Informatiebeveiliging
PM Networking Group

Verklaring van toepasselijkheid
Informatiebeveiligingsbeleid

NEN-ISO/IEC 27001;2022
Versie 1.1, Datum 16-11-2023

Inhoudsopgave

1. Informatiebeveiligingsbeleid

Ons informatiebeveiligingsbeleid stelt veiligheid als hoogste prioriteit, met als doel het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van bedrijfsgegevens en -systemen, en het implementeren van proactieve maatregelen om potentiële risico's en bedreigingen te minimaliseren. Dit omvat continue monitoring, bewustzijnsbevordering en naleving van best practices in informatiebeveiliging.

1.1 Scope

Binnen de scope van het ISMS valt PM Networking Group B.V. en de daaronder liggende werkmaatschappijen: PM Networking B.V. en PM Coded B.V. Dit zal verder worden benoemd als PM Networking Group. De scope is als volgt gedefinieerd:

“Informatiebeveiliging in relatie tot softwareontwikkeling, inrichting en beheer van server- en netwerkomgevingen, werkplekken en ICT consultancy.”

1.2 Activatie Verklaring van Toepasselijkheid

Voor u ligt de definitie Verklaring van Toepasselijkheid (VVT) van PM Networking Group waarin de borging is beschreven van het informatiebeveiligingsbeleid conform NEN-ISO/IEC 27001;2022. De VVT beschrijft het normenkader waar de organisatie zich aan committeert en beschrijft eventuele reden van uitsluiting.

1.3 Verantwoordelijkheden

De reikwijdte van de VVT is vastgesteld in samenspraak met het directieteam. Met het ondertekenen is het de verantwoordelijkheid van de directie om de maatregelen te treffen die noodzakelijkerwijs volgen uit het ISMS. Toetsing van het NEN-ISO/IEC 27001 ISMS vindt plaats door de geaccrediteerde certificatie instelling Kiwa. Om het ISMS doeltreffend en efficiënt te houden treft de organisatie jaarlijks de nodige maatregelen en acties met de benodigde resources.

Ondertekend namens het directieteam van PM Networking Group		
Naam	ing. Maarten Hesse	Handtekening
Functie	CEO - PM Networking Group B.V.	
Plaats	Purmerend	
Datum	17-10-2023	

2. Verklaring van Toepasselijkheid

De verklaring van toepasselijkheid in de volgende tabel met de volgende kolommen: 1. Het nummer van de beheersmaatregel; 2. De naam van de beheersmaatregel; 3. De reden van toepassing, 4. Of de beheersmaatregel is geïmplementeerd en 5. De uitgeschreven beheersmaatregel.

Annex / maatregel nr.	Maatregel omschrijving	Reden van toepassing	Geïmplementeerd	Beheersmaatregel
A.5 Organisatorische beheersmaatregelen				
A.5.1	Beleidsregels voor informatiebeveiliging	Baseline	Ja	Informatiebeveiligingsbeleid en onderwerpspecifieke 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
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Baseline	Ja	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.
A.5.3	Functiescheiding	Baseline	Ja	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.
A.5.4	Managementverantwoordelijkheden	Baseline	Ja	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde

				informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.
A.5.5	Contact met overheidsinstanties	Baseline	Ja	De organisatie moet contact met de relevante instanties leggen en onderhouden.
A.5.6	Contact met speciale belangengroepen	Baseline	Ja	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.
A.5.7	Informatie en analyses over dreigingen	Risicoanalyse	Ja	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.
A.5.8	Informatiebeveiliging in projectmanagement	Risicoanalyse	Ja	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Risicoanalyse	Ja	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Risicoanalyse	Ja	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.
A.5.11	Retourneren van bedrijfsmiddelen	Risicoanalyse	Ja	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.

A.5.12	Classificeren van informatie	Risicoanalyse	Ja	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.
A.5.13	Labelen van informatie	Risicoanalyse	Ja	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
A.5.14	Overdragen van informatie	Risicoanalyse	Ja	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.
A.5.15	Toegangsbeveiliging	Risicoanalyse	Ja	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.
A.5.16	Identiteitsbeheer	Risicoanalyse	Ja	De volledige levenscyclus van identiteiten moet worden beheerd.
A.5.17	Authenticatie-informatie	Risicoanalyse	Ja	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.

A.5.18	Toegangsrechten	Risicoanalyse	Ja	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.
A.5.19	Informatiebeveiliging in leveranciersrelaties	Risicoanalyse	Ja	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Risicoanalyse	Ja	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.
A.5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Risicoanalyse	Ja	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-productenen -diensten te beheersen.
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Risicoanalyse	Ja	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Risicoanalyse	Ja	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten

				overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Baseline	Ja	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie- beveiligingsincidenten te definiëren, vast te stellen en te communiceren.
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsincidenten	Baseline	Ja	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.
A.5.26	Reageren op informatiebeveiligingsincidenten	Baseline	Ja	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.
A.5.27	Leren van informatiebeveiligingsincidenten	Baseline	Ja	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de en voor informatiebeveiliging te versterken en te verbeteren.
A.5.28	Verzamelen van bewijsmateriaal	Risicoanalyse	Ja	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.
A.5.29	Informatiebeveiliging tijdens een verstoring	Risicoanalyse	Ja	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	Risicoanalyse	Ja	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis

				van bedrijfscontinuïteitsdoel- stellingen en ICT-continuïteitseisen.
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wetgeving	Ja	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.
A.5.32	Intellectuele-eigendomsrechten	Wetgeving	Ja	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.
A.5.33	Beschermen van registraties	Wetgeving	Ja	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.
A.5.34	Privacy en bescherming van persoonsgegevens	Wetgeving	Ja	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	Risicoanalyse	Ja	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.
A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Baseline	Ja	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de

				normen van de organisatie moet regelmatig worden beoordeeld.
A.5.37	Gedocumenteerde bedieningsprocedures	Baseline	Ja	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.
A.6 Mensgerichte beheersmaatregelen				
A.6.1	Screening	Risicoanalyse	Ja	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.
A.6.2	Arbeidsovereenkomst	Baseline	Ja	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Risicoanalyse	Ja	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures

				van de organisatie, voor zover relevant voor hun functie, krijgen.
A.6.4	Disciplinaire procedure	Risicoanalyse	Ja	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Risicoanalyse	Ja	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Baseline	Ja	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.
A.6.7	Werken op afstand	Risicoanalyse	Ja	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	Risicoanalyse	Ja	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede

				informatiebeveiligings- gebeurtenissen tijdig via passende kanalen kan melden.
A.7 Fysieke beheersmaatregelen				
A.7.1	Fysieke beveiligingszones	Risicoanalyse	Ja	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.
A.7.2	Fysieke toegangsbeveiliging	Risicoanalyse	Ja	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.
A.7.3	Beveiliging van kantoren, ruimten en faciliteiten	Risicoanalyse	Ja	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.
A.7.4	Monitoren van de fysieke beveiliging	Risicoanalyse	Ja	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Risicoanalyse	Ja	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.
A.7.6	Werken in beveiligde zones	Risicoanalyse	Ja	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.
A.7.7	‘Clear desk’ en ‘clear screen’	Risicoanalyse	Ja	Er moeten ‘clear desk’-regels voor papieren documenten en verwijderbare opslagmedia en ‘clear screen’-regels voor informatieverwerkende

				faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.
A.7.8	Plaatsen en beschermen van apparatuur	Risicoanalyse	Ja	Apparatuur moet veilig worden geplaatst en beschermd.
A.7.9	Beveiliging van bedrijfsmiddelen buiten het terrein	Risicoanalyse	Ja	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.
A.7.10	Opslagmedia	Risicoanalyse	Ja	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.
A.7.11	Nutsvoorziening	Risicoanalyse	Ja	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.
A.7.12	Beveiliging van bekabeling	Risicoanalyse	Ja	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.
A.7.13	Onderhoud van apparatuur	Risicoanalyse	Ja	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Risicoanalyse	Ja	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.

A.8 Technologische beheersmaatregelen				
A.8.1	'User endpoint devices'	Risicoanalyse	Ja	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.
A.8.2	Speciale toegangsrechten	Risicoanalyse	Ja	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.
A.8.3	Beperking toegang tot informatie	Risicoanalyse	Ja	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.
A.8.4	Toegangsbeveiliging op broncode	Risicoanalyse	Ja	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.
A.8.5	Beveiligde authenticatie	Risicoanalyse	Ja	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.
A.8.6	Capaciteitsbeheer	Risicoanalyse	Ja	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.
A.8.7	Bescherming tegen malware	Risicoanalyse	Ja	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.
A.8.8	Beheer van technische kwetsbaarheden	Risicoanalyse	Ja	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde

				informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.
A.8.9	Configuratiebeheer	Risicoanalyse	Ja	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.
A.8.10	Wissen van informatie	Risicoanalyse	Ja	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.
A.8.11	Maskeren van gegevens	Risicoanalyse	Ja	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.
A.8.12	Voorkomen van gegevenslekken	Risicoanalyse	Ja	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.
A.8.13	Back-up van informatie	Risicoanalyse	Ja	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.

A.8.14	Redundantie van informatieverwerkende faciliteiten	Risicoanalyse	Ja	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.
A.8.15	Logging	Risicoanalyse	Ja	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.
A.8.16	Monitoren van activiteiten	Risicoanalyse	Ja	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.
A.8.17	Kloksynchronisatie	Risicoanalyse	Ja	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.
A.8.18	Gebruik van speciale systeemhulpmiddelen	Risicoanalyse	Ja	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om en voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.
A.8.19	Installeren van software op operationele systemen	Risicoanalyse	Ja	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.
A.8.20	Beveiliging netwerkcomponenten	Risicoanalyse	Ja	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.

A.8.21	Beveiliging van netwerkdiensten	Risicoanalyse	Ja	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.
A.8.22	Netwerksegmentatie	Risicoanalyse	Ja	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.
A.8.23	Toepassen van webfilters	Risicoanalyse	Ja	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.
A.8.24	Gebruik van cryptografie	Risicoanalyse	Ja	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Risicoanalyse	Ja	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.
A.8.26	Toepassingsbeveiligingseisen	Risicoanalyse	Ja	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Risicoanalyse	Ja	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.
A.8.28	Veilig coderen	Risicoanalyse	Ja	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.

A.8.29	Testen van beveiliging tijdens ontwikkeling en acceptatie	Risicoanalyse	Ja	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.
A.8.31	Scheiding van ontwikkel-, test productieomgevingen	Risicoanalyse	Ja	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.
A.8.32	Wijzigingsbeheer	Risicoanalyse	Ja	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.
A.8.33	Testgegevens	Risicoanalyse	Ja	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.
A.8.34	Bescherming van informatiesystemen tijdens audits	Risicoanalyse	Ja	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.

3. Niet van toepassing zijnde maatregelen

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

Annex / maatregel nr.	Maatregel omschrijving	Reden van niet toepassing	Geïmplementeerd
A.8.30	Uitbesteden softwareontwikkeling	Risicoanalyse	N.v.t.
	PM Networking Group besteedt het ontwikkelen van software niet uit. Enkel eigen software of standaard software(pakketten) zullen worden gebruikt voor het uitvoeren van de diensten.		