Informatiebeveiligingsbeleid

Versie 2.3 **Auteur** Dieter Vorderhake **Datum** 20/04/22

Classificatie OPENBAAR

Inhoudsopgave

1. Inleiding

1.1 Toelichting

Dit document beschrijft het beleid van HealthConnected met betrekking tot de beveiliging van informatie. Informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van HealthConnected. Zowel op papier als geautomatiseerd is HealthConnected bij het dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. De organisatie en de informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt. Dit beleid is vastgelegd in het onderhavige document.

1.2 Definitie van informatiebeveiliging

Informatiebeveiliging wordt als volgt gedefinieerd:

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

Opgemerkt wordt dat informatiebeveiliging een *samenhangend stelsel van maatregelen* omvat. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Het stelsel van beveiligingsmaatregelen heeft tot doel een blijvend niveau van beveiliging te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn gehandhaafd blijft. Informatiebeveiliging is gericht op het realiseren van een optimaal niveau van beveiliging. Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

1.3 Doelstelling informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen HealthConnected vast te stellen en vast te leggen. Hiermee vormt het beleid de leidraad voor alle medewerkers binnen HealthConnected. HealthConnected heeft informatiebeveiliging hoog in het vaandel staan, omdat zij:

- patiëntgegevens wil beveiligen;
- het bewustzijnsniveau m.b.t. informatiebeveiliging onder de medewerkers wil vergroten (zie voor verdere uitwerking het jaarplan);
- wil voldoen aan wet- en regelgeving;
- wil aantonen door middel van certificering dat zij betrouwbaar omgaat met informatie en dat zij hierdoor een betrouwbare partner is (realiseren van klantenbinding).

1.4 Doelstelling informatiebeveiliging

Zoals in de definitie van informatiebeveiliging is verwoord, is het doel van informatiebeveiliging om een *optimaal niveau te realiseren van*:

- **Beschikbaarheid**: de informatie moet op de gewenste momenten beschikbaar zijn;
- **Integriteit**: de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- **Vertrouwelijkheid**: de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Om te kunnen bepalen wat het niveau is van beschikbaarheid, integriteit en vertrouwelijkheid en of het aan de eisen voldoet, zijn er periodieke controles ingericht op maandelijkse, kwartaal en halfjaarlijkse basis. Deze controles bestaan uit administratieve en technische controles en zijn direct gerelateerd aan de beschikbaarheid, integriteit en vertrouwelijkheid. De acceptatiecriteria zijn:

- 90% - 100% acceptabel
- 70% - 90% acceptabel, wel melden als verbeterpunt
- 0% - 70% onacceptabel, direct melden bij directie

Het percentage van de controles worden bepaald op basis van tellingen (goed/fout) tijdens de controles. Deze kunnen bestaan uit tellingen van servers, laptops/computers, medewerkers, accounts & steekproeven van procedures. Daarnaast zijn er nog controles op basis van (interne en externe) audits, PEN testen en restore testen waarbij de uitkomst in zijn geheel goed of fout is.

De uitkomst van de periodieke controles wordt gerapporteerd in de kwartaalrapportage en bij afwijkingen behandeld in het directieoverleg (zie §4.5).

1.5 Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op:

Ontwerpen, ontwikkelen en functioneel beheer van HealthConnected software voor elektronische patiëntdossiers in de eerstelijnszorgverlening.

HealthConnected hanteert als uitgangspunt dat zij verantwoordelijk is voor de correcte verwerking van alle gegevens die door klanten met behulp van HealthConnected software worden vastgelegd. HealthConnected is daarbij verantwoordelijk voor het treffen van passende technische en organisatorische maatregelen bij het ontwikkelen, beheren, hosten en ondersteunen van deze HealthConnected software.

HealthConnected is nadrukkelijk niet verantwoordelijk voor de apparatuur waarop onze producten worden gebruikt, de juistheid van de uit andere bronnen verkregen of handmatig ingevoerde data en de werking van aan HealthConnected software gekoppelde applicaties.

HealthConnected faciliteert gebruikers van HealthConnected software bij het voldoen aan de voor hen van toepassing zijnde wet- en regelgeving. HealthConnected is niet verantwoordelijk voor de wijze waarop gebruikers van HealthConnected software ook daadwerkelijk gebruik maken van deze mogelijkheden.

Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie. Een uitleg over de context waarbinnen HealthConnected opereert is te vinden in het document ‘Context van HealthConnected’.

1.6 Verantwoordelijkheid informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid.

De CISO is verantwoordelijk voor het onderhoud van het informatie-beveiligingsbeleid.

1.7 Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is binnen HealthConnected verder uitgewerkt in o.a. de volgende documenten:

- Handboek informatiebeveiliging;
- ISMS;
- Risicoanalyse;
- Directiebeoordeling;
- Procedures;
- Werkinstructies.

Een overzicht van alle documentatie is te vinden in het ISMS. De documentatie is opgeslagen op de gedeelde schijf binnen de beveiligde kantooromgeving.

1.8 Middelen

HealthConnected gebruikt de volgende middelen voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging:

- Microsoft Office;
    - Word: opstellen beleidstukken, protocollen, procesbeschrijvingen en overige documenten;
    - Excel: inrichten, registreren en onderhouden van het ISMS en risicoanalyses;
    - Visio: maken van stroomschema's voor procesbeschrijvingen.
- Adobe Acrobat; (intern) publiceren van beleidstukken, protocollen, procesbeschrijvingen en overige documenten;
- Gedeelde schijf (binnen de beveiligde kantooromgeving): opslag voor alle documentatie binnen HealthConnected.

1.9 Inhoud informatiebeveiligingsbeleid

In hoofdstuk 2 zijn de uitgangspunten vastgelegd die worden gehanteerd bij de toepassing van informatiebeveiliging binnen HealthConnected. In hoofdstuk 3 wordt aandacht besteed aan het beleidsproces voor informatiebeveiliging. Hoofdstuk 4 beschrijft de organisatie van informatiebeveiliging.

2. Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen HealthConnected worden de volgende uitgangspunten gehanteerd:

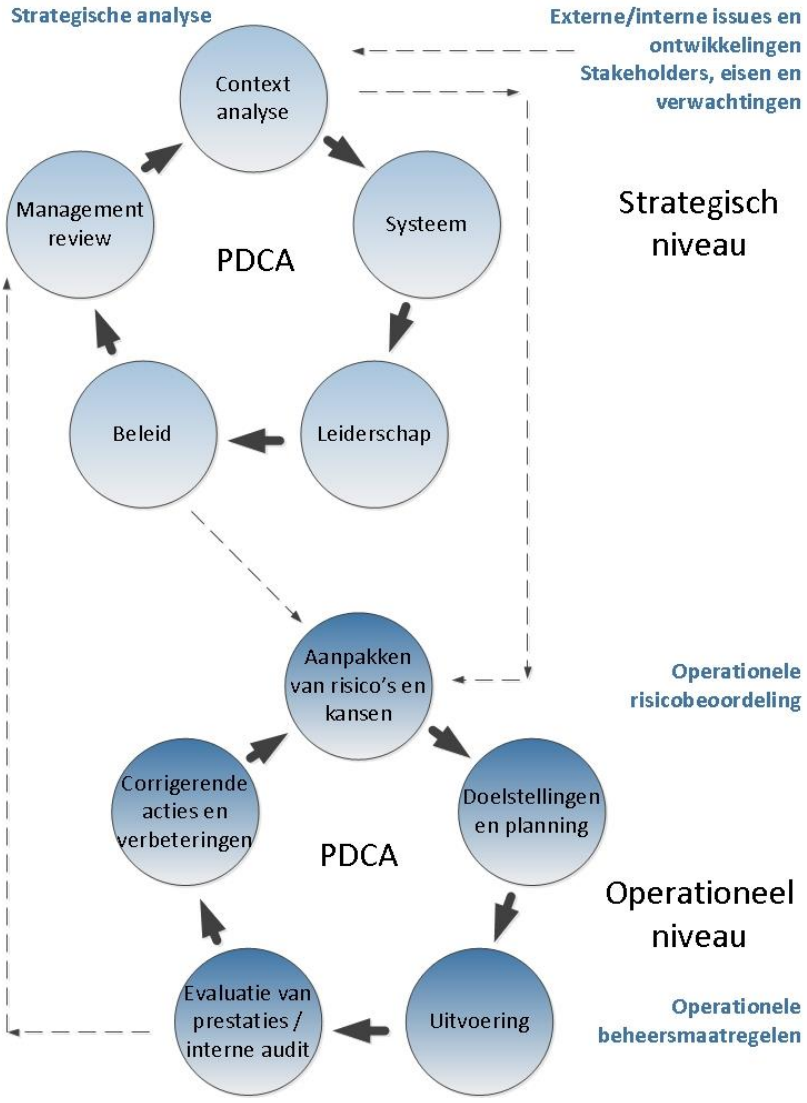
- HealthConnected voldoet aantoonbaar aan de ISO 27001:2013 en de NEN 7510 normen.
- HealthConnected voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
    - Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG)
    - Algemene Verordening Gegevensbescherming (AVG)
    - Wet Geneeskundige Behandelingsovereenkomst (WGBO).
    - Wet Computer Criminaliteit (WCC)
    - Archiefwet
    - Belastingwet
- Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle onderdelen van HealthConnected hebben hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd. De in hoofdstuk 4 beschreven organisatie van informatiebeveiliging vormt hierbij de leidraad.
- Wanneer (onderdelen van) HealthConnected samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
- De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van HealthConnected zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
- Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
- HealthConnected voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren.
- HealthConnected beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.

- Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de directie een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in het handboek informatiebeveiliging.
- Alle onderdelen van HealthConnected hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
- Alle onderdelen van HealthConnected hebben maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, etc.) vormen hiervan een belangrijk onderdeel.
- Alle onderdelen van HealthConnected hebben maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
- Bij de ontwikkeling en aanschaf van informatiesystemen wordt in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan informatiebeveiliging.
- Alle onderdelen van HealthConnected hebben adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
- Als onderdeel van het beleidsproces voor informatiebeveiliging wordt binnen HealthConnected door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
- Alle onderdelen van HealthConnected beschikken over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligings-incidenten wordt benut voor de verbetering van informatiebeveiliging.

3. Beleidsproces voor informatiebeveiliging

3.1 Overzicht beleidsproces informatiebeveiliging

Binnen het beleidsproces voor informatiebeveiliging is het belangrijk dat de strategische richting van de organisatie gekoppeld is aan de bedrijfsvoering om ervoor te zorgen dat het managementsysteem niet meer in de zijlijn staat van de echte bedrijfsvoering. In de volgende paragrafen worden de twee PDCA-cyclussen toegelicht.



3.2 Contextanalyse

De eerste stap van het beleidsproces voor informatiebeveiliging bestaat uit twee delen:

- het vaststellen van interne en externe onderwerpen die relevant zijn voor de doelstelling en die het vermogen beïnvloeden om de beoogde resultaten van het managementsysteem voor informatiebeveiliging te behalen;
- inzicht verkrijgen in de belanghebbenden, en de verwachtingen en eisen die zij hebben, die van belang zijn voor het managementsysteem voor informatiebeveiliging.

3.3 Systeem

Dit omvat het toepassingsgebied van het managementsysteem voor informatiebeveiliging waarin de grenzen en toepasselijkheid van de interne en externe onderwerpen, de verwachtingen en eisen evenals de raakvlakken van activiteiten met de activiteiten van andere organisaties worden vastgesteld.

3.4 Leiderschap

De directie zal leiderschap en betrokkenheid moeten tonen met betrekking tot het managementsysteem voor informatiebeveiliging door:

- het beleid en de doelstellingen vast te stellen en aan te laten sluiten bij de strategische richting van de organisatie;
- het beleid in de organisatie te integreren;
- ervoor te zorgen dat de benodigde middelen beschikbaar zijn om het beleid uit te voeren;
- het belang van een doeltreffend beleid te communiceren;
- ervoor te zorgen dat het beleid zijn beoogde resultaten behaald;
- mensen aan te sturen en te ondersteunen om bijdrage te leveren aan de doeltreffendheid van het beleid;
- continue verbetering te bevorderen;
- andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebied.

3.5 Beleid

Onderhavig document dat:

- passend is voor het doel van de organisatie;
- beschikbaar is als gedocumenteerde informatie;
- gecommuniceerd wordt binnen de organisatie;
- een verbintenis aan gaat om te voldoen aan de van toepassing zijnde eisen voor informatiebeveiliging en het continu verbeteren van het managementsysteem voor informatiebeveiliging.

3.6 Directiebeoordeling

Dit is de beoordeling door de directie van het managementsysteem voor informatiebeveiliging om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen. Het bevat beslissingen met betrekking tot kansen voor verbetering en de noodzaak tot wijziging van het managementsysteem voor informatiebeveiliging. Gedocumenteerde informatie moet bewaard blijven als bewijsmateriaal van de resultaten van de directiebeoordeling. In de beoordeling wordt opgenomen:

- De status van de acties van de voorgaande beoordelingen;
- Wijzigingen in de interne en externe onderwerpen die relevant zijn voor het managementsysteem voor informatiebeveiliging;
- Feedback over de informatiebeveiligingsprestaties, waaronder; afwijkingen en corrigerende maatregelen, resultaten van monitoren en meten, auditresultaten en of er voldaan is aan informatiebeveiligingsdoelstellingen;
- Feedback van belanghebbenden;
- Resultaten van de risicobeoordelingen en status van het risicobehandelplan;
- Kansen voor continue verbetering.

3.7 Aanpakken van risico's en kansen

De risico's en kansen van de onderwerpen die naar voren gekomen zijn en eisen die gesteld zijn in de contextanalyse worden vastgesteld, beoordeeld en aangepakt. De risicoanalyse wordt gemaakt aan de hand van:

- een risicobeoordelingsprocedure voor informatiebeveiliging;
- een behandelprocedure voor informatiebeveiligingsrisico's. Beheersmaatregelen die hier uit voortkomen moeten passend zijn voor de risicobeoordeling;
- verklaring van toepasselijkheid (bevat beheersmaatregelen, de rechtvaardiging daarvan, of het is geïmplementeerd of niet en de rechtvaardiging van uitsluiting van beheersmaatregelen);
- aanvaarding en goedkeuring van het behandelplan door de risico-eigenaren en de acceptatie van de overblijvende informatiebeveiligingsrisico's.

3.8 Doelstellingen en planning

Het vastleggen van relevante informatiebeveiligingsdoelstellingen voor relevante functies en op relevante niveaus. Deze zijn consistent met het informatiebeveiligingsbeleid, meetbaar, houden rekening met informatiebeveiligingseisen en resultaten van risicobeoordeling en –behandeling, worden gecommuniceerd en geactualiseerd. In de planning van de doelstellingen staat:

- Wat er gedaan moet worden;
- Welke middelen er nodig zijn;
- Wie er verantwoordelijk is;
- Wanneer het voltooid moet zijn;
- Hoe de resultaten worden geëvalueerd.

3.9 Uitvoering

Aan de hand van het informatiebeveiligingsplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van management en medewerkers.

3.10 Evaluatie van prestaties/interne audit

Hier wordt vastgesteld door wie, wanneer en wat er gemonitord en gemeten moet worden en met welke methoden. De resultaten worden geanalyseerd en geëvalueerd en bewaard als bewijsmateriaal. De interne audit wordt uitgevoerd om informatie te verkrijgen of het managementsysteem voor informatiebeveiliging functioneert en overeenkomt met het eisen die gesteld zijn door de organisatie en de (inter)nationale norm. Deze audit loopt volgens een vast programma dat regelmatig wordt uitgevoerd en controleert op de doeltreffendheid van het managementsysteem voor informatiebeveiliging.

De organisatie van deze controle en de afspraken voor de bijbehorende rapportage wordt in hoofdstuk 4 nader uitgewerkt.

3.11 Corrigerende acties en verbeteringen

Wanneer er uit de evaluatie afwijkingen geconstateerd zijn dan worden die beoordeeld en gecorrigeerd door juiste maatregelen te treffen. Deze maatregelen moeten doeltreffend en passend zijn voor de effecten van de afwijking. Wanneer nodig moeten wijzigingen aangebracht worden in het managementsysteem voor informatiebeveiliging. Documentatie over de afwijking, de genomen maatregelen en de resultaten daarvan moeten bewaard blijven als bewijsmateriaal.

3.12 Cyclisch proces

Het managementsysteem voor informatiebeveiliging is een continu en cyclisch proces. Dit betekent dat op basis van de uitkomst van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn om het informatiebeveiligingsbeleid aan te passen of om extra beveiligingsmaatregelen te treffen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen, informatiesystemen of wetgeving aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen.

4. Organisatie van informatiebeveiliging

4.1 Toelichting

In dit hoofdstuk wordt de organisatie van informatiebeveiliging binnen HealthConnected beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft. Bovendien levert de toewijzing van taken en verantwoordelijkheden de mogelijkheid om decharge te verlenen voor de uitgevoerde werkzaamheden.

De organisatie van informatiebeveiliging wordt beschreven volgens de volgende invalshoeken:

- het niveau van de beveiligingstaken, waarbij onderscheid wordt gemaakt naar strategische en operationele informatiebeveiliging;
- rollen en functies voor informatiebeveiliging binnen de HealthConnected.

Tenslotte wordt in dit hoofdstuk ook aandacht besteed aan de overlegvormen die in het kader van informatiebeveiliging van belang zijn en aan de manier waarop controle en rapportage is vormgegeven.

4.2 Strategisch en operationeel niveau

In het onderstaande overzicht wordt een indeling van activiteiten met betrekking tot informatiebeveiliging weergegeven waarbij het niveau van de activiteiten als onderscheidend criterium is gehanteerd.

Niveau	Activiteit	Verantwoordelijk	Documentatie
Strategisch	Beleidsvorming	Directie	Informatiebeveiligings-beleid Directiebeoordeling
Operationeel	Planning Uitvoering	Medewerkers	Risicobeoordeling Operationele procedures per eenheid

Op strategisch niveau vindt de beleidsvorming met betrekking tot informatiebeveiliging plaats. De directie is verantwoordelijk voor deze beleidsvorming en wordt hierin ondersteund door de CISO. De beleidsvorming wordt vastgelegd in het Informatiebeveiligingsbeleid.

De planning en uitvoering van activiteiten met betrekking tot informatiebeveiliging vindt plaats op operationeel niveau. Het ISMS is het meet- en stuurinstrument dat hierbij wordt ingezet. Verantwoordelijke voor deze activiteiten zijn de medewerkers.

Ten behoeve van het structureren van de uitvoering van taken met betrekking tot informatiebeveiliging worden procedures en werkinstructies opgesteld.

4.3 Rollen en functies voor informatiebeveiliging

Alle onderdelen binnen HealthConnected zijn bij informatiebeveiliging betrokken. In dit informatiebeveiligingsbeleid worden de verantwoordelijkheden van de volgende functies en rollen beschreven:

- Directie;
- CISO;
- Medewerkers;
- Functionaris voor de gegevensverwerking;
- Interne auditor.

4.3.1 Directie

De directie is eindverantwoordelijk voor alle activiteiten binnen HealthConnected en dus ook voor informatiebeveiliging.

De verantwoordelijkheid voor informatiebeveiliging omvat:

- het vaststellen van het HealthConnected-brede informatiebeveiligingsbeleid;
- het toezien op de naleving van het informatiebeveiligingsbeleid door de organisatieonderdelen;
- het evalueren van de toepassing en werking van het informatiebeveiligingsbeleid op basis van rapportages over informatiebeveiliging.

4.3.2 Chief Information Security Office (CISO)

Alle activiteiten met betrekking tot informatiebeveiliging worden binnen HealthConnected bewaakt door de CISO. De CISO is dus verantwoordelijk voor de ondersteuning en bewaking van de realisatie en naleving van het informatiebeveiligingsbeleid. De CISO is de spin in het web met betrekking tot informatiebeveiliging binnen HealthConnected. Tevens vormt de CISO ook het aanspreekpunt inzake informatiebeveiliging voor de directie, de teamleiders en de medewerkers.

De CISO heeft de volgende verantwoordelijkheden:

- beleidsvorming, het beheren van HealthConnected-brede informatiebeveiligingsbeleid en hieruit voortvloeiende procedures;
- controle en registratie, het bewaken van het niveau van informatiebeveiliging binnen HealthConnected;
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn binnen de organisatie;
- evaluatie en advies, het adviseren van de directie en de teamleiders over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen HealthConnected.

Daarnaast specifiek over beveiligingsincidenten:

- het verzamelen van informatie over (potentiële) informatiebeveiligingsincidenten en beveiligingslekken;
- het centraal registreren van (potentiële) informatiebeveiligingsincidenten;
- het analyseren en beoordelen van de aard, omvang en oorzaak van het informatiebeveiligingsincident;
- het organiseren van de evaluatie van de afhandeling van informatiebeveiligingsincidenten;

- het adviseren van de organisatie over de te nemen preventieve en herstelacties bij informatiebeveiligingsincidenten;
- het informeren en instrueren van de direct betrokkenen over de uit te voeren preventieve en herstelacties;
- het centraal informeren van gebruikers over (potentiële) informatiebeveiligingsincidenten;
- het coördineren van de uitvoering van preventieve en herstelacties.

4.3.3 Medewerkers

De leidinggevenden en de teamleider(s) zijn verantwoordelijk voor de inrichting en uitvoering van de informatiebeveiliging voor de bedrijfsprocessen. Zij worden hierbij ondersteund door de CISO.

De verantwoordelijkheid van de leidinggevenden en de teamleider(s) omvat onder andere de volgende taken:

- verantwoordelijk voor de beveiliging van de hele ICT-infrastructuur;
- positieve en actieve houding ten aanzien van informatiebeveiliging;
- fungeren als voorbeeldfunctie;
- toezicht houden op de naleving van informatiebeveiligingsmaatregelen;
- medewerking verlenen aan verbeteracties;
- autoriseren van medewerkers;
- informatiebeveiliging behandelen in werkoverleg, beoordelingen;
- afhandelen van vertrouwelijke Informatiebeveiligingsincidenten.

4.3.4 Functionaris voor de Gegevensbescherming

De functionaris voor de gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de wetgeving (zie punt 2) binnen de HealthConnected. Deze functionaris doet hiertoe aanbevelingen voor een betere bescherming van verwerkingen van persoonsgegevens. De CISO en de functionaris voor de gegevensbescherming stemmen hun activiteiten regelmatig af om een goede taakverdeling met betrekking tot informatiebeveiliging en privacybescherming binnen HealthConnected te waarborgen. De functionaris gegevensbescherming is ook het aanspreekpunt voor vragen van klanten.

4.3.5 Interne auditor

HealthConnected voert jaarlijks interne audits uit. Een interne audit is een onderzoek dat, met een systematische en gedisciplineerde aanpak, wordt uitgevoerd naar het goed en betrouwbaar functioneren van de interne

organisatie door (interne) auditors die in dienst zijn van die organisatie of extern wordt ingehuurd. In het geval van HealthConnected is gekozen om de interne audit te laten uitvoeren door een externe auditor. De auditor van HealthConnected richt zich op de normen ISO 27001/27002 en de NEN7510.

4.4 Overlegvormen voor informatiebeveiliging

Voor overleg, coördinatie en afstemming op het gebied van informatiebeveiliging worden de volgende overlegvormen onderscheiden:

- Bilateraal overleg directie en CISO;
- IBMF (informatiebeveiligingsmanagementforum) onder leiding van CISO.

De directie en de CISO overleggen regelmatig bilateraal over informatiebeveiliging. In dit overleg wordt aandacht besteed aan kwartaalrapportages, voorstellen voor de directie, voorstellen voor wijzigingen van het informatiebeveiligingsbeleid, investeringsvoorstellen voor beveiligingsmaatregelen, etc. Dit overleg wordt minimaal tweemaal per jaar gehouden.

De CISO voert overleg met key medewerkers van de afdelingen Beheer, Ontwikkeling, Business- & Accountmanagement en Support in het IBMF. Het overleg vindt plaats op maandelijkse basis en kent een standaard agenda. Het IBMF heeft de taak om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie.

4.5 Controle en rapportage over informatiebeveiliging

Met betrekking tot informatiebeveiliging worden de volgende controlevormen onderscheiden:

- operationele controle op de naleving van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen;

- controle op de voortgang van de implementatie en borging van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen;
- onafhankelijke controle.

De operationele controle op de naleving van beleid en richtlijnen wordt verricht door de leidinggevenden en de teamleider(s). Zij rapporteren aan de CISO over de voortgang van de implementatie van informatiebeveiliging binnen de eigen afdeling. Hierbij wordt de voortgang afgezet tegen de gemaakte afspraken. Deze rapportage wordt maandelijkse uitgevoerd.

Controle op de voortgang gebeurt op kwartaalbasis. De CISO verzameld de rapportages van de afdelingen. Van deze verschillende rapportages en andere interne/externe factoren wordt een geconsolideerde voortgangsrapportage gemaakt (de kwartaalrapportage). Deze rapportages wordt door de CISO besproken met de directie op het directieoverleg. Van het directieoverleg wordt een verslag gemaakt (de directiebeoordeling) waarin sturing en verbeteringen worden opgenomen alsmede het wijzigen van strategie en beleid. De CISO zorgt voor het doorvoeren van genoemde zaken in de bedrijfsvoering (ISMS).

Onafhankelijke controle (interne audit) met betrekking tot informatiebeveiliging wordt uitgevoerd door een externe auditor. Deze auditor stemt de planning van zijn activiteiten af met de CISO. De CISO wordt over de uitkomsten van de controles geïnformeerd.

Akkoord directie, 25-11-2021

Paul Witteman