
# INFORMATIE BEVEILIGINGSBELEID

**Inhoud**

1.Algemeen

2. Reikwijdte van het beleid

3. Doelstelling informatiebeveiligingsbeleid en doelstellingen 2022

4. Beleidsuitgangspunten en principes

5. Organisatie informatiebeveiliging en toewijzing van verantwoordelijkheden

6. Documenten informatiebeveiliging

**Algemeen**

Onder informatiebeveiliging wordt binnen DMG verstaan, het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatie te garanderen.

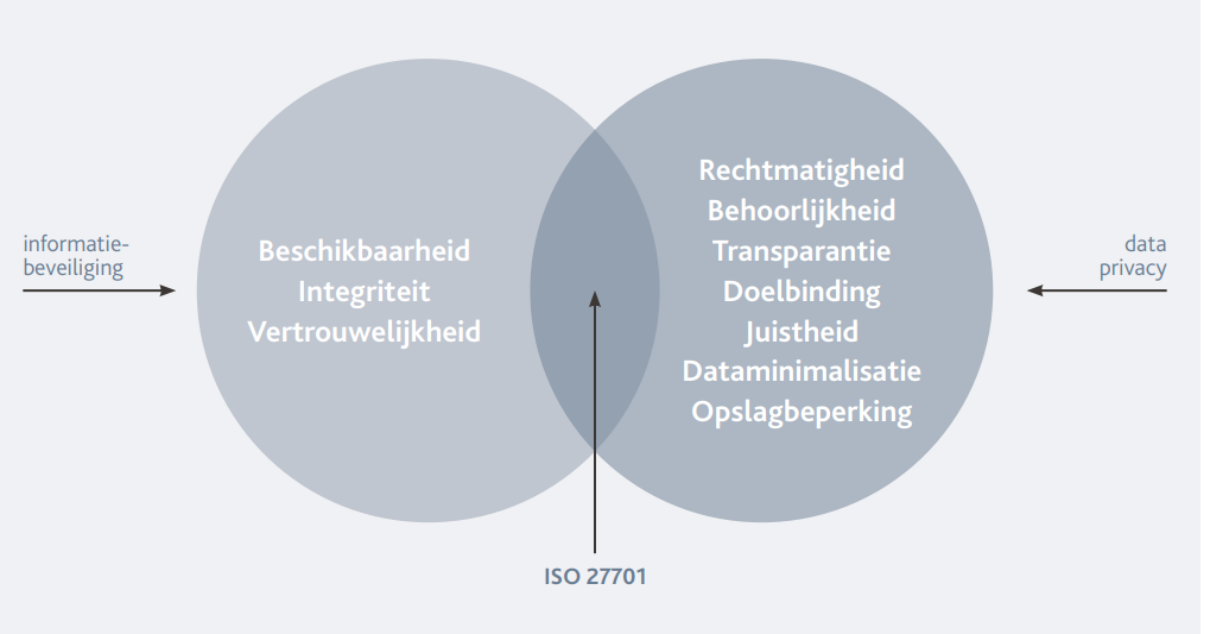
Hieronder wordt verstaan:

- Beschikbaarheid: de mate waarin gegevens of functionaliteiten op de juiste momenten beschikbaar zijn voor gebruikers;
- Integriteit: de mate waarin gegevens of functionaliteit juist ingevuld zijn;
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen. Informatiebeveiliging is een beleidsverantwoordelijkheid van de directie van DMG (hierna genoemd 'onze organisatie'). Binnen de markt van onze organisatie is sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onze dienstverlening. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

DMG heeft als ambitie om met het onderhavige beleidsdocument informatiebeveiliging structureel naar een hoger niveau te gaan brengen en daarop te houden door de aspecten governance, wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid -ook in hun onderlinge relatie- duidelijk te beschrijven en vast te stellen.

Doelstellingen 2022 IB/AVG




- DMG draagt in 2022 en 2023 zorg voor dat men in control is over informatiebeveiligingsrisico's dankzij de implementatie van een set van maatregelen, processen en procedures die de beschikbaarheid, integriteit en vertrouwelijkheid van

informatie verhogen door het volgen van Qarebase en het volgen van de kwaliteit (jaar) planning.
- Het verder aan laten sluiten van zowel het technische (IT) deel als organisationele onderdelen (zoals gedrag van medewerkers, beleid, de interne organisatie en procedures en richtlijnen). Dit zal in 2022-2023 middels overleggen, awareness, Qarebase verder gestalte krijgen.
- Het steeds alert blijven en continu anticiperen en verbeteren is het uitgangspunt om goed te kunnen acteren op steeds veranderende dreigingen. Dit krijgt gestalte door het steeds in werkoverleggen IB/AVG als agendapunt op te nemen en het gebruik maken van de meldingen systematiek in Qarebase.

**Reikwijdte en opbouw van het beleid**

De focus van het informatiebeveiligingsbeleid binnen onze organisatie ligt deels op algemene, persoons- en op de cliënt-patiënt gegevens. Dit laatste is gebaseerd op de ambulancetak binnen DMG. Daarnaast heeft het informatiebeveiligingsbeleid betrekking op de personeels-, contract-, financiële, kwaliteitsgegevens, informatie (gegevens) gebruikt door medewerkers, stagiaires, externe relaties (leveranciers en stakeholders), op alle organisatieonderdelen. De gegevensdragers zijn binnen scope(s).

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van onze organisatie. Dit heeft zowel betrekking op gecontroleerde informatie, die door onze organisatie zelf is gegenereerd en wordt beheerd, als ook op niet-gecontroleerde informatie.

Het beleid wordt in belangrijke mate beïnvloed door de gemeenschappelijke betrouwbaarheidseisen van kritische componenten (processen en systemen) van onze organisatie. Zie voor meer details: ***de Contextanalyse*.**

Belangrijk onderdeel van het beleid is het waarborgen van de continuïteit van de bedrijfsprocessen die een afhankelijkheid hebben van onze software en hardware.

Het informatiebeveiligingsbeleid wordt vertaald naar concrete acties en is opgenomen in het kwaliteitshandboek ISMS DMG. (Informatie Security Management System)  Het beleid komt tot stand en wordt beoordeeld middels periodieke externe- en interne audits waarbij het beleid getoetst wordt aan de norm ISO 27001 en NEN 7510-2017.

**Doelstelling informatiebeveiligingsbeleid**

Het informatiebeveiligingsbeleid van onze organisatie heeft als doel het beschermen van bovenstaande informatie. Door het uitbrengen van het informatiebeveiligingsbeleid geeft de directie uitdrukking aan het belang dat zij hecht aan informatiebeveiliging en demonstreert zij dat zij dit beleid van harte ondersteunt.

Hierbij wordt onderscheid gemaakt naar kritische en minder kritische informatie, afhankelijk van de aard van de informatie, waarbij hogere of lagere eisen aan de betrouwbaar (beschikbaarheid, integriteit en vertrouwelijkheid) gesteld worden. Deze classificatie is terug te lezen in een separaat document. Zie autorisatiematrix.

Tevens heeft het informatiebeveiligingsbeleid als doel het waarborgen van de continuïteit van de kritische bedrijfsprocessen die afhankelijk zijn van software en hardware.

**Beleidsuitgangspunten en principes**

Wij gaan uit van de ISO 27001 en NEN 7510 norm bij ons informatiebeveiligingsbeleid. De NEN 7510 is gericht op de Ambulance Tak. De overige labels gaan mee in de ISO 27001 certificering.

De beleidsuitgangspunten en principes m.b.t. informatiebeveiliging binnen onze organisatie zijn:

- Het uit te dragen informatiebeveiligingsbeleid is vastgelegd in dit document waarbij het ISMS de uitwerking in concrete maatregelen is.
- De in het ISMS beschreven concrete maatregelen geven de ambitie van DMG weer.
- Alleen die Cliënt- Patientgegevens worden vastgelegd die nodig zijn voor de relevantie processen zoals uitgevoerd onder de scope[1] (conform wet- en regelgeving, zie voor meer detail de contextanalyse) en dit betreft Broeder de Vries Dutch Medical Services B.V.
- Er worden geen cliënt-patientgegevens doorgegeven aan derden zonder toestemming van de belanghebbende(n)
- Alleen geanonimiseerde of gepseudonimiseerde cliënt-patiëntgegevens worden eventueel gebruikt voor onderzoek naar de effectiviteit en efficiency van de behandelingen en interventies.
- Het beleid moet toetsbaar zijn aan de ISO 27001 en NEN 7510 norm, waarbinnen het gaat om richtlijnen die specifiek voor onze organisatie toepasbaar zijn. Op sommige punten kan (gemotiveerd) worden afgeweken van de voorgestelde maatregelen en/of zijn er wellicht aanvullende maatregelen nodig.
- Bewustzijn: Informatiebeveiliging is ieders verantwoordelijkheid: Iedereen die met informatie van onze organisatie werkt, zowel medewerkers, stagiaires als externe relaties, dienen zich bewust te zijn van de informatiebeveiligingsuitgangspunten van onze organisatie.
- Verplichting: Alle medewerkers (en leveranciers van diensten) van DMG conformeren zich aan het Informatiebeveiligingsbeleid via ondertekening van gedragscodes en overeenkomsten waarbinnen de directie de verplichting heeft de medewerkers(derden)het beleid kenbaar te maken via interne nieuwsbrieven, werkoverleggen, evaluatiemomenten en trainingen.
- De informatiebeveiliging dient te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de algemene verordening gegevensbescherming(AVG); de Wet Bescherming Persoonsgegevens en de Wet Geneeskundige Behandel Overeenkomst (WGBO).

De informatiebeveiliging dient de volgende betrouwbaarheidsaspecten te waarborgen:

**Beschikbaarheid, Integriteit en Vertrouwelijkheid.**

1. Informatiebeveiliging is een lijnverantwoordelijkheid: dat betekent dat de managers en regioverantwoordelijken de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging binnen hun team. Dit omvat ook de keuze van maatregelen en

[1] **Meditaxi**
Het verzorgen van huisartsenvervoer en assisterende taken tijdens visite t.b.v. huisartsenposten in Nederland
**Dutch Medical College**
Het ontwikkelen en verzorgen van opleidingen voor huisartsenchauffeurs, huisartsen, doktersassistenten, praktijkondersteuners, verpleegkundigen, verzorgenden IG en overige hulpverleners
**Broeder de Vries Dutch Medical Services B.V.**
Het verzorgen van internationale repatriëringen, het internationale ambulancevervoer, waaronder ver-voer van en naar de Nederlandse luchthavens alsmede het verzorgen van B-vervoer voor RAV's, evenementenzorg en een bereikbaarheidsdienst voor derden.
**Dutch Medical College;** Het ontwikkelen en verzorgen van de opleidingen voor huisartsenchauffeurs, huisartsen, doktersassistentes, praktijkondersteuners, verpleegkundigen, verzorgenden IG en overige hulpverleners..
**Broeder De Vries Dutch Medical Services B.V**.; Het verzorgen van internationale repatriëringen, het internationale ambulancevervoer, waaronder vervoer van en naar de Nederlandse luchthavens alsmede het verzorgen van B-vervoer voor RAV's.

de uitvoering en handhaving ervan, waarbinnen actieve bevordering van het beveiligingsbewustzijn een belangrijk onderdeel is van ons informatiebeveiligings-beleid.

2. Informatiebeveiliging is een continue proces. Periodiek , o.a. door het op de agenda van het MT middels IFMS, wordt het beleid herzien en getoetst aan de hand van interne en externe audits: technologische en organisatorische ontwikkelingen binnen en buiten de organisatie maken het noodzakelijk het informatiebeveiligingsbeleid periodiek te bezien. De frequentie van de beoordeling is gerelateerd aan de planning en control cyclus van DMG. De naleving van genomen maatregelen wordt periodiek getoetst.
3. Bij alle vernieuwingen, zoals herziening van de infrastructuur wordt structureel rekening gehouden met informatiebeveiliging. Er zal voorafgaand aan de vernieuwing een risico-inventarisatie /DPIA opgesteld worden.
4. Het beleid wordt eens per 2Vjaar herzien en indien nodig tussentijds aangepast. Het informatiebeveiligingsbeleid doorloopt de zogenaamde Deming Cyclus die de fases Plan, Do, Check Act bevat. De uit te voeren werkzaamheden zijn als volgt te plaatsen in de cyclus:

**Plan** (initiële risico analyse. Informatiebeveiligingsbeleid waarna een informatiebeveiligingsplan wordt opgesteld waarbij hiaten tussen 1 en 2 worden beheerst).

**Do:** Invoeren en uitvoeren van de maatregelen waarbinnen de volgende items binnen dit jaar onze focus hebben:

**Check:** Controle en evaluatie van maatregelen aan de hand van interne of externe audits. Uitvoeren van risicoanalyse om verbetering aan te tonen

**Act:** Bijstellen informatiebeveiligingsplan of beleid aan de hand van de 'return on investment' (rendement van de investering).

Bovenstaande stappen worden cyclisch uitgevoerd op basis van de uitkomst van controles en evaluaties, of door nieuwe ontwikkelingen die het noodzakelijk maken het informatiebeveiligingsbeleid te wijzigen waarbij constant aandacht is voor het bewustwordingsproces : Inzichtelijk maken van de maatregelen/ Gerichte acties die gericht zijn op het vergroten van het bewustzijn.

**Organisatie informatiebeveiliging en toewijzing van verantwoordelijkheden**

**Doel:** Het beheren van de Informatiebeveiliging waarbij de continuïteit van informatiebeveiliging wordt geborgd in de organisatie en de processen.

**Werkwijze:** Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken worden in onze organisatie een aantal rollen onderkend die aan functionarissen zijn toegewezen.

***Directie***

De directie is eindverantwoordelijk voor de informatiebeveiliging binnen onze organisatie en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast en stelt de middelen beschikbaar. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de hoofddirectie en de DGA.

De directie is tevens verantwoordelijk voor het sluiten van overeenkomsten met externe partijen.

***Functionaris voor de gegevensbescherming (FG)***

De FG houdt controle op de naleving van de AVG. Deze functie is uitbesteed aan een externe onafhankelijke adviseur van Qarebase Company.

***CISO-Compiance Adviseur CA (i.a.)***

De CA is verantwoordelijk voor het uitdragen van het informatiebeveiligingsbeleid binnen onze organisatie. Hij is tevens inhoudelijk verantwoordelijk voor de informatiebeveiliging binnen onze organisatie. Dit moet nog worden belegd. Het voornemen is dit onder ICT te beleggen.

De CA zorgt voor borging van het informatiebeveiligingsbeleid in de kwaliteitsdocumenten en procedures.

De CA  is verantwoordelijk voor het volgens de richtlijnen afhandelen van incidenten en klachten.

Deze functionaris heeft een onafhankelijke positie in de organisatie.

***Functioneel systeembeheerder***

De Functioneel Systeembeheer vervult een rol bij de vertaling van het informatiebeveiligingsbeleid naar operationele inrichting en gebruik van ICT-systemen. Deze rol is uitbesteed aan een gekwalificeerd bedrijf MEOS genaamd.

***Proces eigenaar***

Een proces eigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, zoals Facilitair, HRM en Finance. Binnen DMG is dit belegd bij het Shared Service Center.  Informatiebeveiligingsbeleid is hierbij een belangrijk aspect.

***Leidinggevende***

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

· er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;

· toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers;

· periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;

· als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevenden kunnen hierin ondersteund worden door de Functioneel Systeembeheerder.

**Documenten informatiebeveiliging**

Het informatiebeveiligingsbeleid is onderdeel van het kwaliteitsbeleid van DMG en verweven in de documenten (formulieren en instructies) van het kwaliteitshandboek.

Voor informatiebeveiliging wordt bij onze organisatie dezelfde managementcyclus gevolgd, die ook voor andere onderwerpen geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie zoals beschreven in onze kwaliteitshandboeken.

De documenten van zowel het handboek Kwaliteit als handboek ISMS is gedocumenteerd in het documentbeheersysteem van Qarebase.

Naast het kwaliteitshandboek kent het beleid in het kader van informatiebeveiliging de volgende documenten:

**Het informatiebeveiligingsbeleid**

Het informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de instelling. In het informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om ervoor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie ernaar handelt wordt het uitgedragen door de een vertegenwoordiger van de directie. Het informatiebeveiligingsbeleid wordt opgesteld door de directie en het MT van DMG.

**Directiebeoordeling en jaarplan**

Elk jaar, stelt de directie in samenwerking met de leden in het MT een directiebeoordeling en een jaarplan op. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles/audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen (IB) maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus.

**3. Risicoscan**

Bij de risicoanalyse wordt uitgegaan van de processen binnen de organisatie en de risico's op informatiebeveiliging die daar gelopen worden. Deze risico's worden vervolgens geclassificeerd naar impact en kans dat het risico voorkomt. Dit vindt plaats middels de Bow Tie  methode. Dit betreft ook calamiteiten risico's waarbij het BCP ook onderdeel van vormt.

Vervolgens wordt van de risico's met de hoogste classificering de oorzaak beschreven (mensen/methode/middelen) en de te nemen (SMART) maatregelen.

**Richtlijnen, toezicht en naleving**

Wettelijke richtlijnen, gedragscodes en richtlijnen voor medewerkers, en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging.

**De ISO 27001 en NEN 7510 normen en relevantie aanverwante gegevens.**

De Nen-normen worden gewaarborgd in procedures in het ISMS en in het kwaliteitshandboek[2]. Zie Qarebase.

[2] In Qarebase staat een KMS en ISMS waarbij een aantal elementen geïntegreerd zijn.