INFORMATIE BEVEILIGINGSBELEID

Inhoud

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:

1. Beschikbaarheid: de mate waarin gegevens of functionaliteiten op de juiste momenten beschikbaar zijn voor gebruikers;
1. Integriteit: de mate waarin gegevens of functionaliteit juist ingevuld zijn;
2. 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.

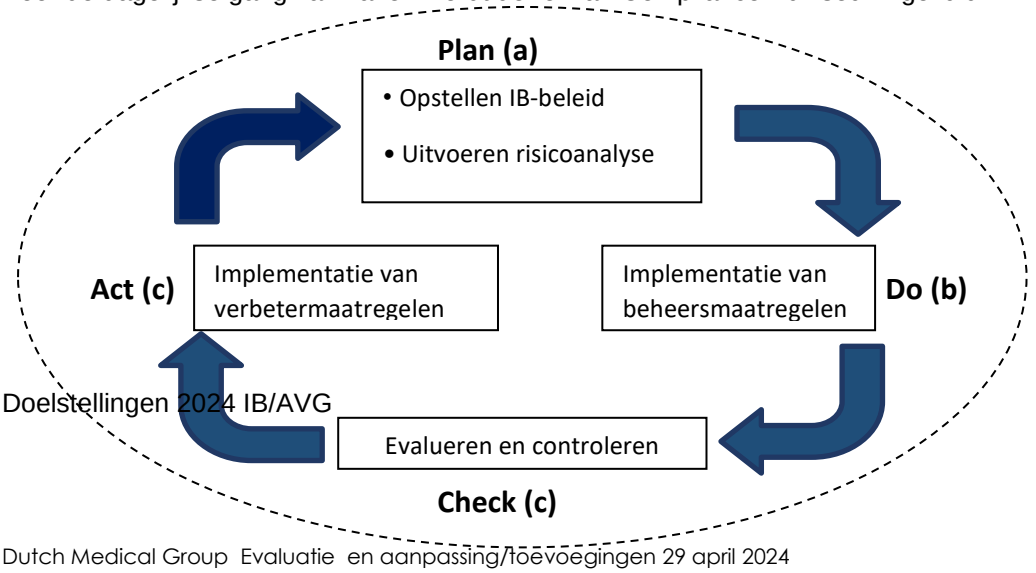
DMG heeft als ambitie om met het onderhavige beleidsdocument informatiebeveiliging structureel naar een hoger niveau te gaan brengen en daarop te houden door de aspecten governance, wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid -ook in hun onderlinge relatie- duidelijk te beschrijven en vast te stellen. Dutch Medical Group stelt dat alle medewerkers een rol hebben binnen de informatiebeveiliging. Alle gebruikers van informatiesystemen, applicaties en netwerken worden geacht het informatiebeveiligingsbeleid na te leven en zich bewust te zijn van relevante beveiligingsaspecten.

1.1 Taken, Verantwoordelijkheden en Bevoegdheden (TVB)

Binnen de organisatie is een MT-lid als portefeuillehouder informatiebeveiliging aangewezen. Dat betreft de manager bedrijfsvoering.
Hier liggen de belangrijkste verantwoordelijkheden ten aanzien van de implementatie en beschikbaarheid van het managementsysteem:

- Directievertegenwoordiger
- Beschikbaarheid van middelen
- Beoordelen van het managementsysteem op voortdurende geschiktheid
- Opzetten, beschrijven, implementeren en onderhouden van het systeem
- Voldoen van managementsysteem aan ISO 27001 en NEN 7510

Voor de dagelijkse gang van zaken wordt de rol van Compliance Adviseur ingevuld.



Doelstellingen 2024 IB/AVG

Doelstelling informatiebeveiligingsbeleid

In het jaar 2022 was het eerste jaar dat het information security managementsysteem, hierna het “ISMS”, door de organisatie gehanteerd wordt, Er zijn inmiddels interne audits uitgevoerd , directiebeoordelingen, directieverklaring en risicomanagement toegepast. Ook de externe audit heeft in 2023 plaatsgevonden door een Certiicerende instelling.

Alhoewel het behalen van het ISO 27001 en NEN 7510 certificaat niet als informatiebeveiligingsdoelstellingen gehanteerd mag worden, is duidelijk dat dit wel degelijk een doelstelling voor DMG is gebaseerd op het borgen en beheersen van de bedrijfsvoering.

- DMG te beschermen tegen aansprakelijkheid of schade door misbruik of uitval van haar systemen die door klanten worden gebruikt.

DMG zet hier de volgende KPI op.

1. Jaarlijks geen enkel beveiligingsincident waarvoor DMG aansprakelijk kan worden gehouden door haar klanten.

- Het creëren van bewustwording tot de naleving van alle huidige en relevante interne procedures en richtlijnen. Het onderliggende doel is om te zorgen dat alle medewerkers (in en extern) hun eigen verantwoordelijkheden begrijpen met betrekking tot de vertrouwelijkheid en integriteit van de gegevens die zij behandelen binnen hun werkzaamheden voor DMG.

DMG zet hier de volgende KPI op.

1. Jaarlijks nul datalekken waarbij gegevens van klanten betrokken zijn.

- Het zorgen voor een systematische vastlegging van incidenten, de analyse hiervan en de preventieve maatregelen die worden genomen die leiden tot een betere veiligheid van de systemen die binnen DMG worden gebruikt. DMG zet hier de volgende KPI op.

De overkoepelende doestellingen voor 2024 zijn als volgt geformuleerd:

1. Behouden van de certificeringen waarbij de bedrijfsvoering geborgd en beheerst blijft
2. Het optimaliseren van informatiebeveiligingsbewustzijn bij medewerkers, management en inhuurkrachten binnen de organisatie.
3. Het implementeren/optimaliseren van de beheersmaatregelen, conform prioritering in de IB-actielijst (zie Qarebase)
4. Het inrichten van een managementsysteem waarin het beleid en daaruit voortvloeiende beheersmaatregelen traceerbaar zijn geborgd.

Specifieker:
Doelen management:

1. Conformeren aan de doelstellingen van NEN7510:2017 en NEN7512 en NEN7513 en blijven inbedden in de organisatie.
2. Beleid voor informatiebeveiliging uitdragen en de uitvoering bewaken
3. Het optimaliseren van informatiebeveiligingsbewustzijn bij medewerkers, management en inhuurkrachten binnen de organisatie
4. Het positioneren van de functionaris gegevensbescherming (FG) volgens de TVB-inrichting met betrekking tot Informatiebeveiliging en de bescherming van persoonsgegevens.
5. De implementatie en het optimaliseren van de beheersmaatregelen, conform prioritering in de IB-actielijst (zie Qarebase)
6. Het ‘in control’ zijn op geïmplementeerde informatiebeveiligingsmaatregelen verankerd in het controleprogramma.

Doelen ICT

1. Het implementeren/optimaliseren van de beheersmaatregelen, conform prioritering in de IB-actielijst (zie Qarebase)
2. In control zijn op de bestaande en nog te implementeren beheersmaatregelen, in het bijzonder:
    a. Het inrichten van periodieke controle op uitgegeven toegangsrechten

b. Borgen dat bij de implementatie van het project ‘de nieuwe werkplek’ alle mobiele apparatuur is voorzien van encryptie.
c. Inrichten van monitoring van alle laptops in het netwerk bij hernieuwen licentie voor netwerk monitoring.

Doelen HR

1. Het implementeren/optimaliseren van de beheersmaatregelen die van toepassing zijn op HR-processen, conform prioritering, in de IB-actielijst (zie Qarebase)
2. In control zijn op de bestaande en nog te implementeren beheersmaatregelen, in het bijzonder:
    a. Screening (verificatie van de achtergrond van alle medewerkers en kandidaten voor een dienstverband en ingehuurd personeel).

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 in Qarebase*.*

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 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. Dit geldt ook voor de aangesloten locatie Halsteren.

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. Dit geldt ook voor de locatie Halsteren.

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. en locatie Halsteren
- 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). Zie verder hete overzicht Wet- en Regelgeving.

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 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.

[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.
BAS Ambulancezorg Nationaal en internationaal gedifferentieerd vervoer

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 jaar 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.

Compiance Adviseur

De CA is verantwoordelijk voor het uitdragen van het informatiebeveiligingsbeleid binnen onze organisatie. Zijj is tevens inhoudelijk verantwoordelijk voor de informatiebeveiliging binnen onze organisatie.

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/teamleiders/managers

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 managementsysteem (ISMS)

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 betreffende ISMS zijn gedocumenteerd in het documentbeheersysteem van Qarebase.

Naast de documenten in Qarebase 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. Zie risicomanagement Qarebase.

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 de managementsystemen [2]. Zie Qarebase.

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

Beheer van bedrijfsmiddelen

De bedrijfsmiddelen zoals hardware, software en media zijn belangrijk voor de uitvoering van de bedrijfsprocessen binnen de organisatie. De bedrijfsmiddelen worden geadministreerd door de afdeling ICT, periodiek wordt de actualiteit hiervan gecontroleerd.

Bij uitgifte van hardware tekent de medewerker een gebruikersovereenkomst waarin de voorschriften voor gebruik zijn opgenomen.

Beheer en onderhoud van middelen

Aangeschafte hardware wordt afgeschreven volgens economische levensduur per apparaat. Bedrijfsmiddelen die niet meer worden gebruikt dan wel worden ingenomen worden op een passende wijze geschoond.
Indien van toepassing kunnen bedrijfsmiddelen opnieuw worden uitgegeven. Indien bedrijfsmiddelen worden verwijderd, wordt alle informatie van deze middelen verwijderd. Afdeling ICT is verantwoordelijk en draagt zorg voor de fysieke vernietiging van hardware/ informatiedragers.

Classificatie van informatie

Informatie heeft waarde voor de organisatie. De waarde is een van de belangrijkste assets voor de organisatie.

1.2 Relevantie Classificatie

Classificatie is relevant om de volgende redenen:

1. Het vormt de basis voor de **Risicobeoordeling**. Classificatie is nodig om de waarde van informatie c.q. systemen te kunnen vaststellen.
2. Het vormt input bij de inrichting van de **Toegangsbeveiliging en autorisaties van systemen**.
3. De classificatie vormt input voor het **Continuïteitsplan**. Voor informatie c.q. systemen met een als hoog geclassificeerde beschikbaarheid, moeten continuïteitsmaatregelen worden overwogen.
4. Het vormt de basis voor specifieke **Behandelwijzen** van vastgestelde soorten informatie. Indien noodzakelijk, wordt voor bepaalde informatie (met name de zeer vertrouwelijke) **Labeling** ingericht**.**

1.3 Classificatie voor risicobeoordeling

Informatie wordt altijd geclassificeerd voor drie categorieën: beschikbaarheid, integriteit en vertrouwelijkheid. Per categorie wordt een impact vastgesteld. De classificatie heeft plaatsgevonden en is vastgelegd in de **Business Impact Analyse** (onderdeel van de Risicobeoordeling).

Toelichting BIV:

Beschikbaarheid (B)	*Informatie mag niet verloren gaan of onbereikbaar zijn*
Integriteit (I)	*Informatie mag alleen door daartoe geautoriseerde personen worden bewerkt en mag niet onbetrouwbaar zijn*
Vertrouwelijkheid (V)	*Informatie mag alleen door daartoe bevoegde personen worden ingezien*

ZIE: RISICOMANAGEMENT

Input voor toegangsbeveiliging systemen

De score geeft het belang van de informatie aan. Hiermee kan het vereiste niveau van toegangsbeveiliging worden bepaald. Hoe hoger de score, hoe strikter de logische toegangsbeveiliging wordt ingeregeld.
ZIE : LOGISCHE TOEGANGSBEVEILIGING

Input voor continuïteitsplan

Informatie wordt altijd geclassificeerd voor drie categorieën: beschikbaarheid, integriteit en vertrouwelijkheid. Per categorie wordt een impact vastgesteld. Voor informatie c.q. systemen met een als hoog geclassificeerde beschikbaarheid, moeten continuïteitsmaatregelen worden overwogen.
ZIE: CONTINUÏTEITSPLANNING

Verantwoordelijkheden classificatie

6.5.1 Rol eigenaar van informatie

Binnen Dutch Medical Group is de eigenaar van informatie verantwoordelijk voor het toekennen van de classificatie. De eigenaar kan degene zijn die een document heeft opgesteld of onder wiens verantwoordelijkheid het is opgesteld. Het kan echter ook gaan om de eindverantwoordelijke voor de inhoud van een database of de beheerder van klantinformatie.
Wanneer de informatie is geclassificeerd dient de eigenaar van de informatie te zorgen voor passende bescherming van de informatie.

6.5.2 Rol gebruiker van informatie

Bij het delen van informatie is het belangrijk dat gebruikers weten welke voorschriften daarbij gelden, gerelateerd aan het niveau van vertrouwelijkheid
Bij de classificatie van informatie zijn voor de mate van vertrouwelijkheid 4
niveaus bepaald conform de beschreven werkwijze in ‘Risicoanalyse en Beoordeling’.
Hieronder wordt uitgelegd wat deze vertrouwelijkheidsniveaus inhouden:

- **Zeer Vertrouwelijk (impact: Hoog)**
  Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.
- **Vertrouwelijk (impact: Middel)**
  Deze classificatie verwijst naar gevoelige informatie, die bij uitlekken substantiële schade kan toebrengen aan de reputatie van het bedrijf en negatief beoordeeld zal worden door de publieke opinie. Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- **Intern (impact: Laag)**
  Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s) en/of die in het belang van Dutch Medical Group moet worden verstrekt aan derden. Vertrouwelijkheid is gering, maar de informatie mag niet worden gecommuniceerd naar of in handen vallen van onbevoegde derden. Schending van deze classificatie kan enige (in)directe schade toebrengen.
- **Openbaar (impact: Geen)**
  Informatie die op de website staat vermeld of op een andere manier vrij toegankelijk is voor iedereen.

De gebruikers van informatie worden geacht zich te houden aan de voorschriften voor omgaan met de 2 hoogste niveaus van vertrouwelijkheid. De “Autorisatiematrix” geeft een gedetailleerd overzicht van de classificatie en de toegang tot bepaalde informatiebronnen. In dit overzicht staan voor elk classificatieniveau voorschriften (behandelwijzen) voor het opslaan, verwerken en verspreiden van informatie. Zo kan worden voorkomen dat informatie verloren gaat, ten onrechte wordt gewijzigd of bij de verkeerde personen terecht komt.

Labeling

Dutch Medical Group maakt gebruik van fysieke labeling van informatie, in het bijzonder labeling van patiëntinformatie op elektronische ritformulieren en kopieën daarvan.

Nog steeds bepaalt de plaats waar de informatie wordt opgeslagen in combinatie met de toegangsautorisaties de labeling, echter met de aanvulling dat: Fysieke output met gezondheidsgegevens wordt voorzien van het label ‘Vertrouwelijk’.

Systeembeheer

Verantwoordelijkheden

Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
Uitsluitend bevoegd personeel mag beheertaken uitvoeren.
Bij externe hosting van data en/of services (uitbesteding aan hosting partij/datacenter, Cloud computing) blijft de organisatie eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.

Schadelijke software

De organisatie zal een actief beleid voeren om schade door computervirussen, Trojaanse paarden en ongeautoriseerde mobile code (software die zichzelf automatisch installeert) tot een minimum te beperken. De organisatie zal daartoe het juiste gebruik van protectiemiddelen ondersteunen. Er moeten bijzondere beheersmaatregelen getroffen worden om deze ongewenste software te ontdekken, te verwijderen en ‘mobile code’ te beheersen.

Technische aspecten

Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimumniveau (servicelevels) komt.
De belangrijkste aspecten betreffen capaciteitsmanagement en logging. Monitoring is op diverse niveaus ingericht. De monitoring in dit document heeft betrekking op het monitoren van de gezondheid van systemen. (‘system health checks’).

Bedieningsprocedures

De belangrijkste bedieningsprocedures zijn:

- Bedieningsvoorschriften ten aanzien van de installatie en configuratie van systemen
- De verwerking en behandeling van informatie
- Back-up proces
- Het melden van en het afhandelen van incidenten
- Het opstarten en herstellen van systemen in geval van storingen

Back-up beleid

Om de continuïteit van de processen verder te garanderen wordt er een actief back-up beleid met een bijbehorende back-upstrategie gevolgd. Er worden reguliere back-ups van de gegevens gemaakt zodanig dat de schade bij een mogelijke uitval beperkt blijft. De eisen aan mogelijke minimale uitval zullen worden bepaald door de uitvoering van risicoanalyses, maar wordt opgelegd vanuit wettelijke eisen en overeenkomsten.
Regelmatig zal geoefend worden met het herstel van de gegevens. Aan het bewaren en de opslag van de back-up media worden uiteraard specifieke eisen gesteld. De media dienen onder geconditioneerde omstandigheden te worden opgeslagen, waarbij de opslag niet aan dezelfde gevaren mag blootstaan als de oorspronkelijke locatie. Tevens is de locatie waar de back-up media zijn opgeslagen slechts toegankelijk voor geautoriseerde medewerkers.

Netwerkkoppelingen

De organisatie maakt gebruik van netwerkkoppelingen en netwerken van en met derden. Ten aanzien van het beheer en de beveiliging hiervan worden door deze partijen extra aanvullende beveiliging eisen gesteld en worden maatregelen getroffen om de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gegevens te garanderen. De organisatie is zich bewust van haar verantwoordelijkheid en zal de vereiste beheersmaatregelen treffen.

Indien er een uitwisseling van informatie tussen organisaties, zoals andere organisaties of overheidsinstanties plaatsvindt, zal dit worden uitgevoerd op basis van een formeel uitwisselingsbeleid, in overeenstemming met relevante wet- en regelgeving.

Loggegevens

Om adequaat te kunnen reageren op incidenten en beveiligingsgebeurtenissen zullen, in overeenstemming met de wet- en regelgeving, de activiteiten van gebruikers worden vastgelegd De loggegevens zullen worden opgeslagen en alleen worden ingezien door de geautoriseerde medewerkers. De gegevens zullen periodiek worden gecontroleerd en gerapporteerd aan het management. Tevens wordt er gebruik gemaakt van logbestanden van operators en storingsregistraties om te waarborgen dat de problemen met de informatiesystemen worden vastgesteld.

Wijzigingsbeheer

De organisatie is zich er van bewust dat wijzigingen in IT-voorzieningen en informatiesystemen op een beheerste en gecontroleerde wijze plaats moeten vinden. De verantwoordelijkheden voor het goedkeuren en doorvoeren voor de wijzigingen zijn vastgelegd om afdoende beheersing van alle wijzigingen aan apparatuur, programmatuur of procedures te waarborgen. Wijzigingen in IT-voorzieningen en informatiesystemen zullen beoordeeld worden op het potentiële effect op de beveiliging voordat de wijziging wordt doorgevoerd. De wijzigingen worden gedocumenteerd met alle relevante informatiebeleid cryptografie (versleuteling van gegevens en verbindingen)
Indien de organisatie gebruik maakt van cryptografie zal er een beleid voor het gebruik van crypto grafische beveiliging worden ontwikkeld. Dit beleid zal aangeven hoe de organisatie omgaat met de opslag van vertrouwelijke gegevens en de verbindingen welke worden gebruik om deze gegevens te verzenden. Er behoort een sleutelbeheerprogramma te zijn om het gebruik van crypto grafische technieken te ondersteunen. Het beleid zal aansluiten bij de geldende wet en regelgeving en eisen van derden. Dit houdt in dat de organisatie aandacht heeft voor mogelijk gebruik en zal daar adequaat op reageren.

Cryptografie en sleutelbeheer

Beleid

Alle informatietransporten van persoonsgegevens of andere vertrouwelijke gegevens buiten het eigen netwerk zijn beveiligd met een vorm van encryptie.
Data op mobiele datadragers (laptop, tablets, USB-sticks) zijn beschermd bij verlies of diefstal.
De gebruikte encryptiemethodes zijn conform de huidige industriestandaarden.

Realisatie

Het beleid is op de volgende wijze geïmplementeerd:

- Tussen de verschillende locaties (netwerken) zijn site-to-site VPN-verbindingen opgezet.
- Voor verbindingen met operationele systemen via een openbaar netwerk is two-factor-authenticatie vereist.
- Voor portalen die via openbare netwerken toegankelijk zijn, wordt gebruik gemaakt van beveiligde verbindingen met SSL/TLS-certificaten (De geldigheidsduur van certificaten wordt gemonitord door systeembeheer of de SAAS-leverancier).
- Applicaties die gebruik maken van lokale opslag van persoonsgegevens op mobiele devices maken gebruik van encryptie.
- Vertrouwelijke gegevens (waaronder persoonsgegevens) worden, indien verzonden via e-mail, altijd versleuteld.

Beheer

ICT is verantwoordelijk voor het monitoren van de geldigheid van cryptografische sleutels. Bitlockersleutels van mobiele devices worden vastgelegd. De beheerwachtwoorden zijn opgeslagen en voorzien van encryptie.

Distributie

ICT beheert sleutels en kan deze op verzoek beschikbaar stellen.

Vernietiging

ICT beheert sleutels en kan deze op verzoek vernietigen.

Verantwoordelijkheden

Directie:
Jaarlijks wordt geëvalueerd of de gemaakte afspraken en regels worden gehanteerd, om informatiebeveiliging te kunnen realiseren.
Systeembeheer:
In de Gedragscode Informatiebeveiliging staan regels met betrekking tot het gebruik van ICT-middelen beschreven. Deze gedragscode is van toepassing op alle medewerkers.

Logische toegangsbeveiliging

Toegang tot systemen en netwerken

Binnen de organisatie wordt gebruik gemaakt van digitale en niet digitale informatie. De organisatie is zich er van bewust dat al deze informatie beveiligd moet worden tegen ongeautoriseerde kennisname, en wijzigingen. De toegang wordt afgeschermd en is slechts toegankelijk op basis van de rol die een medewerker heeft (“need to know”, “need to do”). Er zijn formele procedures aanwezig voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen en -diensten.

Gebruikersaccount

Een toegang is persoonlijk en gebonden aan een medewerker. Een nieuwe medewerker zal slechts mogen werken als deze zijn persoonlijke inloggegevens (gebruikersaccount en wachtwoord) heeft

ontvangen. De organisatie zal beveiligingsvoorzieningen treffen om toegang tot en binnen de toepassingssystemen te beperken. De logische toegang tot toepassingsprogrammatuur en informatie wordt beperkt tot bevoegde gebruikers.

Toegang tot bedrijfsapplicaties

- Dutch Medical Group verleent toegang tot haar interne systemen op basis van het need-to-know principe, dat wil zeggen dat gebruikers toegang krijgen tot systemen die nodig zijn om hun rollen en verantwoordelijkheden te vervullen.
- Waar nodig en technisch mogelijk is 2FA ingericht.
- Het verlenen van toegang is gebaseerd op een formeel proces, dat wil zeggen dat verzoeken via e-mail worden aangevraagd bij ICT door HRM of door teamleider in geval van aanpassing/uitbreiding van taken/rol.
- Toegang tot netwerkmappen wordt op verzoek van de eigenaar van de map toegekend.
- Toegangsrechten worden opgeheven of verwijderd indien er geen legitieme reden meer is om toegang te krijgen tot een systeem.

Verantwoordelijkheid

Een doeltreffende beveiliging is afhankelijk van de medewerking van geautoriseerde gebruikers. Zij moeten hun verantwoordelijkheid voor het handhaven van doeltreffende toegangsbeveiliging nemen, vooral met betrekking tot het gebruik van wachtwoorden en de beveiliging van gebruikersapparatuur. Hiertoe zullen zij dan regelmatig bewust worden gemaakt van deze verantwoordelijkheden en bijbehorende plichten.

Privilegerechten

- Toegang tot beheeraccounts hebben de systeembeheerders. De bijbehorende wachtwoorden zijn opgeslagen in een separate wachtwoordkluis.
- Voor deze accounts wordt zo veel mogelijk een gepersonaliseerd account aangemaakt. Het gebruik van generieke accountnamen, zoals bijvoorbeeld administrator, is verboden tenzij het een onwijzigbaar rootaccount betreft.

Toezicht op autorisaties

- Rechten worden toegekend aan medewerkers op basis van rollen of rechtengroepen
- Rollen die worden aangevraagd buiten de bestaande inrichting, worden goedgekeurd door IBMF groep, in overleg met de eigenaar van de gegevens.
- Periodiek wordt een controle op de uitgegeven toegangsrechten uitgevoerd.

Systeemontwikkeling en onderhoud

Dutch Medical Group ontwikkelt zelf geen informatiesystemen maar maakt indien deze zijn gewenst gebruik van externe partijen. Bij de ontwikkeling van systemen zal de organisatie van de partij eisen dat de beveiligingseisen in het te ontwikkelen systeem worden meegenomen. Ontwerp en implementatie van het informatiesysteem dat het bedrijfsproces ondersteund kunnen van doorslaggevend belang zijn voor de beveiliging. Beveiligingseisen behoren voorafgaand aan de ontwikkeling en/of implementatie van informatiesystemen te worden vastgesteld en overeengekomen. Alle beveiligingseisen behoren te worden vastgesteld tijdens de specificatie van de eisen voor het project en behoren te worden verantwoord, overeengekomen en gedocumenteerd als onderdeel van de totale aanschaf van het informatiesysteem.
Voor systemen waarop gevoelige, waardevolle of kritische informatie wordt verwerkt, of die invloed hebben op deze informatie, kunnen aanvullende beheersmaatregelen vereist zijn. Dergelijke beheersmaatregelen behoren te worden opgesteld op basis van de interne en externe beveiligingseisen en een risicobeoordeling.

4.1 Testgegevens

De organisatie verbiedt het gebruik van productiedata en -databases in testomgevingen. De productiedata zal uitsluitend binnen de organisatie op productiesystemen worden gebruikt. Daar waar productiedata (noodzakelijkerwijs) wel gebruikt wordt, wordt deze data geanonimiseerd.

Incident Management

5.1 Doel

Het nemen van corrigerende maatregelen naar aanleiding van afwijkingen in processen en systemen. Het treffen van verbeterende maatregelen naar aanleiding van verbetervoorstellen valt tevens onder deze procedure.

5.2 Afwijkingen

Vanuit interne of externe audits, klachten van klanten of verstoringen van de processen, kunnen zich afwijkingen manifesteren die erop kunnen duiden dat niet wordt voldaan aan de eisen zoals die gesteld worden door het (handboek Qarebase voor) Management Systeem voor Informatiebeveiliging e/o de norm eis(en).
Onder een klacht wordt verstaan:

- Een uitdrukking van ontevredenheid gericht aan het bedrijf over geleverde producten en diensten, waarbij een klant of leverancier een respons of oplossing verwacht.

Onder afwijkingen worden verstaan:

- Klachten van klanten
- Klachten van/over leveranciers
- Incidenten rondom informatiebeveiliging (*)
- Schademeldingen
- Interne procesverstoringen
- Systeemafwijkingen (vanuit audits, steekproeven, signaleringen)

(*) Informatiebeveiligingsincident: afzonderlijke gebeurtenis of een serie ongewenste of onverwachte gebeurtenissen waarvan het waarschijnlijk is dat ze nadelige gevolgen voor de bedrijfsvoering hebben en een bedreiging vormen voor de informatiebeveiliging.

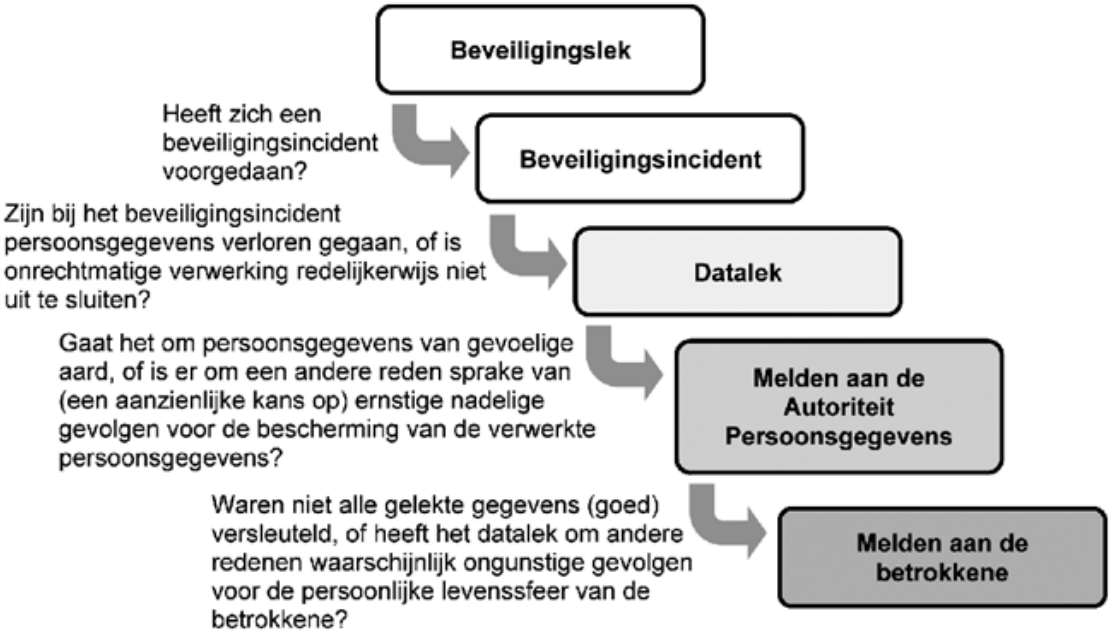
5.3 Informatiebeveiligingsgebeurtenissen en -incidenten

Zowel afwijkingen als IB-gebeurtenissen, IB-incidenten als mogelijke zwakke plekken (vermoeden dat mogelijk inbreuk op informatiebeveiliging aan de orde is) in de informatiebeveiliging, moeten gemeld worden bij de Compliance Adviseur zodat registratie en nadere analyse kan plaatsvinden. Doel van deze analyses is om te achterhalen wat de mogelijke oorzaak is geweest of zou kunnen zijn zodat corrigerende en preventieve maatregelen getroffen kunnen worden. Deze stappen moeten ertoe leiden dat de kans op herhaling van de ongewenste gebeurtenis wordt geminimaliseerd.
Meldingen die ICT signaleert worden geregistreerd in Qarebase en onderzocht. Bij geen ernstige problemen wordt de Compliance Adviseur niet geïnformeerd maar wordt dit gewoon afgehandeld. Binnen de escalatieprocedure worden zo nodig directe (correctieve) maatregelen getroffen om vervolgschade tot een minimum te beperken.

5.3.1 In contact treden met de Autoriteit Persoonsgegevens en betrokkene(n)

De FG doet melding van een datalek op de website van de Autoriteit Persoonsgegevens. De FG maakt ook de afweging of de betrokkenen (bijv. getroffen patiënten) moeten worden geïnformeerd.

Het onderstaande schema geeft in het kort deze afwegingen weer:



Bron: AP

5.3.2 In contact treden met leverancier

Overigens is het ook mogelijk dat een IB-incident bij een leverancier ontstaat. Met leveranciers zijn aanvullende contractuele afspraken in dit kader gemaakt.

5.3.3 Oplossen incident

In het kader van datalekken is bij het oplossen van het incident vooral van belang het voorkomen van meer schade of herhaling.
Maatregelen dienen te zijn gericht op:

- Dichtzetten systeem
- Zorgvuldige vastlegging van acties en bewijsmateriaal
- Communicatie aan alle betrokkenen
- Voorkomen van imagoschade

5.3.4 Afsluiten incident en evalueren

Na oplossing wordt het incident gesloten. De werkgroep Informatiebeveiliging en FG-er bespreken de afhandeling van het incident en leggen deze evaluatie vast. Doel hiervan is om eenzelfde situatie te voorkomen (leren van incidenten) en eventueel preventieve maatregelen te nemen. De evaluatie wordt vastgelegd in TopDesk.

5.3.5 Escalatie

Als, door het optreden van een (informatiebeveiligings-) incident, een proces dusdanig verstoord is of kan worden, dat dit leidt tot ernstige problemen of verlies van de vertrouwelijkheid, integriteit of beschikbaarheid van informatie, dan wordt direct geëscaleerd (opgeschaald) om gericht actie te kunnen ondernemen om (vervolg) schade zoveel mogelijk te voorkomen.

5.3.6 Continuïteitsplan

In het Continuïteitsplan zijn voor diverse (informatiebeveiligings)incidenten die zouden kunnen optreden, scenario's uitgewerkt waarmee de gevolgen van een calamiteit zo veel mogelijk beperkt

kunnen worden en In het Continuïteitsplan zijn voor diverse (informatiebeveiligings)incidenten die zouden kunnen optreden, scenario's uitgewerkt waarmee de gevolgen van een calamiteit zo veel mogelijk beperkt kunnen worden en de continuïteit van de dienstverlening zoveel mogelijk kan worden geborgd.
Het Continuiteïtsplan wordt periodiek beoordeeld en waar nodig herzien.
Het Continuïteitsplan wordt volgens een vast schema geoefend en getest (zie Controleprogramma) om zodoende de effectiviteit van (beheers) maatregelen en mogelijke verbeterpunten te kunnen bepalen. De resultaten van de oefening worden besproken en vastgelegd in de managementreview.

5.3.7 Opvolging van corrigerende maatregelen

Eventuele maatregelen naar aanleiding van meldingen of afwijkingen worden opgenomen in de actielijst die wordt besproken in IB-overleg waar voortgang en effectiviteit van de maatregelen bepaald worden. In de directiebeoordeling worden de corrigerende maatregelen nader beschouwd, wat kan leiden tot aanpassing van doelstellingen, de risico-matrix, de maatregelen set of controleprogramma.

5.3.8 Verantwoordelijkheden

Security Officer:

- Opvolgen incidenten en rapporteren aan FG en IB-werkgroep
- Bespreken actielijst in IB-overleg

Iedereen:

- Rapporteren IB-gebeurtenissen en IB-incidenten

1. Communicatie

6.1 Doel

Het stimuleren en bevorderen van de interne en externe communicatie met betrekking tot Informatiebeveiliging binnen Dutch Medical Group. Dit moet leiden tot:
Uitwisselen van kennis en informatie
Beslissen over te nemen acties
Maken van duidelijke afspraken

6.2 Communicatie

Binnen Dutch Medical Group vindt op diverse manieren en op verschillende momenten, gepland en ongepland, communicatie plaats. Een belangrijk deel van deze communicatie vindt plaats in de vorm van overleggen en betreft de interne processen en aansturing en informeren van de medewerkers. In onderstaande tabel een overzicht van de overlegvormen.

Naast intern overleg, vindt er ook (projectmatig) overleg met onze klanten en leveranciers plaats. In deze overleggen wordt niet alleen ingegaan op het project zelf, maar wordt ook aandacht besteed aan ontwikkelingen in de sector en de markt en wordt geïnventariseerd wat de wensen en verwachtingen zijn, bij zowel opdrachtgevers als leveranciers, ten aanzien van informatiebeveiliging.

Controleprogramma

Doel

Het opstellen en uitvoeren van een controleprogramma om de werking van de beheersmaatregelen te verifiëren en beoordelen.

Methode Controleprogramma

Er dient te worden vastgesteld welke controles nodig zijn om problemen met de informatiebeveiliging te voorkomen en/of vroegtijdig te herkennen.

Vaststellen controles

Voor het controleren op de mate van beheersing van informatiebeveiliging worden de volgende drie soorten controles onderscheiden:

- **Toetsen**: bespreken of uitvoeren van tests om te beoordelen of beheersmaatregelen het beoogde effect hebben,
- **Doornemen**: doornemen procedures en instructies met betrokkenen, bijvoorbeeld door interne audit met als doel te beoordelen of er significante wijzigingen zijn ten opzichte van het Managementsysteem.
- **Meten:** nagaan of beheersmaatregelen het beoogde effect hebben, bijvoorbeeld door meten en analyseren.

Opvolging toetsen

Wanneer bij een verificatie-controle een afwijking wordt ontdekt wordt nagegaan hoe de fout heeft kunnen ontstaan en wordt zo mogelijk een corrigerende maatregel genomen om een dergelijke fout in de toekomst te voorkomen.

Opvolging doornemen

Wanneer tijdens het doornemen van een procedure of instructie een afwijking ten opzichte van de praktijk wordt ontdekt, wordt hierop zo snel mogelijk actie ondernomen. Dit kan resulteren in twee soorten maatregelen. De medewerker conformeert zich weer aan de procedure/instructie of de procedure/instructie wordt aangepast aan de nieuwe situatie/afspraken.

Opvolging meten

Wanneer bij een praktijk-controle wordt ontdekt dat een beheersmaatregel in de praktijk niet het beoogde effect heeft, wordt nagegaan wat hier de oorzaak van is. Op basis van de vastgestelde oorzaak wordt een corrigerende maatregel opgesteld.

Registratie maatregelen

De vastgestelde maatregelen worden geregistreerd en bewaakt in de IB actielijst.

Controleprogramma

In het controleprogramma zijn de voor de organisatie relevante controles opgenomen. Per controle zijn de volgende elementen beschreven:

- Controlenummer (V[nr], D[nr] of P[nr]);
- Controlevorm;
- Omschrijving;
- Doelstelling;
- Betrokkenen;
- Frequentie

Evaluatie van het controleprogramma

Het controleprogramma wordt jaarlijks tijdens de Directiebeoordeling geëvalueerd, waarbij wordt beoordeeld in hoeverre de controles zijn uitgevoerd en of deze controles het beoogde effect hebben gehad. Op basis hiervan wordt het controleprogramma desgewenst aangepast.

Interne Audit

Doel

Interne audits hebben 3 doelen (de 3 V's):
Vaststellen (verifiëren) dat er gewerkt wordt volgens de vastgelegde procedures
Vormen van bewustzijn van medewerkers
Verbeteren van het proces
Met deze doelen wordt onder meer bereikt dat regelmatig en op systematische wijze de mate van implementatie en doeltreffendheid van het managementsysteem wordt getoetst.

Procedure

Selectie van auditonderwerpen

Om te kunnen beoordelen of het managementsysteem voor informatiebeveiliging en de invulling van de processen goed verloopt, worden interne audits uitgevoerd. De uitvoering van de interne audits vindt **plaats** aan de hand van een meerjarenplanning (auditmatrix) die wordt vastgesteld op basis van “status en belang”. Processen waarvan het afbreukrisico groot is, waar (veel) klachten/afwijkingen (kunnen) optreden of die van groot belang zijn bij het behalen van de beoogde doelen, zullen vaker worden ge-audit. De verantwoordelijkheid voor het plannen en (laten) uitvoeren van de interne audits ligt bij de Compliance Adviseur.

Uitvoering van interne audits

De interne audits worden uitgevoerd door interne auditoren onder leiding van de Compliance Advisuer die beschikt over de benodigde kennis, ervaring en vaardigheden om dit op de juiste manier te kunnen doen. Kennis van de norm (NEN7510), ervaring met het uitvoeren en rapporteren van de interne audits en kennis van het eigen managementsysteem, zijn belangrijke randvoorwaarden m.b.t. de keuze van in te zetten auditoren. Daarbij is ook van belang dat de interne auditor onafhankelijk is ten opzichte van de te auditen systemen of processen.

Rapportage bevindingen

De bevindingen van de interne audits worden vastgelegd in een auditrapportage, waarbij afwijkingen worden ingedeeld in een tekortkoming of een aanbeveling ter verbetering. Bij een tekortkoming is er sprake van een serieuze afwijking op een normeis of een werkwijze en is actie op korte termijn gewenst, een afwijking die de kwalificatie "aanbeveling" krijgt, kan gezien worden als een verbeterpunt die een minder hoge prioriteit behoeft. De geconstateerde afwijkingen en daarbij behorende acties of maatregelen, worden opgenomen in de actielijst zodat toewijzing van actiehouder, einddatum en opvolging daarvan kunnen plaatsvinden. Opvolging van deze acties en maatregelen valt onder verantwoordelijkheid van de ict manager en Compliance Adviseur

Auditplan

Voor de jaarplanning van alle audits wordt verwezen naar het Auditplan.

Continuïteitsplanning

De bedrijfscontinuïteit van de informatiesystemen wordt als belangrijk gezien. Als informatie een bepaalde periode niet beschikbaar is, kan de organisatie haar burgers niet meer bedienen. De organisatie stelt vast dat er diverse maatregelen getroffen moeten worden om te zorgen dat uitval van de processen tot een minimum wordt beperkt. Echter erkent de organisatie dat er altijd situaties kunnen optreden dat deze maatregelen niet meer zullen voldoen. De organisatie zal een beheerproces van bedrijfscontinuïteit implementeren om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie (als gevolg van bijvoorbeeld natuurrampen, ongevallen, uitval van apparatuur en opzettelijke handelingen) en het herstellen daarvan, tot een aanvaardbaar niveau te beperken.

Identificatie bedrijfsprocessen

Om inzage te krijgen in het belang van de te onderkennen bedrijfsprocessen zullen alle processen beoordeeld worden op hun aard. Er is een proces aanwezig welke de kritische bedrijfsprocessen

identificeert. Het behoort de informatiebeveiligingseisen voor de bedrijfscontinuïteit te integreren met andere continuïteiteisen, zoals die zijn bepaald voor personeel, operaties (bijv. verhuizingen), materialen, transport en voorzieningen.

Business impact analyse

De gevolgen van rampen, beveiligingsincidenten, uitval van diensten en de beschikbaarheid van diensten behoren te worden beoordeeld aan de hand van een “business impact” analyse. Er behoren continuïteitsplannen te worden ontwikkeld en geïmplementeerd om het tijdig hervatten van essentiële bedrijfsprocessen te waarborgen. Informatiebeveiliging behoort een integraal onderdeel te zijn van het totale bedrijfscontinuïteit proces en andere beheerprocessen binnen de organisatie.

Het beheersproces van bedrijfscontinuïteit behoort beheersmaatregelen te omvatten voor het identificeren en verminderen van risico's, als aanvulling op het algemene risicobeoordelingsproces, het beperken van de consequenties van incidenten die schade toebrengen en veiligstellen dat informatie die vereist is voor het bedrijfsproces vlot weer beschikbaar is.

Uitwijk

In veel gevallen zullen na een calamiteit de werkzaamheden op de huidige locatie voortgezet kunnen worden, maar in uitzonderlijke omstandigheden zal een uitwijk noodzakelijk zijn. De organisatie zal hiervoor passende maatregelen treffen, hierbij zullen niet alleen de technische voorzieningen aanwezig zijn. Er zullen ondersteunende maatregelen (zoals opslag van noodzakelijke documentatie en andere bedrijfsmiddelen) getroffen worden om de voortgang van het proces te waarborgen.

Naleving wet- en regelgeving

Dutch Medical Group zal relevante wettelijke en regelgevende eisen en contractuele verplichtingen naleven en passende maatregelen treffen binnen de organisatie.
Specifiek betreft het de wettelijke vereisten vanuit:

- Algemene Verordening Gegevensbescherming
- Auteurswet en octrooiwet;
- Wet Computer Criminaliteit;
- Goed Beheerd Zorgsysteem
- Wet Ambulancezorgvoorzieningen.

De maatregelen zullen worden getroffen voor zowel de bediening, het gebruik als het beheer van informatiesystemen.

De organisatie zal bij haar activiteiten de relevante wet- en regelgeving nauwlettend in de gaten houden en daar waar nodig hieraan verdere invulling geven.

Indien de organisatie besluit een informatiesysteem te laten ontwerpen zal bij de ontwikkeling de relevante wet- en regelgeving worden betrokken.

Advisering

Ten aanzien van specifieke juridische eisen zal de organisatie advies in winnen bij interne en/of externe juridische adviseurs.

Reikwijdte van het beleid: Scope

Dit beleid is van toepassing op alle bedrijfsprocessen, alle informatiesystemen (bestaande en nieuw aan te leggen), de gebruikte interne netwerken, de netwerkkoppelingen, de toepassingen, alle organisatie locaties en interne en externe medewerkers.

Goedkeuring van het beleid

Dit informatiebeveiligingsbeleid is goedgekeurd op 09-2023 door het management van Dutch Medical Group , te Lijnden en na revisie goedgekeurd door management op 29 april 2024

Geldigheid van het beleid

Het informatiebeveiligingsbeleid heeft een geldigheidsduur van 4 jaar na vaststelling door het management Dutch Medical Groupt, waarna het opnieuw wordt beoordeeld en waar noodzakelijk bijgesteld. Bij een belangrijke wijziging van de fysieke of logische omgeving, of een belangrijke wijziging van mogelijke dreigingen en kwetsbaarheden zal het informatiebeveiligingsbeleid eerder worden bijgesteld. Tevens zal het informatiebeveiligingsbeleid worden aangepast indien dit op basis van aanpassingen van landelijke wet- en regelgeving noodzakelijk blijkt.

2. Beleidsverklaring directie

De directie van Dutch Medcial Group hecht grote waarde aan informatiebeveiliging. Met het ondertekenen van deze beleidsnotitie wil de directie de kaders aangeven die ertoe leiden dat de continuïteit van informatie en de informatievoorziening gewaarborgd is en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau beperkt blijft.
De directie verwacht van de medewerkers en leidinggevenden:

- Een proactieve opstelling ten aanzien van risicobeheersing op het gebied van informatiebeveiliging.
- Bij het vaststellen van een risicosituatie, een adequate reactie richting de direct leidinggevende en indien mogelijk direct wegnemen van het gevaar.
- Het blijven behouden van medeverantwoordelijkheid en meedenken over oplossingen ten aanzien van ervaren risicosituaties.
- Dat zij elkaar aanspreken op onzorgvuldig gedrag en dat zij dit ‘elkaar aanspreken’ van elkaar accepteren.

DGA en MT Dutch Medical Group
Edzard Enschede

Datum: 29 april 2024

2. Personeel

Personeel vormt een belangrijk onderdeel van de bedrijfsprocessen. Zonder het personeel zal geen bedrijfsproces worden uitgevoerd - de medewerkers vormen dan ook een belangrijke schakel in de informatiebeveiliging. De organisatie stelt dat er specifieke personeelsmaatregelen noodzakelijk zijn om de betrouwbaarheid van de bedrijfsprocessen te garanderen.
Dit betekent dat de medewerkers op de hoogte moeten zijn en blijven van de voor hen geldende beveiligingsregels en -maatregelen.
De organisatie heeft hiervoor een communicatiekanaal ingericht om de maatregelen bekend te maken. Daarnaast is de lijnmanager aanspreekpunt voor beveiligingsvragen, hierin bijgestaan door de security officer.

18.1 Indiensttreding

Bij aanstelling worden nieuwe medewerkers, ingehuurd personeel en externe gebruikers op geschikte wijze gescreend, in het bijzonder voor vertrouwensfuncties. Medewerkers die in dienst zijn hebben minimaal een VOG. Voor ingehuurde medewerkers geldt dat in de overeenkomst met het uitzendbureau de voorwaarden t.a.v. door hen uitgevoerde screening zijn vastgelegd. Bij de screening van personeel wordt rekening gehouden met de aard van de functie en aansluiting bij de geldende regelgeving. De verantwoordelijkheden van iedere werknemer zijn vastgelegd in een bijbehorende functiebeschrijving.
In het arbeidscontract met bijbehorende arbeidsvoorwaarden is de verplichting tot geheimhouding en naleven van de ‘Gedragscode Informatiebeveiliging’ opgenomen.

18.2 Uitdiensttreding

Als een medewerker, intern, ingehuurd of externe gebruiker de organisatie verlaat worden de toegekende toegangsrechten ingetrokken en levert de medewerker alle in bruikleen gegeven apparatuur en programmatuur in. Dit wordt bewaakt d.m.v. een checklist.

18.3 Bewustwordingsproces

Het is van belang dat eenieder zich bewust is van de mogelijke beveiligingsrisico’s. Daartoe heeft de organisatie een bewustwordingsprogramma ontwikkeld, dat door alle medewerkers (intern en inhuur) gevolgd wordt. Deze niet vrijblijvende bewustwordingscampagne zal afgestemd zijn op de functie van de medewerker.

18.4 Disciplinair proces

In geval van beveiligingsinbreuken zijn de cao, de arbeidsovereenkomst, de functieprofielen, de Gedrags- en Beroepscode en het Burgerlijk Wetboek van toepassing.

3. Fysieke beveiliging

Informatiebeveiliging begint bij de voordeur. Uitgangspunt is dat IT-voorzieningen en data/informatie (zowel elektronisch als niet elektronisch) fysiek ondergebracht dienen te worden in beveiligde ruimten en in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze worden fysiek beschermd tegen toegang door onbevoegden en tegen alle andere schade en storingen.
Deze bescherming dient in overeenstemming te zijn met de vastgestelde risico's, dit betekent dat bij de uit te voeren risicoanalyses de fysieke omgeving meegenomen wordt.

19.1 Beveiliging apparatuur

Apparatuur dient beschermd te zijn tegen fysieke bedreigingen en gevaren van buitenaf.

Bescherming van apparatuur en data die buiten de locatie wordt gebruikt is noodzakelijk om het risico van toegang door onbevoegden tot deze informatie uit te sluiten en om de apparatuur en informatie te beschermen tegen verlies of schade. De organisatie zal aanvullende maatregelen treffen om mobiele apparatuur, die zich bevindt in de voertuigen, te beveiligen.