PM networking

ICT Solutions
Software development
Business Services
Webhosting

Informatiebeveiligingsbeleid

ISMS01

Documenteigenaar: Bram Bekebrede

Versie	Auteur	Wijziging (omschrijving)	Datum vaststelling
V1.0	Bram Bekebrede	Opstellen webversie informatiebeveiligingsbeleid	29-9-2023

Inhoudsopgave

1. Doel van dit document

In dit beleidsdocument beschrijft PM Networking Group de wijze waarop haar Information Security Management System (ISMS) is ingericht. Dit document fungeert als basis voor het inrichten van informatieveiligheid van PM Networking Group en als motivator voor het continu verhogen van het beveiligingsniveau. De directie van PM Networking Group is betrokken bij de uitvoering hiervan en conformeert zich aan de informatiebeveiligingsdoelstellingen.

De inrichting van het ISMS is gebaseerd op de ISO27001.

Het ISMS omvat een samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen.

Een samenhangend stelsel van maatregelen betekent dat de maatregelen niet los van elkaar kunnen worden gezien, maar in onderlinge relatie tot elkaar staan. Het stelsel van beveiligingsmaatregelen heeft tot doel een blijvend niveau van informatiebeveiliging te realiseren. Door zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd. Het gewenste niveau is ook het optimale niveau dat mede bereikt wordt door een zorgvuldige afweging van kosten en baten.

Informatiebeveiligingsmaatregelen omvatten maatregelen op het gebied van:

- Fysieke beveiliging, zoals de beveiliging van gebouwen en de fysieke toegang door individuen.
- Personele beveiliging, zoals maatregelen gericht op het verbeteren van gedrag en getraindheid van medewerkers.
- Maatregelen op het werkterrein van de ICT, zoals firewalls, virusscanners etc.

2. Reikwijdte en gebruikers

Reikwijdte

Binnen de scope van het ISMS vallen PM Networking B.V. en PM Coded B.V. De scope is als volgt gedefinieerd:

Informatiebeveiliging in relatie tot alle processen in de PM Networking Group, met als doel het uitvoeren van systeembeheer, programmeerwerkzaamheden en consult verlenen. Conform laatste versie van de Verklaring van Toepasselijkheid.

Gebruikers

De gebruikers van dit document zijn:

- Medewerkers van PM Networking Group
- Belanghebbenden van PM Networking Group

3. Informatiebeveiligingsdoelstellingen

PM Networking Group heeft op basis van haar missie informatiebeveiligingsdoelstellingen opgesteld. Dit is gedaan om ervoor te zorgen dat het geheel aan maatregelen die voortvloeit uit de informatiebeveiligingsdoelstellingen passend is voor de PM Networking Group. De missie van PM Networking Group is omschreven in de bedrijfsstrategie en het jaarplan. De volgende informatiebeveiligingsdoelstellingen zijn gesteld:

1. De dienstverlening van PM Networking Group verloopt ongestoord en op het juiste kwaliteitsniveau.
   - KPI: Incidenten binnen 1 werkdagen behandelen (responsetijd).
   - KPI: Klantverzoeken binnen 3 werkdagen behandelen (standaard changes, niet standaard changes).
   - KPI: Klachten binnen 3 werkdagen behandelen (indien ingediend op de juiste wijze).
2. De Directie van PM Networking Group is in control van informatiebeveiligingsrisico's (conform Datalekken Protocol Data Pro code).
   - KPI: 1 risicoanalyse per jaar.
   - KPI: 2 awareness sessies per jaar omtrent relevante onderwerpen.
   - KPI: 10 keer per jaar een securityoverleg.
   - KPI: Verwerkingstijd voor risico's met risicoscore 20 of hoger binnen 1 week.
   - KPI: Verwerkingstijd voor risico's met risicoscore van 10 tot 20 binnen 1 maand.
3. De informatie van PM Networking Group is ingericht conform een need-to-know principe en beperkt beschikbaar:
   - KPI: Het on- en offboarden van medewerkers wordt bewerkstelligd binnen 1 werkdag.

4.Relevante kenmerken en belanghebbenden

4.1 Relevante kenmerken

Met relevante kenmerken wordt uitgegaan van alle zaken die keuzes op het gebied van informatiebeveiliging kunnen beïnvloeden. Dit wordt ook wel 'interne en externe context' genoemd. De volgende kenmerken van PM Networking Group groep zijn relevant voor het informatiebeveiligingsbeleid en de inrichting van het ISMS:

- PM Networking Group werkt met klanten die werkzaam zijn in diverse sectoren. Het beschermen van de vertrouwelijkheid van de gegevens van haar klanten heeft bij PM Networking Group de hoogste prioriteit.
- PM Networking Group heeft projecten die niet kunnen worden gecommuniceerd naar de buitenwereld in verband met de gevoelige informatie die hierbij gemoeid is. Het beschermen van de vertrouwelijkheid van informatie en gegevens van deze projecten heeft bij PM Networking Group een hoge prioriteit.

- PM Networking Group heeft een grote expertise op het gebied van ICT. Door gebruik te maken van deze expertise is het mogelijk om constant te ontwikkelen op de gebieden beschikbaarheid, integriteit en vertrouwelijkheid.
- PM Networking Group voert haar werkzaamheden uit op diverse locaties. Medewerkers maken, naast het kantoor van PM Networking Group zelf, gebruik van kantoorruimtes van andere organisaties of medewerkers voeren hun werkzaamheden uit vanuit huis.
- Vanuit de privacywetgeving worden eisen gesteld aan veiligheidsmaatregelen van PM Networking Group.

4.2 Belanghebbenden

De belanghebbenden van PM Networking Group zijn de medewerkers en de externen die bij PM Networking Group werkzaam zijn, de verzekeraars en klanten, die belang hebben bij de kwaliteit van de dienstverlening van PM Networking Group en partners waar PM Networking Group samenwerkt aan projecten.

De belanghebbenden zijn in meer detail vastgelegd in het tactisch beleidsdocument *ISMSog Voldoen aan overeenkomsten en wet- en regelgeving*.

5. Rollen binnen het ISMS

Informatiebeveiliging is de verantwoordelijkheid van iedereen binnen PM Networking Group. Een aantal medewerkers heeft een specifieke rol gekregen. Een goede verdeling van taken, bevoegdheden en verantwoordelijkheden tussen deze rollen is belangrijk voor een effectief en efficiënt procesverloop.

In de organisatiematrix hieronder zijn in een tabel de functionarissen weergegeven PM Networking Group de verantwoordelijkheden aangaande informatiebeveiliging heeft belegd. Onder de tabel staat de rol die daarbij hoort nader toegelicht.

De Directie van PM Networking Group stelt in dit hoofdstuk ten behoeve van informatiebeveiliging een duidelijke organisatiestructuur vast, met passende verantwoordelijkheden en bevoegdheden. In de tabel hieronder is een organisatiematrix opgenomen. Deze matrix geeft inzicht in de verdeling van verantwoordelijkheden en taken over de fases van de PDCA-cyclus (Plan, Do, Check, Act). Hierin staan ook de RACI-rollen aangegeven. De RACI-rollen staan na de tabel toegelicht.

5.1 Verantwoordelijkheden

De verantwoordelijkheden zijn verdeeld over de directie, CISO, security officer en verantwoordelijke HR. Voor de rest van de medewerkers zijn geen functie specifieke rollen, maar werkt iedereen mee aan het verbeteren van de informatiebeveiliging binnen PM Networking Group.

5.3 Securityoverleg

Eens per maand vindt een securityoverleg plaats. Dit overleg wordt uitgevoerd met de directie en de Security Officer. Op het moment dat een incident (zowel intern als bij klanten) heeft plaatsgevonden

zal een ad-hoc overleg kunnen worden ingeplant. Als deze kort voor een geplant overleg plaatsvindt zal het geplande overleg komen te vervallen. De gemaakte notulen van een securityoverleg wordt opgeslagen in de daarvoor bestemde map in de SharePoint.

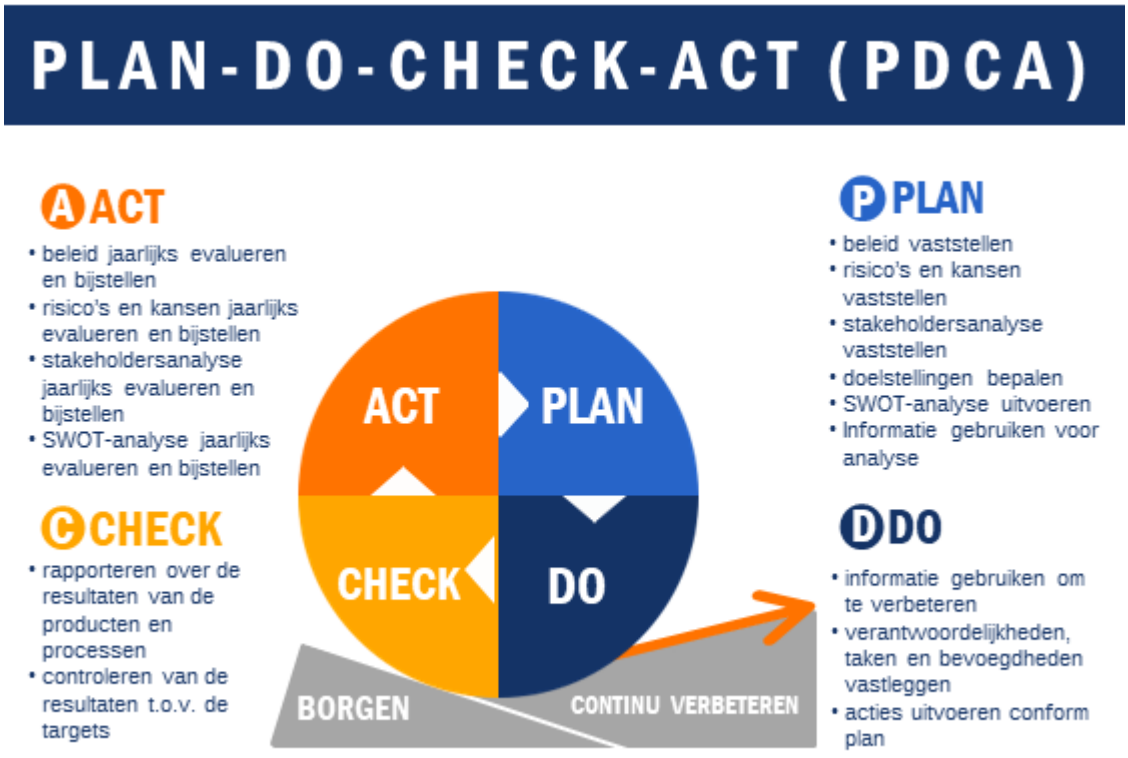
5.4 Scheiding van taken

Daar waar zich de kans voordoet dat er conflicterende taken en verantwoordelijkheidsgebieden ontstaan worden deze gescheiden om de kans op onbevoegde wijziging of misbruik van persoons-/bedrijfsinformatie of misbruik van de bedrijfsmiddelen van PM Networking Group te verminderen. Waar dit kan optreden wordt dat vastgesteld met behulp van de risicoanalyse. Afspraken worden vastgelegd in relevante procedures en werkafspraken. Voorbeeld; marketing kan niet bij systeem wachtwoorden, ontwikkelaars zijn de enige die toegang hebben tot broncode, etc.

6. Het ISMS

De informatiebeveiliging van PM Networking Group is een cyclisch proces. Het proces wordt beheerst door middel van het ISMS (Informatie Security Management System). De cyclus wordt jaarlijks tenminste éénmaal doorlopen.

Uitgangspunt is dat zoveel mogelijk aangesloten wordt bij de gangbare planning en control- en rapportagecyclus. De onderdelen van het ISMS zijn in onderstaand schema weergegeven.



6.1 Plan, beleid, risicomanagement en jaarplan beveiliging

De basis voor de besturing van informatiebeveiliging wordt gelegd met het vaststellen van doelen, en de daaruit voortvloeiende activiteiten en benodigde middelen. Deze zijn vastgelegd in dit beleidsdocument.

Door middel van een systematiek van risicobeoordeling worden jaarlijks de afhankelijkheden en risico's van PM Networking Group opnieuw beoordeeld, en door de directie vastgesteld. Waar nodig worden verbeterprojecten in het behandelplan uitgewerkt. Wanneer zich ontwikkelingen voordoen die (mogelijk) impact hebben op de beveiligingssituatie, wordt een specifieke risicobeoordeling uitgevoerd.

6.2 Do, uitvoeren en implementatie

Dit gebeurt door implementatie, onderhoud en toepassing van een adequate set van procedurele, technische en organisatorische maatregelen (verbeterprojecten). Over de goede werking van deze maatregelen wordt de Security Officer regelmatig geïnformeerd door degenen die verantwoordelijk zijn voor de uitvoering. Alle medewerkers zijn verantwoordelijk voor een geode werking van de getroffen maatregelen. De benodigde controlemaatregelen hiervoor staan niet op zich, maar zijn geïntegreerd onderdeel van de algemene kwaliteitszorg. De genomen maatregelen zijn beschreven in beleidsdocumenten, procedures en/of richtlijnen.

6.3 Check, controles en audits

Door middel van dit onderdeel van het ISMS realiseert PM Networking Group dat fouten in het ISMS worden ontdekt en dat inbreuken op het gewenste beveiligingsniveau worden geïdentificeerd. Hierdoor wordt de directie van PM Networking Group tijdig geïnformeerd en kan zij adequate actie ondernemen.

Onder controle worden zowel interne controles door de eigen organisatie, als periodieke toetsing door een onafhankelijke derde partij verstaan. De toetsing richt zich zowel op het informatiebeveiligings-beleid als op de maatregelen die uit dit beleid voortvloeien.

De jaarlijkse controle op beveiliging bestaat uit drie onderdelen:

- **Beoordelen effectiviteit van getroffen maatregelen**: Voor elk project die in het Jaarplan is opgenomen, zijn één of meerdere doelstellingen bepaald. Een aangewezen verantwoordelijke controleert op basis van vooraf gestelde criteria of deze doelstellingen bereikt zijn.
- **Interne en externe audits**: Een correcte borging van het ISMS is opgenomen in de auditstructuur. Hierbij wordt rekening gehouden met noodzakelijke functiescheiding. De functionarissen die zelf deel uitmaken van de beveiligingsorganisatie (i.e. de Security Officer) mogen niet de rol van interne auditor vervullen op hun eigen werkzaamheden. Dit om belangenverstrengeling te voorkomen.
- **Beoordeling toereikendheid**: Jaarlijks wordt het vastgestelde beleid, met inbegrip van alle maatregelen, op toereikendheid beoordeeld. Concreet betekent dit dat vastgesteld wordt of

- het beleid en de maatregelen zorgen voor een afdoende beveiligingsniveau van de processen en de informatiestromen van PM Networking Group.

Voor de beoordeling op toereikendheid wordt gebruik gemaakt van de resultaten van audits, risicobeoordelingen, incidenten en controles op procedures en richtlijnen. De resultaten van deze beoordelingen worden vastgelegd in de (jaarlijkse) *Managementreview*. Daar waar nodig wordt de toereikendheid van het beleid tussentijds beoordeeld.

6.4 Evaluatie, monitoren en beoordelen

Onder evaluatie wordt verstaan het nagaan of de kaders van de beveiliging inhoudelijk nog toereikend zijn. Hierbij worden twee niveaus onderscheiden: de evaluatie van het beleid en de evaluatie van het beheer. Het resultaat van de evaluatie kan leiden tot de bijstelling en vaststelling van beleidsdocumenten door de directie.

Door middel van monitoren en beoordelen zorgt PM Networking Group ervoor dat de resultaten van de interne en externe audits, en andere controles, worden vertaald naar adequate, corrigerende en preventieve maatregelen.

Om tijdige corrigerende en preventieve acties te borgen, heeft PM Networking Group voor het monitoren en- beoordelen de volgende maatregelen genomen:

- Er is een incidentmeldingsproces ingericht waarin geborgd is dat er direct geacteerd wordt bij ernstige incidenten. Onderdeel hiervan is ook het tijdig melden van een datalek bij de Autoriteit Persoonsgegevens.
- Periodiek analyseert de Security Officer de incidenten, rapporteert aan de Directie en doet een voorstel voor preventieve en corrigerende maatregelen.
- Alle informatiebeveiligingsbeleidsdocumenten bevatten controleprocedures om vast te stellen dat deze doeltreffend zijn, en nageleefd worden.

7. Samenvatting

In dit beleidsdocument informatiebeveiliging heeft de directie van PM Networking Group de strategische uitgangspunten en randvoorwaarden vastgesteld die worden gehanteerd ten aanzien van informatiebeveiliging. Om het informatiebeveiligingsbeleid binnen PM Networking Group te implementeren, is in de voorgaande hoofdstukken het volgende vastgesteld:

- De strategische uitgangspunten en randvoorwaarden en doelen die PM Networking Group hanteert ten aanzien van informatiebeveiliging, waaronder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid.
- De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.
- De bevordering van het veiligheids-/beveiligingsbewustzijn.

Op basis van dit beleidsdocument heeft PM Networking Group beleidsregels en geconcretiseerde normen vastgesteld. Constant worden beveiligingsmaatregelen uitgewerkt en geïmplementeerd om het informatiebeveiligingsniveau te verhogen.

8. Directie

De directie van PM Networking Group staat achter de laatste versie het informatiebeveiligingsbeleid en zal zich actief inzetten om de naleving van dit beleid te waarborgen.

Naam directielid *Peter van Kessel*	Naam directielid *Maarten Hesse*
Handtekening directielid	Handtekening directielid