VERKLARING VAN TOEPASSELIJKHEID

VAN ROEY AUTOMATION | 9/09/2024

vanroey

INGE VAN BEERS | INGE.VANBEERS@VANROEY.BE | +32 14 470 600

INHOUDSTABEL

INLEIDING

Doelstelling

De Verklaring van Toepasselijkheid (Statement of Applicability - SoA) beschrijft de beveiligingsmaatregelen die zijn geïmplementeerd binnen het Informatiebeveiligingsmanagementsysteem (ISMS) van VanRoey. Dit document bevat een overzicht van de relevante controles uit Annex A van de ISO 27001:2022-norm, met daarbij een toelichting op welke maatregelen zijn toegepast, welke niet van toepassing zijn, en waarom.

De Verklaring van Toepasselijkheid (SoA) heeft betrekking op alle systemen en processen binnen de scope van het ISMS van VanRoey en dekt het volledige bereik van de organisatie waar informatiebeveiligingsmaatregelen van toepassing zijn.

Versiebeheer

Versie document	Datum wijziging	Auteur	Samenvatting wijzigingen
0.0	09/09/2024	Inge Van Beers	Opmaak document
1.0	09/12/2024	Inge Van Beers	Update, aanpassing 'Reden van insluiting'

ANNEX A CONTROLES

De Verklaring van Toepasselijkheid bevat de onderbouwing voor inclusie en exclusie van de Annex A controls.

Control	Vereiste	Relevant	Reden	Status
A.5.1 Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerp specifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	JA	Risicobeoordeling	Geïmplementeerd
A.5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	JA	Risicobeoordeling	Geïmplementeerd
A.5.3 Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.	JA	Risicobeoordeling	Geïmplementeerd
A.5.4 Managementverantwoordelijkheden	Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerp specifieke beleidsregels en procedures van de organisatie.	JA	Risicobeoordeling	Geïmplementeerd
A.5.5 Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.	JA	Risicobeoordeling	Geïmplementeerd
A.5.6 Contact met speciale belangengroepen	De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.	JA	Risicobeoordeling	Geïmplementeerd
A.5.7 Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	JA	Risicobeoordeling	Geïmplementeerd
A.5.8 Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er behoort een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, te worden opgesteld en onderhouden.	JA	Risicobeoordeling	Geïmplementeerd
A.5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	JA	Risicobeoordeling	Geïmplementeerd
A.5.11 Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren.	JA	Risicobeoordeling	Geïmplementeerd
A.5.12 Classificeren van informatie	Informatie behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	JA	Risicobeoordeling	Geïmplementeerd
A.5.13 Labelen van informatie	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie	JA	Risicobeoordeling	Geïmplementeerd
A.5.14 Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.15 Toegangsbeveiliging	Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen	JA	Risicobeoordeling	Geïmplementeerd
A.5.16 Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	JA	Risicobeoordeling	Geïmplementeerd
A.5.17 Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.5.18 Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerp specifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	JA	Risicobeoordeling	Geïmplementeerd
A.5.19 Informatiebeveiliging in leveranciersrelaties	Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er behoren processen en procedures te worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	JA	Risicobeoordeling	Geïmplementeerd
A.5.23 Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld..	JA	Risicobeoordeling	Geïmplementeerd
A.5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren	JA	Risicobeoordeling	Geïmplementeerd
A.5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	JA	Risicobeoordeling	Geïmplementeerd
A.5.26 Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.5.27 Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	JA	Risicobeoordeling	Geïmplementeerd
A.5.28 Verzamelen van bewijsmateriaal	De organisatie behoort procedures vast te stellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.29 Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	JA	Risicobeoordeling	Geïmplementeerd
A.5.30 ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.31 Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, behoren te worden geïdentificeerd, gedocumenteerd en actueel gehouden.	JA	Risicobeoordeling	Geïmplementeerd
A.5.32 Intellectuele-eigendomsrechten	De organisatie behoort passende procedures te implementeren om intellectuele-eigendomsrechten te beschermen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.33 Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave	JA	Risicobeoordeling	Geïmplementeerd
A.5.34 Privacy en bescherming van persoonsgegevens	De organisatie behoort de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen.	JA	Risicobeoordeling	Geïmplementeerd
A.5.35 Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	JA	Risicobeoordeling	Geïmplementeerd
A.5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerp specifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.5.37 Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	JA	Risicobeoordeling	Geïmplementeerd
A.6.1 Screening	De achtergrond van alle kandidaten voor een dienstverband behoort te worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's	JA	Risicobeoordeling	Geïmplementeerd
A.6.2 Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging	JA	Risicobeoordeling	Geïmplementeerd
A.6.3 Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerp specifieke beleidsregels en procedures van de organisatie, krijgen voor zover relevant voor hun functie.	JA	Risicobeoordeling	Geïmplementeerd
A.6.4 Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	JA	Risicobeoordeling	Geïmplementeerd
A.6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	JA	Risicobeoordeling	Geïmplementeerd
A.6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.6.7 Werken op afstand	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	JA	Risicobeoordeling	Geïmplementeerd
A.6.8 Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	JA	Risicobeoordeling	Geïmplementeerd
A.7.1 Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.	JA	Risicobeoordeling	Geïmplementeerd
A.7.2 Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	JA	Risicobeoordeling	Geïmplementeerd
A.7.3 Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.	JA	Risicobeoordeling	Geïmplementeerd
A.7.4 Monitoren van de fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.	JA	Risicobeoordeling	Geïmplementeerd
A.7.5 Beschermen tegen fysieke en omgevingsdreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, te worden ontworpen en geïmplementeerd.	JA	Risicobeoordeling	Geïmplementeerd
A.7.6 Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	JA	Risicobeoordeling	Geïmplementeerd
A.7.7 ‘Clear desk’ en ‘clear screen’	Er behoren ‘clear desk’-regels voor papieren documenten en verwijderbare opslagmedia en ‘clear screen’-regels voor informatieverwerkende faciliteiten te worden gedefinieerd en op passende wijze te worden afgedwongen.	JA	Risicobeoordeling	Geïmplementeerd
A.7.8 Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd.	JA	Risicobeoordeling	Geïmplementeerd
A.7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.7.10 Opslagmedia	Opslagmedia behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	JA	Risicobeoordeling	Geïmplementeerd
A.7.11 Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	JA	Risicobeoordeling	Geïmplementeerd
A.7.12 Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.	JA	Risicobeoordeling	Geïmplementeerd
A.7.13 Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	JA	Risicobeoordeling	Geïmplementeerd
A.7.14 Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	JA	Risicobeoordeling	Geïmplementeerd
A.8.1 'User Endpoint Devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.2 Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten behoort te worden beperkt en beheerd	JA	Risicobeoordeling	Geïmplementeerd
A.8.3 Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	JA	Risicobeoordeling	Geïmplementeerd
A.8.4 Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.5 Beveiligde authenticatie	Er behoren beveiligde authenticatietechnologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.8.6 Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	JA	Risicobeoordeling	Geïmplementeerd
A.8.7 Bescherming tegen Malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn	JA	Risicobeoordeling	Geïmplementeerd
A.8.8 Beheer van technische kwetsbaarheden	Er behoort informatie te worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behorende passende maatregelen te worden getroffen.	JA	Risicobeoordeling	Geïmplementeerd
A.8.9 Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld	JA	Risicobeoordeling	Geïmplementeerd
A.8.10 Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer vereist is	JA	Risicobeoordeling	Geïmplementeerd
A.8.11 Maskeren van gegevens	Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerp specifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerp specifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving	JA	Risicobeoordeling	Geïmplementeerd
A.8.12 Voorkomen van gegevenslekken (Data leak prevention)	Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.13 Back-up van informatie	Back-ups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerp specifieke beleid inzake back-ups.	JA	Risicobeoordeling	Geïmplementeerd
A.8.14 Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.8.15 Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd	JA	Risicobeoordeling	Geïmplementeerd
A.8.16 Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	JA	Risicobeoordeling	Geïmplementeerd
A.8.17 Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen	JA	Risicobeoordeling	Geïmplementeerd
A.8.18 Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.19 Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	JA	Risicobeoordeling	Geïmplementeerd
A.8.20 Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen	JA	Risicobeoordeling	Geïmplementeerd
A.8.21 Beveiliging netwerkdiensten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen	JA	Risicobeoordeling	Geïmplementeerd
A.8.22 Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd	JA	Risicobeoordeling	Geïmplementeerd
A.8.23 Toepassen van webfilters	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd	JA	Risicobeoordeling	Geïmplementeerd
A.8.24 Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.25 Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.	JA	Risicobeoordeling	Geïmplementeerd

Control	Vereiste	Relevant	Reden	Status
A.8.26 Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	JA	Risicobeoordeling	Geïmplementeerd
A.8.27 Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	JA	Risicobeoordeling	Geïmplementeerd
A.8.28 Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling	JA	Risicobeoordeling	Geïmplementeerd
A.8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	JA	Risicobeoordeling	Geïmplementeerd
A.8.30 Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.	JA	Risicobeoordeling	Geïmplementeerd
A.8.31 Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.32 Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	JA	Risicobeoordeling	Geïmplementeerd
A.8.33 Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	JA	Risicobeoordeling	Geïmplementeerd
A.8.34 Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	JA	Risicobeoordeling	Geïmplementeerd

GOEDKEURINGEN

Dit document en de hierin opgenomen beveiligingsmaatregelen zijn formeel goedgekeurd door het management van VanRoey. De goedkeuring bevestigt het engagement van het management voor de implementatie en het voortdurende beheer van het ISMS.

REVISIE EN HERZIENING

Deze Verklaring van Toepasselijkheid wordt jaarlijks herzien of wanneer er substantiële wijzigingen zijn in de organisatie, de informatiebeveiligingsrisico's of de relevante regelgeving. Wijzigingen worden gedocumenteerd en goedgekeurd door de directie.

DocuSigned by: David Verwerft 9F45360ADFE148B...
DocuSigned by: Hans Hoskens 7A93B282442F46A...
Ondertekend door: 274B099D65E24D2...
DocuSigned by: Karin Versmissen CA55B7423D134BB...
Ondertekend door: Roel Van Looy 10381171B0764F4...
DocuSigned by: Jeroen Lavrysen 11B175057F064D6...