoanalyse	Ja
A.09.02.02	Gebruikers toegang verlenen	Risicoanalyse	Ja
A.09.02.03	Beheren van speciale toegangsrechten	Risicoanalyse	Ja
A.09.02.04	Beheer van geheime authenticatie-informatie van gebruikers	Risicoanalyse	Ja
A.09.02.05	Beoordeling van toegangsrechten van gebruikers	Risicoanalyse	Ja
A.09.02.06	Toegangsrechten intrekken of aanpassen	Risicoanalyse	Ja
A.09.03.01	Geheime authenticatie-informatie gebruiken	Risicoanalyse	Ja
A.09.04.01	Beperking toegang tot informatie	Risicoanalyse	Ja
A.09.04.02	Beveiligde inlogprocedures	Risicoanalyse	Ja
A.09.04.03	Systemen voor wachtwoordbeheer	Risicoanalyse	Ja
A.09.04.04	Speciale systeemhulpmiddelen gebruiken	Risicoanalyse	Ja
A.09.04.05	Toegangsbeveiliging op programmabroncode	Risicoanalyse	Ja
A.10 Cryptografie			
A.10.01.01	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Baseline	Ja
A.10.01.02	Sleutelbeheer	Risicoanalyse	Ja

A.11 Fysieke beveiliging en beveiliging van de omgeving			
A.11.01.01	Fysieke beveiligingszone	Risicoanalyse	Ja
A.11.01.02	Fysieke toegangsbeveiliging	Risicoanalyse	Ja
A.11.01.03	Kantoren, ruimten en faciliteiten beveiligen	Risicoanalyse	Ja
A.11.01.04	Bescherming tegen bedreigingen van buitenaf	Risicoanalyse	Ja
A.11.01.05	Werken in beveiligde gebieden	Risicoanalyse	Ja
A.11.01.06	Laad- en loslocatie	Risicoanalyse	Ja
A.11.01.05	Werken in beveiligde ruimten	Risicoanalyse	Ja
A.11.02.01	Plaatsing en bescherming van apparatuur	Risicoanalyse	Ja
A.11.02.02	Nutsvoorzieningen	Risicoanalyse	Ja
A.11.02.03	Beveiliging van bekabeling	Risicoanalyse	Ja
A.11.02.04	Onderhoud van apparatuur	Risicoanalyse	Ja
A.11.02.05	Verwijdering van bedrijfsmiddelen	Risicoanalyse	Ja
A.11.02.06	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Risicoanalyse	Ja
A.11.02.07	Veilig verwijderen of hergebruiken van apparatuur	Risicoanalyse	Ja
A.11.02.08	Onbeheerde gebruikersapparatuur	Risicoanalyse	Ja
A.11.02.09	‘Clear desk’- en ‘clear screen’-beleid	Risicoanalyse	Ja
A.12 Beveiliging bedrijfsvoering			
A.12.01.01	Gedocumenteerde bedieningsprocedures	Risicoanalyse	Ja
A.12.01.02	Wijzigingsbeheer	Risicoanalyse	Ja
A.12.01.03	Capaciteitsbeheer	Risicoanalyse	Ja
A.12.01.04	Scheiding van ontwikkel-, test- en productieomgevingen	Risicoanalyse	Ja
A.12.02.01	Beheersmaatregelen tegen malware	Risicoanalyse	Ja
A.12.03.01	Back-up van informatie	Risicoanalyse	Ja
A.12.04.01	Gebeurtenissen registreren	Risicoanalyse	Ja

A.12.04.02	Beschermen van informatie in logbestanden	Risicoanalyse	Ja
A.12.04.03	Logbestanden van beheerders en operators	Risicoanalyse	Ja
A.12.04.04	Kloksynchronisatie	Risicoanalyse	Ja
A.12.05.01	Software installeren op operationele systemen	Risicoanalyse	Ja
A.12.06.01	Beheer van technische kwetsbaarheden	Risicoanalyse	Ja
A.12.06.02	Beperkingen voor het installeren van software	Risicoanalyse	Ja
A.12.07.01	Beheersmaatregelen betreffende audits van informatiesystemen	Baseline	Ja
A.13 Communicatiebeveiliging			
A.13.01.01	Beheersmaatregelen voor netwerken	Risicoanalyse	Ja
A.13.01.02	Beveiliging van netwerkdiensten	Risicoanalyse	Ja
A.13.01.03	Scheiding in netwerken	Risicoanalyse	Ja
A.13.02.01	Beleid en procedures voor informatietransport	Baseline	Ja
A.13.02.02	Overeenkomsten over informatietransport	Risicoanalyse	Ja
A.13.02.03	Elektronische berichten	Risicoanalyse	Ja
A.13.02.04	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Risicoanalyse	Ja
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen			
A.14.01.01	Analyse en specificatie van beveiligingseisen	Risicoanalyse	Ja
A.14.01.02	Toepassingsdiensten op openbare netwerken beveiligen	Risicoanalyse	Ja
A.14.01.03	Transacties van toepassingsdiensten beschermen	Risicoanalyse	Ja
A.14.02.01	Beleid voor veilig ontwikkelen	Risicoanalyse	Ja
A.14.02.02	Procedures voor wijzigingsbeheer met betrekking tot systemen	Risicoanalyse	Ja
A.14.02.03	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Risicoanalyse	Ja
A.14.02.04	Beperkingen op wijzigingen van softwarepakketten	Risicoanalyse	Ja
A.14.02.05	Principes voor engineering van beveiligde systemen	Risicoanalyse	Ja
A.14.02.06	Beveiligde ontwikkelomgeving	Risicoanalyse	Ja
A.14.02.08	Testen van systeembeveiliging	Risicoanalyse	Ja

A.14.02.09	Systeemacceptatietests	Risicoanalyse	Ja
A.14.03.01	Bescherming van testgegevens	Risicoanalyse	Ja
A.15 Leveranciersrelaties			
A.15.01.01	Informatiebeveiligingsbeleid voor leveranciersrelaties	Risicoanalyse	Ja
A.15.01.02	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Risicoanalyse	Ja
A.15.01.03	Toeleveringsketen van informatie- en communicatietechnologie	Risicoanalyse	Ja
A.15.02.01	Monitoring en beoordeling van dienstverlening van leveranciers	Risicoanalyse	Ja
A.15.02.02	Beheer van veranderingen in dienstverlening van leveranciers	Risicoanalyse	Ja
A.16 Beheer van informatiebeveiligingsincidenten			
A.16.01.01	Verantwoordelijkheden en procedures	Baseline	Ja
A.16.01.02	Rapportage van informatiebeveiligingsgebeurtenissen	Baseline	Ja
A.16.01.03	Rapportage van zwakke plekken in de informatiebeveiliging	Baseline	Ja
A.16.01.04	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Baseline	Ja
A.16.01.05	Respons op informatiebeveiligingsincidenten	Baseline	Ja
A.16.01.06	Lering van informatiebeveiligingsincidenten	Baseline	Ja
A.16.01.07	Verzamelen van bewijsmateriaal	Baseline	Ja
A.17 Informatiebeveiligingsaspecten en bedrijfscontinuïteitsbeheer			
A.17.01.01	Informatiebeveiligingscontinuïteit plannen	Baseline	Ja
A.17.01.02	Informatiebeveiligingscontinuïteit implementeren	Baseline	Ja
A.17.01.03	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Baseline	Ja
A.17.02.01	Beschikbaarheid van informatie verwerkende systemen	Baseline	Ja
A.18 Naleving			
A.18.01.01	Vaststellen van toepasselijke wetgeving en contractuele eisen	Baseline	Ja
A.18.01.02	Intellectuele eigendomsrechten	Wet- en Regelgeving	Ja
A.18.01.03	Beschermen van registraties	Risicoanalyse	Ja
A.18.01.04	Privacy en bescherming van persoonsgegevens	Wet- en Regelgeving	Ja

A.18.01.05	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Baseline	Ja
A.18.02.01	Onafhankelijke beoordeling van informatiebeveiliging	Baseline	Ja
A.18.02.02	Naleving van beveiligingsbeleid en -normen	Baseline	Ja
A.18.02.03	Beoordeling op technische naleving	Baseline	Ja

4.2. Niet van toepassing zijnde maatregelen

Onderstaande maatregelen zijn niet van toepassing bij Parantion. Deze worden echter wel meegenomen met de jaarlijkse review en risicobeoordeling.

Maatregel nr.	Maatregelomschrijving	Reden niet van toepassing	Geïmplementeerd
A.14.02.07	Uitbestede softwareontwikkeling	Parantion besteedt de ontwikkeling van programmatuur niet uit. Zij doet de ontwikkeling van haar applicaties allenmaal binnen de organisatie zelf.	Nee