4net interactive

# Verklaring van Toepasselijkheid

ISO27001:2022

| | |
|---|---|
| Auteur | Robin van Eck van der Sluijs *CSO* |
| Datum | 08 April 2026 |
| Versie | 1.8 |
| Nummer | V.2026.04.08 |

PUBLIEK

## Inhoudsopgave

# 1. Inleiding

Voor u ligt de Verklaring van Toepasselijkheid (VvT) van 4net Interactive. Dit document beschrijft de maatregelen die wij nemen om onze informatie te beveiligen en aan de eisen van de ISO 27001:2022-norm te voldoen. De VvT is een essentieel onderdeel van onze ISO 27001:2022-certificering en dient als bewijs dat wij voldoen aan de norm en onze verplichtingen op het gebied van informatiebeveiliging serieus nemen. In deze verklaring worden de relevante maatregelen en hun effectiviteit beschreven, zodat belanghebbenden inzicht krijgen in ons informatiebeveiligingsbeleid en de manier waarop wij risico's op het gebied van informatiebeveiliging beheersen. Wij hebben deze verklaring opgesteld om transparantie te bieden over onze informatiebeveiligingsmaatregelen en om aan te tonen dat wij ons inzetten voor het beschermen van onze gevoelige informatie en die van onze klanten.

# 2. Verklaring van Toepasselijkheid

Deze verklaring van toepasselijkheid geldt voor ISO27001:2022. De maatregelen in de Verklaring van Toepasselijkheid volgen uit beleid en/of risicoanalyse.

| | **Beheersmaatregel** | **Van toepassing** | **Geïmplementeerd, (onderbouwing)** | **Grondslag**<br>- Risico<br>- Wettelijk<br>- Contractueel<br>- Beleid |
|---|---|---|---|---|
| **5 - Organisatorische beheersmaatregelen** | | | | |
| 5.1 Beleidsregels voor informatiebeveiliging | *Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoren te 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, te worden beoordeeld.* | Ja | Ja | - Risico |
| 5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging | *Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden* | Ja | Ja | - Risico<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| | *gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.* | | | |
| 5.3 Functiescheiding | *Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.* | Ja | Ja | - Risico |
| 5.4 Managementverantwoordelijkheden | *Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.* | Ja | Ja | - Risico |
| 5.5 Contact met overheidsinstanties | *De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.* | Ja | Ja | - Wettelijk<br>- Risico<br>- Contractueel |
| 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 | Ja | - Risico |
| 5.7 Informatie en analyses over dreigingen | *Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te* | Ja | Ja | - Wettelijk<br>- Risico<br>Contractueel |

| | | | | |
|---|---|---|---|---|
| | *worden verzameld en geanalyseerd om informatie over dreigingen te produceren.* | | | |
| 5.8 Informatiebeveiliging in projectmanagement | *Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico<br>- Contractueel |
| 5.12 Classificeren van informatie | *Informatie behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| | *organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.* | | | |
| 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 | Ja | - Risico |
| 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 | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| 5.16 Identiteitsbeheer | *De volledige levenscyclus van identiteiten behoort te worden beheerd.* | | | - Risico |
| 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 | Ja | - Risico |
| 5.18 Toegangsrechten | *Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |
| 5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten | *Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| | *leveranciersrelatie te worden overeengekomen.* | | | |
| 5.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen | *Er behoren processen en procedures te worden bepaald en geïmplementeerd om de informatie-beveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |
| 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 | Ja | - Wettelijk<br>- Risico<br>- Contractueel |
| 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* | Ja | Ja | - Risico<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| | *informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.* | | | |
| 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 | Ja | - Risico<br>- Contractueel |
| 5.26 Reageren op informatiebeveiligingsincidenten | *Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.* | Ja | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico |
| 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 | Ja | - Risico<br>- Wettelijk |

| | | | | |
|---|---|---|---|---|
| 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 | Ja | - Risico<br>- Wettelijk<br>- Contractueel |
| 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 | Ja | - Risico<br>- Wettelijk<br>- Contractueel |
| 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 | Ja | - Risico<br>- Wettelijk<br>- Contractueel |
| 5.32 Intellectuele-eigendomsrechten | *De organisatie behoort passende procedures te implementeren om intellectuele-eigendomsrechten te beschermen.* | Ja | Ja | - Risico<br>- Wettelijk<br>- Contractueel |
| 5.33 Beschermen van registraties | *Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.* | Ja | Ja | - Risico<br>- Wettelijk<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| 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 | Ja | - Risico<br>- Wettelijk<br>- Contractueel |
| 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 | Ja | - Risico |
| 5.36 Naleving van beleid, regels en normen voor informatiebeveiliging | *De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.* | Ja | Ja | - Risico<br>- Contractueel |
| 5.37 Gedocumenteerde bedieningsprocedures | *Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| | *te worden gesteld aan het personeel dat ze nodig heeft.* | | | |
| **6 - Mensgerichte beheersmaatregelen** | | | | |
| 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 | Ja | - Risico |
| 6.2 Arbeidsovereenkomst | *In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.* | Ja | Ja | - Risico<br>- Contractueel |
| 6.3 Bewustwording van, opleiding en training in informatiebeveiliging | *Personeel van de organisatie en relevante belanghebbenden behoren een passende bewustwording van, opleiding en training* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| | *in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.* | | | |
| 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 | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico<br>- Contractueel |
| 6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten | *Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de* | Ja | Ja | - Risico<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| | *bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.* | | | |
| 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 | Ja | - Risico |
| 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 | Ja | - Risico<br>- Contractueel |
| **7 - Fysieke beheersmaatregelen** | | | | |
| 7.1 Fysieke beveiligingszones | *Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.* | Ja | Ja | - Risico<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| 7.2 Fysieke toegangsbeveiliging | *Beveiligde zones behoren te worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.* | Ja | Ja | - Risico |
| 7.3 Beveiligen van kantoren, ruimten en faciliteiten | *Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.* | Ja | Ja | - Risico |
| 7.4 Monitoren van de fysieke beveiliging | *Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |
| 7.6 Werken in beveiligde zones | *Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.* | Ja | Ja | - Risico |
| 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* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| | *worden gedefinieerd en op passende wijze te worden afgedwongen.* | | | |
| 7.8 Plaatsen en beschermen van apparatuur | *Apparatuur behoort veilig te worden geplaatst en beschermd.* | Ja | Ja | - Risico |
| 7.9 Beveiligen van bedrijfsmiddelen buiten het terrein | *Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |
| 7.11 Nutsvoorzieningen | *Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.* | Ja | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| 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 | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico<br>- Contractueel |
| **8 - Technologische beheersmaatregelen** | | | | |
| 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 | Ja | - Risico |
| 8.2 Speciale toegangsrechten | *Het toewijzen en het gebruik van speciale toegangsrechten behoort te worden beperkt en beheerd.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| 8.4 Toegangsbeveiliging op broncode | *Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |
| 8.6 Capaciteitsbeheer | *Het gebruik van middelen behoort te worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.* | Ja | Ja | - Risico<br>- Contractueel |
| 8.7 Bescherming tegen malware | *Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.* | Ja | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| 8.9 Configuratiebeheer | *Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.* | Ja | Ja | - Risico |
| 8.10 Wissen van informatie | *In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer vereist is.* | Ja | Ja | - Risico<br>- Wettelijk |
| 8.11 Maskeren van gegevens | *Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.* | Ja | Ja | - Risico |
| 8.12 Voorkomen van gegevenslekken (data leakage 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 | Ja | - Risico<br>- Wettelijk<br>- Contractueel |
| 8.13 Back-up van informatie | *Back-ups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest* | Ja | Ja | - Risico<br>- Contractueel |

| | | | | |
|---|---|---|---|---|
| | *overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.* | | | |
| 8.14 Redundantie van informatieverwerkende faciliteiten | *Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.* | Ja | Ja | - Risico<br>- Contractueel |
| 8.15 Logging | *Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico<br>Contractueel |
| 8.17 Kloksynchronisatie | *De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.* | Ja | Ja | - Risico |
| 8.18 Gebruik van speciale systeemhulpmiddelen | *Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| | *beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.* | | | |
| 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 | Ja | - Risico<br>- Contractueel |
| 8.20 Beveiliging netwerkcomponenten | *Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.* | Ja | Ja | - Risico |
| 8.21 Beveiliging van netwerkdiensten | *Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord.* | Ja | Ja | - Risico |
| 8.22 Netwerksegmentatie | *Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.* | Ja | Ja | - Risico |
| 8.23 Toepassen van webfilters | *De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.* | Ja | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| 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 | Ja | - Risico |
| 8.25 Beveiligen tijdens de ontwikkelcyclus | *Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.* | Ja | Ja | - Risico |
| 8.26 Toepassingsbeveiligingseisen | *Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |
| 8.28 Veilig coderen | *Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling.* | Ja | Ja | - Risico<br>- Contractueel |
| 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 | Ja | - Risico |

| | | | | |
|---|---|---|---|---|
| 8.30 Uitbestede systeemontwikkeling | *De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.* | Ja | Ja | - Risico |
| 8.31 Scheiding van ontwikkel-, test- en productieomgevingen | *Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.* | Ja | Ja | - Risico |
| 8.32 Wijzigingsbeheer | *Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.* | Ja | Ja | - Risico<br>- Contractueel |
| 8.33 Testgegevens | *Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.* | Ja | Ja | - Risico |
| 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 | Ja | - Risico |