MODEL

Management Systeem Informatiebeveiliging Information Security Management System (ISMS)

(Hoort bij Model Richtlijn Classificatie en Risicoanalyse Gegevensverwerkingen)

Handreiking voor de leden
GGZ Nederland, mei 2016

Met dank aan Tactus Verslavingszorg

<naam instelling>

<datum>

Brancheorganisatie voor de geestelijke gezondheids- en verslavingszorg
Piet Mondriaanplein 25 • 3812 GZ Amersfoort • Postbus 830 • 3800 AV Amersfoort • T 033 460 89 00 • KVK 40483580
info@ggznederland.nl • www.ggznederland.nl • IBAN: NL56 INGB 0687 2118 08 BIC: INGBNL2A • IBAN: NL08 ABNA 0408 3901 07 BIC: ABNANL2A

Inhoud

1 Inleiding

1.1 Achtergrond

<vermelden van informatie over de ggz instelling/ organisatie, evt missie/visie>

Wat betekent informatiebeveiliging voor < naam instelling > ?
In de gezondheidszorg is zorgvuldige en doelmatige informatievoorziening essentieel. De complexiteit van de informatievoorziening wordt eens te meer duidelijk wanneer men kijkt naar het netwerk van zorginstellingen, cliënten, financiers, medewerkers en andere belanghebbenden die een rol spelen in het verzamelen, verwerken en transporteren van (cliënt-)gegevens.

Een belangrijke verstoring van de informatievoorziening bij < naam instelling > kan een negatieve impact hebben op de zorgverlening door, en het imago van < naam instelling > . Door de groeiende samenwerkingsverbanden wordt de kans op en omvang van gereflecteerde schade op andere systemen dan waar de basisschade zich voordoet ook groter. < naam instelling > onderkent dan ook de noodzaak om risicofactoren ten aanzien van de informatievoorziening te beheersen en hecht waarde aan een adequate beveiliging van deze informatievoorziening. Het treffen van beveiligingsmaatregelen dient te resulteren in het beperken van risico's en het accepteren van risico's die als acceptabel worden beschouwd (*van onbewust risico lopen, naar bewust risico nemen*). Informatiebeveiliging is daarmee een belangrijke randvoorwaarde voor de instandhouding en de goede werking van de (zorg-)activiteiten van < *naam instelling* > en de realisatie van de doelstellingen zoals geformuleerd in de instellingsmissie.

1.2 Inhoud van dit document

Een management systeem biedt een model voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van processen en activiteiten. Met een Management Systeem voor Informatiebeveiliging (ISMS[1]) kunnen alle activiteiten op het gebied van informatiebeveiliging met behulp van een procesbenadering doeltreffend worden samengebracht en beheerst. Het management systeem waarborgt daarmee de keuze van adequate en proportionele beveiligingsmaatregelen die de informatievoorziening van < naam instelling > beschermen en vertrouwen bieden aan belanghebbenden. Het ISMS maakt onderdeel uit van de beleids(P&C-)cyclus van < naam instelling > , en benoemd de leidende uitgangspunten bij de inrichting van de informatiebeveiliging.

In dit document wordt het Management Systeem voor informatiebeveiliging (ISMS) van < naam instelling > beschreven. Het ISMS is zoveel als mogelijk afgestemd op de behoeften en doelstellingen van de instelling, beveiligingseisen, de processen die daarvoor worden ingezet en de omvang en structuur van de instelling.

---

[1] In dit document wordt gebruik gemaakt van de internationaal gebruikelijke aanduiding voor een management systeem voor informatiebeveiliging: Information Security Management System (ISMS).

1.3 Opbouw van dit document

In *hoofdstuk 2* van dit document wordt de doelstelling en de reikwijdte van het Management Systeem voor Informatiebeveiliging (ISMS) van < naam instelling > beschreven.
In *hoofdstuk 3* worden de uitgangspunten beschreven die voor < naam instelling > leidend zijn bij de inrichting van het ISMS, de beveiligingsorganisatie en de te treffen beveiligingsmaatregelen en –voorzieningen.
Hoofdstuk 4 documenteert de organisatie (taken, bevoegdheden en verantwoordelijkheden) rondom het treffen, in stand houden en naleven van informatiebeveiligingsmaatregelen.
In *hoofdstuk 5* wordt het door < naam instelling > toegepaste Plan-Do-Check-Act-(PDCA)model beschreven om de ISMS-processen te structureren.
Tot slot worden in *hoofdstuk 6* het raamwerk en de door < naam instelling > gevolgde methode voor risicoanalyse (SPARK) beschreven.

2 Structuur ISMS

2.1 Inleiding

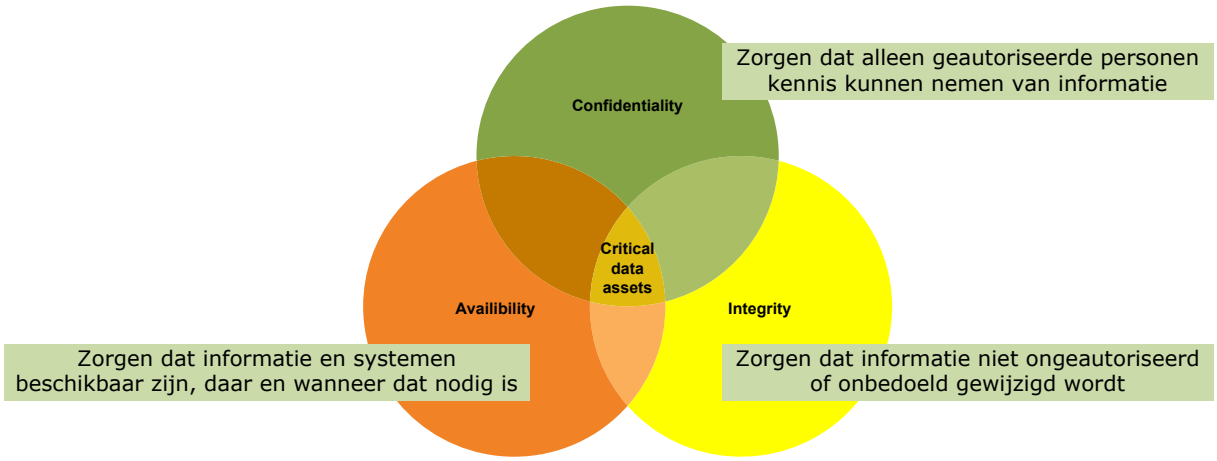
Een managementsysteem maakt het mogelijk bedrijfsprocessen planmatig te beheersen. Door terugkoppeling en zonodig bijstelling vindt systematische verbetering plaats.
In dit hoofdstuk wordt de doelstelling en de reikwijdte van het Management Systeem voor Informatiebeveiliging (ISMS) van < naam instelling > beschreven. Met deze geïntegreerde procesbenadering worden de beveiligingsprocessen gestructureerd en wordt een maximale en geactualiseerde informatieveiligheid gewaarborgd.

2.2 Definitie informatiebeveiliging

Informatiebeveiliging is een samenhangend stelsel van organisatorische en technische maatregelen, in de juiste kosten/nut verhouding, om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade als gevolg van desondanks optredende verstoringen te beperken.
Informatieveiligheid wordt door < naam instelling > gekenschetst als het verzekeren van beschikbaarheid (availibility), integriteit (integrity) en vertrouwelijkheid (confidentiality) met betrekking tot de informatie. De mate van zekerstelling is afhankelijk van de classificatie van het betreffende bedrijfsmiddel. Bedrijfsmiddelen zijn alle middelen die noodzakelijk zijn om de dienstverlening van < naam instelling > richting haar cliënten te kunnen garanderen. Hieronder vallen producten, diensten, services, processen, applicaties, gegevensverzamelingen, infrastructuur, andere informatievoorzieningen en gebouwen.

De begrippen beschikbaarheid, integriteit en vertrouwelijkheid definiëren we als volgt:

- *Beschikbaarheid:* de zekerstelling dat bedrijfsmiddelen op de juiste momenten, in de gewenste toestand beschikbaar zijn;
- *Integriteit:* de waarborging van de correctheid, volledigheid en controleerbaarheid van bedrijfsmiddelen;
- *Vertrouwelijkheid:* de bescherming van bedrijfsmiddelen tegen gebruik of kennisname door niet-geautoriseerde.



Overige termen en definities die betrekking hebben op het Management Systeem voor Informatiebeveiliging zijn beschreven in Bijlage 1: *Termen en definities*.

2.3 Positionering ISMS binnen andere standaarden

Het ISMS van < naam instelling > is gebaseerd op de NEN-ISO/IEC 27001:2005 (nl) norm. In deze internationale norm wordt een procesbenadering gehanteerd voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het ISMS van een organisatie.

In deze internationale NEN-ISO norm wordt het '*Plan-Do-Check-Act*' (PDCA)-model gehanteerd om alle ISMS-processen te structureren. De invoering van het PDCA-model is ook in overeenstemming met de beginselen van de OECD-richtlijn 2002 voor de beveiliging van informatiesystemen en netwerken. Deze internationale norm biedt een betrouwbaar model voor de implementatie van deze richtlijnen voor risicobeoordeling, ontwerp en implementatie van beveiligingsmaatregelen, beveiligingsbeheer en herbeoordeling.

Kwaliteitsmanagementsysteem < naam instelling > (HKZ[2])
Kwaliteitsbeleid is geen apart beleidsterrein. Goede kwaliteit hoort een kenmerk te zijn van alle processen binnen < naam instelling > , het primaire proces voorop. Het HKZ Certificatieschema GGZ is normstellend voor de uitkomst van de primaire, bestuurlijke, beleids- en ondersteunende processen binnen < naam instelling > . < naam instelling > is sinds 2007 HKZ-gecertificeerd.

Bij de beleidscyclus van < naam instelling > is de jaarplansystematiek toonaangevend. Door middel van een meerjaren beleidsperspectief worden missie, visie en strategische doelen over meerdere jaren uitgezet. Jaarlijks worden vervolgens jaarwerkplannen op instellings-, regio-, circuit-, afdelings- en projectniveau opgesteld volgens een vast stramien, waarbij interne en externe factoren tot bijstelling en wijziging kunnen leiden. Tweemaandelijks rapporteert iedere manager aan de RvB over de mate van realisatie c.q. afwijking van de gestelde doelen. Het interne auditteam monitored de uitvoering van de jaarplannen, waaronder ook de ISMS-processen. Eén keer per jaar is het kwaliteitsmanagementsysteem zelf onderwerp van evaluatie in de zgn. directiebeoordeling. Ook op kleinere schaal wordt cyclisch gewerkt. Zo worden van in- en externe beleidsoverleggen, Managementteamvergaderingen en overlegvergaderingen met Ondernemingsraad en Cliëntenraad besluitenlijsten aangelegd, die bij herhaling worden getoetst op hun uitvoering.
Door de processen zoveel mogelijk volgens de kwaliteitscyclus te organiseren wil < naam instelling > de kwaliteit van al haar processen, inclusief het informatiebeveiligingsproces, continu verbeteren.

[2] HKZ: Harmonisatiemodel Kwaliteitsbeoordeling Zorgsector

2.4 Doelstelling ISMS

Een managementsysteem draagt zorg voor de planmatige en systematische beheersing van bedrijfsprocessen, om van te voren bepaalde doelstellingen te realiseren en verbetering van de processen mogelijk te maken. Hierbij vindt tevens terugkoppeling en zo nodig bijstelling (verbetering) plaats.
Het Information Security Management System (ISMS) van < naam instelling > is een geïntegreerde procesbenadering om alle ISMS-processen te structureren en tot een maximale informatieveiligheid te komen.
Het systeem beoogt:

- inzicht in de eisen van de organisatie ten aanzien van informatiebeveiliging en de noodzaak voor het vaststellen van beleid en doelstellingen voor informatiebeveiliging;
- implementeren en uitvoeren van beheersmaatregelen om de risico's voor informatiebeveiliging voor de organisatie te beheren ten opzichte van de algemene bedrijfsrisico's van de organisatie;
- controleren en beoordelen van de prestaties en de doeltreffendheid van het ISMS en
- continue verbetering van de informatieveiligheid, gebaseerd op objectieve meting.

2.5 Reikwijdte ISMS

Het ISMS heeft betrekking op de systemen en processen die van invloed zijn op het primaire zorgproces van < naam instelling > . Systemen buiten de directe invloedssfeer van < naam instelling > , zijnde het justitiële cliëntvolgsysteem en de internetbehandelingen (Tactive), vallen buiten de reikwijdte van het ISMS.
De beheersdoelstellingen en beheersmaatregelen die relevant en toepasbaar zijn op het ISMS van < naam instelling > zijn gedocumenteerd in de Verklaring van toepasselijkheid. Deze door de Raad van Bestuur bekrachtigde verklaring is als bijlage opgenomen in dit document: Bijlage 2 *Verklaring van toepasselijkheid.*

2.6 Beleidskaders

Het beleid heeft betrekking op de beveiliging van de informatie(verwerking) en het geeft de kaders aan waarbinnen maatregelen moeten worden ingevoerd en/of verbeterd. Dit kader wordt binnen < naam instelling > gevormd door de vastlegging van de uitgangspunten van het strategische en tactische beleid, de inrichting van de beveiligingsorganisatie, en een beschrijving van de processtappen die cyclisch in de tijd worden doorlopen (ISMS).
Het beleidskader voor de informatiebeveiliging van < naam instelling > wordt tevens bepaald door relevante wet- en regelgeving, zijnde:

- *Grondwet voor het Koninkrijk der Nederlanden (Grondwet)*. De Grondwet is het belangrijkste staatsdocument en de hoogste nationale wet van Nederland. Naast de regels voor onze staatsinrichting, beschrijft de wet de grondrechten van de burgers, waaronder privacy (artikel 10) en het briefgeheim (artikel 13);
- *Wet Bescherming Persoonsgegevens* (WBP). De wet geeft regels voor een zorgvuldige omgang met persoonsgegevens. De wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de plichten zijn van de instanties of bedrijven die gegevens gebruiken. De Autoriteit Persoonsgegevens (AP) controleert of bedrijven en instanties zich aan de Wbp houden;
- *Wet op de Geneeskundige BehandelingsOvereenkomst (WGBO).* Doel van de wet is het verduidelijken en versterken van de rechtspositie van de patiënt, rekening houdend met de eigen verantwoordelijkheid van de hulpverlener voor zijn handelen als goed hulpverlener;

- *Wet Beroepen in de Individuele Gezondheidszorg* (BIG). De wet bevat regels voor de kwaliteit van de zorgverlening door beroepsbeoefenaren in de gezondheidszorg. De wet wil daarmee patiënten beschermen tegen ondeskundig en onzorgvuldig handelen door zorgverleners;
- *Wet Bijzondere Opnemingen in Psychiatrische Ziekenhuizen (BOPZ),* beschermt mensen die te maken krijgen met gedwongen opname. In de Wet Bopz staat wat de rechten zijn van patiënten tijdens een onvrijwillige opname in een psychiatrische instelling.
- *Wet gebruik burgerservicenummer in de zorg (Wbsn-z)* regelt het gebruik van het BSN in de zorg voor zorgaanbieders, indicatieorganen en zorgverzekeraars. Het doel van de Wbsn-z is het verbeteren van de kwaliteit van de zorg door betrouwbare gegevensuitwisseling. Het BSN wordt ook gebruikt om op een betrouwbare en veilige manier patiëntgegevens uit te wisselen via het elektronisch patiëntendossier.

2.7 Richtlijnen, normen en maatregelen

Uitgangspunt voor de te treffen maatregelen en voorzieningen vormen de wettelijke kaders, de beleidskaders en de uitkomsten van de risicoanalyses. Om deze uitgangspunten concreet te maken worden richtlijnen, normen en maatregelen beschreven. Deze conform wetgeving, beleidskaders en/of risicoanalyses getroffen maatregelen zijn inzichtelijk gemaakt in de Verklaring van Toepasselijkheid.

3 Beleidskader

3.1 Inleiding

Informatiebeveiliging is een belangrijke randvoorwaarde voor de instandhouding en uitvoering van de (zorg-)activiteiten van < naam instelling > . De zorg voor het op de juiste wijze nemen van beveiligingsmaatregelen en -voorzieningen vormt dan ook een integraal onderdeel van het algemene ondernemingsbeleid van < naam instelling > .
In dit hoofdstuk worden de uitgangspunten beschreven die voor < naam instelling > leidend zijn bij de inrichting van het ISMS, de beveiligingsorganisatie en de te treffen beveiligingsmaatregelen en –voorzieningen.

3.2 Belang van Informatiebeveiliging

De informatievoorziening is vatbaar voor velerlei menselijk en niet-menselijke bedreigingen die de betrouwbaarheid van de informatievoorzieningen kunnen aantasten en waarvan de (in-)directe gevolgen ernstig kunnen zijn.
Specifiek is het inregelen van informatiebeveiliging binnen een zorginstelling als < naam instelling > belangrijk om:

- *de privacy van cliënten te kunnen waarborgen;*
- *vertrouwelijke informatie ook vertrouwelijk te houden;*
- *informatiesystemen in de lucht te houden;*
- *de betrouwbaarheid (juistheid, volledigheid en tijdigheid) van de informatievoorziening te waarborgen;*
- *netwerken te beschermen tegen indringers;*
- *informatiesystemen vrij te houden van virussen;*
- *storingen te voorkomen.*

In onderstaande tabel zijn de aspecten benoemd, waarop de informatiebeveiliging van < naam instelling > betrekking heeft, per categorie is de beheersdoelstelling aangegeven:

Beveiligingsaspect	***Beheersdoelstelling***
Beveiligingsbeleid	aangeven en ondersteunen van beleidsrichting op basis van instellingsdoelstellingen en wet- en regelgeving
Beveiligingsorganisatie	vaststellen van beheerkader om de implementatie van informatiebeveiliging in de instelling te initiëren en te beheersen
Beheer van bedrijfsmiddelen	bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de instelling
Personele beveiligingseisen	waarborgen dat medewerkers en gebruikers bewust zijn en blijven van veiligheidsrisico's en het belang van informatiebeveiliging
Fysieke beveiliging en beveiliging van de omgeving	voorkomen van onbevoegde fysieke toegang tot het terrein van de instelling waardoor de informatievoorziening wordt verstoord
Beheer van informatie- en communicatievoorzieningen	garanderen van een correcte en veilige bediening en werking van ICT voorzieningen
Toegangsbeveiliging	beheersen van de toegang tot informatie en

	bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen
Ontwikkeling en onderhoud van informatiesystemen	borgen dat nieuwe systemen de vereiste beveiliging bieden gedurende de volledige levenscyclus
Continuïteitsbeheer	adequaat reageren op verstoring van bedrijfsactiviteiten en beschermen van kritieke processen bij grootschalige calamiteiten
Naleving	door periodieke beoordeling van beleid en maatregelen waarborgen dat de informatievoorziening blijvend is gegarandeerd

3.3 Informatiebeveiligingsbeleid < naam instelling >

Informatiebeveiliging is een belangrijke randvoorwaarde voor de instandhouding en de goede werking van de (zorg-)activiteiten van < naam instelling > . De directie van < naam instelling > erkent de noodzaak om beveiligingsrisico's te beheersen en hecht dan ook waarde aan een adequate beveiliging van de informatievoorziening.
De zorg voor het op de juiste wijze nemen van beveiligingsmaatregelen en -voorzieningen vormt een integraal onderdeel van het algemene ondernemingsbeleid van < naam instelling > . Tot deze zorg behoort ook het inrichten en in stand houden van een adequaat management systeem voor informatiebeveiliging (ISMS) en de daarbij behorende beveiligingsorganisatie. De verantwoordelijkheid voor het opstellen, handhaven en toetsen van het beveiligingsbeleid is belegd bij de directeur Bedrijfsvoering/controller van < naam instelling > . Ten aanzien van de beveiligingsmaatregelen en -voorzieningen vindt een duidelijke toewijzing en delegatie van taken, verantwoordelijkheden en bevoegdheden plaats. Iedere medewerker is verantwoordelijk voor alle aspecten van de informatiebeveiliging die binnen de eigen invloedssfeer vallen. Hiertoe dient iedereen binnen de instelling bekend te zijn met de voor haar/hem geldende relevante beveiligingsmaatregelen en voorzieningen.

Gebeurtenissen die (in)direct te maken hebben met de beveiligingmaatregelen of -voorzieningen, of een inbreuk hierop kunnen maken worden gemeld conform de interne procedure voor incidentmelding (MIT). Het doel van incidentmelding is de kwaliteit van de informatiebeveiliging systematisch te toetsen en te verbeteren. Door objectieve en periodieke toetsing zal < naam instelling > de prestaties en de doeltreffendheid van het ISMS en de noodzakelijke beveiligingsmaatregelen en -voorzieningen bijhouden en continu verbeteren.

3.4 Uitgangspunten

Onderstaande uitgangspunten zijn voor < naam instelling > leidend bij de inrichting van het ISMS, de beveiligingsorganisatie en de te treffen beveiligingsmaatregelen en -voorzieningen:

- < naam instelling > streeft naar risicobeheersing en in dat kader passen adequate maatregelen op het gebied van de informatiebeveiliging;
- het doel van informatiebeveiliging is het waarborgen van de continuïteit van de zorgverlening en het minimaliseren van schade als gevolg van desondanks optredende verstoringen;
- informatiebeveiliging is van toepassing op het gehele proces van de informatievoorziening van zowel de geautomatiseerde als de niet geautomatiseerde informatiesystemen ongeacht de soort informatie en het medium waarop dit is opgeslagen;

- bij het gebruik, opslag, verstrekken en verwerken van gegevens worden de wettelijk eisen in acht genomen; zoals opgenomen in onder andere de Grondwet, Wet Bescherming Persoonsgegevens (WBP), de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), de Wet Beroepen in de Individuele Gezondheidszorg (BIG), Wet Bijzondere Opnemingen in Psychiatrische Ziekenhuizen (BOPZ) en de Wet gebruik burgerservicenummer in de zorg (Wbsn-z);
- voor de inrichting van de informatiebeveiliging gebruikt < naam instelling > de NEN-ISO/IEC 27001 als uitgangspunt, met als onderliggend normenkader de NEN7510-Informatiebeveiliging in de zorg;
- de aard en het niveau van de beveiligingsmaatregelen dient een weloverwogen weging te zijn tussen functionele eisen aan de informatievoorziening (o.a. overal bereikbaar patiëntendossier) en bijzondere risico's (gevoeligheid/vertrouwelijkheid cliëntinformatie);
- beveiligingsmaatregelen mogen niet ten koste gaan van de veiligheid van cliënten, eigen personeel en dat van derden;
- externe contacten en opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan;
- de toegang tot zorginformatie wordt zoveel mogelijk beperkt volgens het 'need-to-know' principe: zorgverleners kunnen enkel die informatie over cliënten raadplegen waarmee een behandelrelatie bestaat, en die ze nodig hebben om hun zorgtaken uit te voeren;
- ten aanzien van beveiligingsbeleid, -maatregelen en -voorzieningen vindt een duidelijke toewijzing en delegatie van taken, verantwoordelijkheden en bevoegdheden plaats;
- het management is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid en de handhaving van de beveiligingsmaatregelen binnen het eigen verantwoordelijkheidsgebied;
- beveiligingseisen worden bepaald door het beveiligingsbeleid en door de beoordeling van de beveiligingsrisico's en -incidenten in specifieke situaties;

4 Organisatie van informatiebeveiliging

4.1 Inleiding

Adequate informatiebeveiliging is alleen mogelijk als alle partijen, die invloed kunnen uitoefenen op de beveiliging van de gegevens binnen het zorgproces van < naam instelling > , zich van hun taken en bevoegdheden bewust zijn en voor iedereen duidelijk is wie waarvoor verantwoordelijk is. In dit hoofdstuk worden de taken, bevoegdheden en verantwoordelijkheden beschreven rondom het treffen, in stand houden en naleven van beveiligingsmaatregelen.

4.2 Beveiligingsorganisatie

Voor een adequate organisatie van de informatiebeveiliging van < naam instelling > zijn de beveiligingsverantwoordelijkheden en -taken belegd bij onderstaande functionarissen en/of organisatorische eenheden.

Raad van Bestuur (RvB)
Primaire verantwoordelijkheid: eindverantwoordelijk voor informatiebeveiliging.
Onderliggende taken:
- vaststellen en uitdragen informatiebeveiligingsbeleid;
- ter beschikking stellen van benodigde middelen voor informatiebeveiliging;
- toekennen van rollen en verantwoordelijkheden voor de informatiebeveiliging;
- evalueren gerealiseerde beveiligingsniveau.

Management (circuit-/regiomanager, afdelingshoofden en hoofden bedrijfsvoering)
Primaire verantwoordelijkheid: implementatie en handhaving van de informatiebeveiliging binnen regio/circuit.
Onderliggende taken:
- vertalen van beveiligingsrichtlijnen en –maatregelen naar organisatorische eenheid;
- toezien op naleving van beveiligingsrichtlijnen en -maatregelen;
- stimuleren van beveiligingsbewustzijn en motiveren van medewerkers;
- rapporteren over naleving en informatiebeveiligingsincidenten.

Directeur Bedrijfsvoering
Primaire verantwoordelijkheid: verantwoordelijk voor de ontwikkeling, implementatie en toetsing van het informatiebeveiligingsbeleid en -beheersmaatregelen.
De informatiebeveiligingsrol is ondergebracht bij de directeur Bedrijfsvoering/controller, die de operationalisering van de informatiebeveiliging delegeert naar de hoofden/functionarissen van de specifieke taakgebieden (Automatisering en Telecommunicatie, Facilitaire Zaken, Informatiemanagement, Personeelszaken) binnen de bedrijfsvoering.
Onderliggende taken:
- opstellen en actualiseren van het informatiebeveiligingsbeleid;
- initiëren en uitvoeren van risicoanalyses;
- coördineren van informatiebeveiliging bij lopende en nieuwe projecten;
- opstellen van criteria, normen en standaarden voor, en het coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het beveiligingsbeleid;
- volgen van nieuwe ontwikkelingen en wet- en regelgeving op het gebied van informatiebeveiliging;

- verzamelen, registreren, onderhouden en actualiseren van informatie over de aanwezige beveiligingsmaatregelen;
- advies aan directie en het management over de te nemen beveiligingsmaatregelen;
- rapporteren aan de leiding over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoek en resultaten van controles;
- stimuleren van beveiligingsbewustzijn en het (doen) opstellen, uitvoeren en onderhouden van een communicatieplan;
- coördineren van voorlichting en interne opleidingen van personeel op het gebied van informatiebeveiliging;

Intern auditteam
Primaire verantwoordelijkheid: controleert naleving van het informatiebeveiligingsbeleid.
Het auditteam bestaat uit Directeur Bedrijfsvoering, Hoofd Zorgontwikkeling en Hoofd Informatiemanagement. Op specifieke onderwerpen kan het auditteam worden aangevuld met experts op deelterreinen.
De taak, samenstelling en bevoegdheden van het auditteam zijn beschreven in het protocol '*Intern Auditteam < naam instelling >*'.
Onderliggende taken:
- door middel van interne audit toezicht houden op implementatie en naleving van beleid;
- opstellen van een controleplan;
- periodiek rapporteren van conclusies en aanbevelingen aan RvB en management (minimaal 4x per jaar).

Medewerker
Van alle medewerkers van < naam instelling > wordt verwacht dat zij op de hoogte zijn van, en de beveiligingsrichtlijnen en -maatregelen navolgen. Alle beveiligingsrichtlijnen en -maatregelen worden gecommuniceerd via en gepubliceerd op het intranet van < naam instelling > .
De hoofden bedrijfsvoering c.q. ondersteunende diensten zien toe op de naleving van beveiligingsmaatregelen door de medewerkers. Beveiligingsincidenten en ondernomen acties worden gerapporteerd via de Melding Incidenten -procedure.

Externe leverancier
Alle externe leveranciers met fysieke of logische toegang tot < naam instelling > worden geacht op de hoogte te zijn van, en de vastgestelde informatiebeveiligingsrichtlijnen en -maatregelen na te leven. De hoofden bedrijfsvoering c.q. ondersteunende diensten zien toe op de naleving van beveiligingsmaatregelen door externe leveranciers. Ook hiervoor geldt dat beveiligingsincidenten en ondernomen acties worden gerapporteerd via de Melding Incidenten -procedure.

4.3 Overige verantwoordelijkheden/rollen

4.3.1 *Managementverantwoordelijkheid*
Het management is verantwoordelijk voor de implementatie en handhaving van de informatiebeveiliging binnen de organisatorische eenheden (circuit/regio of afdeling).
In het kader van het (HKZ-)kwaliteitsmanagementsysteem van < naam instelling > is de controle en toezicht op naleving van interne procedures, aanbevelingen en veranderingen

van beleid binnen de organisatieonderdelen de taak van het interne auditteam. Het auditteam rapporteert haar bevindingen en adviezen ten aanzien van de naleving van de informatiebeveiliging aan de RvB en de circuit-/regio managers.

4.3.2 Adviesgroep Informatiebeveiliging

De permanente adviesgroep Informatiebeveiliging adviseert, toetst en bereidt besluitvorming door de RvB over het informatiebeveiligingsbeleid en de te nemen maatregelen voor. De adviesgroep bestaat uit: Bestuurssecretaris (afgevaardigde RvB), 1ste Geneeskundige, directeur Bedrijfsvoering, hoofd Facilitairmanagement, Hoofd Informatiemanagement en beleidsmedewerker Personeelszaken. De adviesgroep komt ca. 4 keer per jaar bij elkaar.

4.3.3 MIT-commissie

De door medewerkers gerapporteerde informatiebeveiligingsincidenten en ondernomen acties worden door de MIT-commissie geregistreerd en gemeld aan de Adviesgroep Informatiebeveiliging. De taak, samenstelling en bevoegdheden van de MIT-commissie zijn beschreven in het protocol '*Melding Incidenten < naam instelling>)*'. Op basis van de geaggregeerde incidenten geeft de MIT-commissie ieder half jaar een overzicht en advies aan de RvB en het management.

4.4 RACI-matrix

Binnen < naam instelling > zijn de volgende beveiligingstaken (strategisch, tactisch en operationeel niveau) toegewezen aan de volgende verantwoordelijkheidsgebieden:

Taken/Rollen	RvB	Management Bedrijfsvoering	Intern auditteam	Medewerker	Externe leverancier	Adviesgroep IB	MIT-comissie
Opstellen en actualiseren informatiebeveiligingsbeleid	A		R		I		C	
Vaststellen en bewaken van operationele maatregelen	A	I	R		I	I		
Ter beschikking stellen middelen		R						
Implementatie van maatregelen binnen circuit/afdeling	A	R	C					
Implementeren van controlestructuur en rapportages	A	C	R					
Voorlichting en communicatie richting medewerkers	A	R	R		I	I		
Deugdelijk beheer toevertrouwde informatie en bedrijfsmiddelen	A	R			R	R		
Handelen conform gedragscode en beveiligingsmaatregelen	A	R			R	R		
Melden risicovolle situaties of incidenten		A			R	R		
Naleving binnen de afdeling	A	R	R					
Vaststellen naleving informatiebeveiligingsbeleid	I		I	R				
Registratie en advies incidentmeldingen	I	I					I	R
Opleggen sancties bij overtredingen	R							

Jaarlijkse rapportage aan directie over informatiebeveiliging	I		R				I	
Evalueren informatiebeveiligingsbeleid			R				C	

Legenda:

- Responsible - **(R)** - Degene die verantwoordelijk is voor het proces en/of het resultaat (proceseigenaar);
- Accountable - **(A)** - Degene die de proceseigenaar ter verantwoording kan roepen over het resultaat;
- Consulted - **(C)** - Degene die geraadpleegd wordt vooraf: kan resultaat beïnvloeden;
- Informed - **(I)** - Degene die geïnformeerd wordt achteraf: kan resultaat niet meer beïnvloeden.

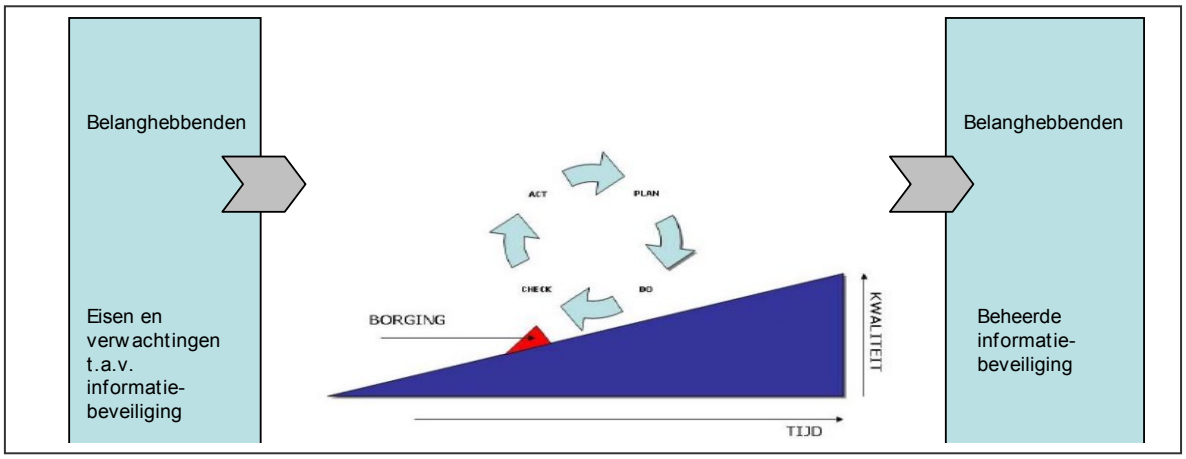
5 Management Systeem voor Informatiebeveiliging (ISMS)

5.1 Inleiding

Het Management Systeem voor Informatiebeveiliging is een geïntegreerde procesbenadering om alle ISMS-processen te structureren en tot een maximale informatieveiligheid te komen. Het systeem garandeert een systematische beheersing en verbetering van de beveiligingsprocessen. Dit hoofdstuk beschrijft het door < naam instelling > toegepaste model om de ISMS-processen te structureren.

5.2 Procesbeschrijving

Het ISMS van < naam instelling > is gebaseerd op de NEN-ISO/IEC 27001:2005 (nl) norm. In deze internationale norm wordt een procesbenadering gehanteerd voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het ISMS van een organisatie.
In de NEN-ISO norm wordt het '*Plan-Do-Check-Act*' (PDCA)-model gehanteerd om het ISMS te structureren. Figuur 1 illustreert de toepassing van het PDCA-model op de ISMS-processen. De eisen voor informatiebeveiliging en de verwachtingen van de belanghebbende partijen worden als input gebruikt, en door middel van de nodige maatregelen en processen, wordt beveiliging van informatie geboden die aan die eisen en verwachtingen voldoet.



Figuur 1 – PDCA model toegepast op ISMS-processen

Het ISMS van < naam instelling > ziet er globaal als volgt uit:

Plan (*beleidsvorming*, *het ISMS vaststellen*)	vast- en opstellen van ISMS-beleid, -doelstellingen, -processen en -procedures die relevant zijn voor het risicobeheer en verbetering van de informatiebeveiliging, om resultaten te leveren die in overeenstemming zijn met algemene beleidslijnen en doelstellingen
Do (*beleidsuitvoering*, *ISMS*	uitwerken van ISMS-beleid en -plannen,

implementeren/uitvoeren)	afspraken over meten van uitvoering en bepalen normen, uitvoeren activiteiten volgens plannen
Check (*beleidsevaluatie*, *ISMS controleren/beoordelen*)	beoordelen van procesprestaties ten opzichte van ISMS-beleid, -doelstellingen en -ervaring uit de praktijk, en rapportage van de resultaten aan de directie ter beoordeling
Act (*bijstellen/formuleren van nieuw beleid, ISMS bijhouden en verbeteren*)	corrigerende en preventieve maatregelen nemen, op basis van de resultaten van de interne ISMS-audit en de directiebeoordeling of andere relevante informatie, om het ISMS continu te verbeteren

Plan, Do, Check en Act bij < naam instelling > (P&C-cyclus)
Door < naam instelling > wordt al enkele jaren een beleidscyclus, gebaseerd op de PDCA-cyclus, toegepast. De systematische beheersing en verbetering van de beveiligingsprocessen is geïntegreerd in deze bestaande kwaliteitscyclus. De beleidscyclus wordt bij < naam instelling > de Planning & Control (P&C) cyclus genoemd. Met de P&C cyclus worden naast de financiële, dus ook alle andere beleidsterreinen bestreken: productie, personeel, organisatie, huisvestings- en facilitair beleid en informatiserings- en automatiseringsbeleid. Sinds 2009 maakt ook het informatiebeveiligingsbeleid onderdeel uit van deze beleidscyclus. Binnen de beleidscyclus van < naam instelling > zijn de uiteenlopende (Jaar-)plannen en het interne auditteam de belangrijkste instrumenten.

Het element ***Planning*** van de P&C-cyclus, kent als belangrijkste ingrediënten:
- *beleidsperspectief*
- *kaderbrief Raad van Bestuur*
- *jaarplan op instellings- , circuit-, regio-, en afdelingsniveau*
- *begroting*
- *protocollen en regelingen in het Handboek < naam instelling > of <intranet of andere interne communicatiekanalen>*
- *besluiten door de RvB al dan niet in het managementteam genomen*
- *directiebeoordeling*

Het beleidsperspectief wordt voorbereid door jaarlijks via een interne enquête ‘sleutelfiguren’ te raadplegen ten aanzien van de verschillende beleidsterreinen. Wensen en behoeften van financiers en andere externe en interne invloeden worden op deze manier ingebracht, waarna de Raad van Bestuur het beleidsdocument vaststelt. Op basis van het beleidsperspectief stellen circuits, regio’s en afdelingen jaarplannen en begrotingen op, en voeren de vastgestelde plannen uit (Jaarplansystematiek). Indien noodzakelijk kunnen onvoorziene belangrijke interne en/of externe invloeden leiden tot tussentijdse wijzigingen van het beleid en de jaarplannen.

Een ander element van de Planning is de Protocollering, zoals deze wordt vastgelegd in het voor alle medewerkers toegankelijke, digitale Handboek < naam instelling > . De wijze waarop deze normerende documenten worden ontwikkeld, opgesteld en beheerd, is uitvoerig beschreven in het Handboek zelf, te raadplegen via Con< naam instelling > , de

intranet website van < naam instelling > . Alleen door de Raad van Bestuur vastgestelde protocollen en richtlijnen halen het Handboek < naam instelling > .

Het element ***Control*** van de P&C-cyclus, kent als belangrijkste ingrediënten:
- *periodieke voortgangs rapportage (PVR)*
- *het interne auditteam*
- *check tijdens RvB- en M.T.-overleg*
- *check tijdens circuit en regio- en teamoverleggen*
- *periodieke terugkoppeling vanuit het Management Informatie Systeem waaronder kengetallen over resultaten (financieel, personeel, zorginhoudelijk)*

Om de informatiestromen binnen < naam instelling > te organiseren en de controlcyclus te faciliteren is een geprotocolleerd rapportagesysteem ontworpen, de periodieke voortgangsrapportage (PVR). Hiervoor wordt 'harde' informatie uit het management informatie systeem (MIS) samengevat in een Prestatiemeter. Deze informatie wordt aangevuld met de bevindingen van het auditteam, zijnde de belangrijkste geconstateerde afwijkingen ten opzichte van de gemaakte beleids- en werkafspraken. Het interne auditteam voert hiertoe periodiek gesprekken met de verantwoordelijke managers. Hierin worden de bereikte resultaten en de voortgang in de uitvoering van de (jaar-)plannen en andere afspraken besproken en getoetst. Ieder jaar wordt een auditplanning, inclusief specifieke aandachtspunten opgesteld. Aan de agenda van het auditteam zijn vanaf 2009 specifieke informatiebeveiligingsaspecten toegevoegd.

De verantwoordelijke circuit- en regiomanagers en directeur Bedrijfsvoering rapporteren 2-maandelijks aan de Raad van Bestuur de in- en externe highlights en analyseren en duiden de door het auditteam geconstateerde afwijkingen. Op basis hiervan worden vervolgafspraken gemaakt met de managers om bij te sturen op afwijkingen, die vorm krijgen in verbeterplannen. Bereikte resultaten, gevolgde werkwijze en planning worden geëvalueerd. Leerpunten en nieuwe doelen voor de volgende interne audit worden opgesteld. Daarmee krijgt niet alleen het element "check" aandacht, maar ook de elementen "plan", "do" en "act".

In- en externe actoren en factoren
Het kwaliteitsmanagementsysteem van < naam instelling > is géén gesloten systeem. Bij de opstelling van plannen en bij het verdere verloop van de P&C cyclus middels periodieke audits worden op systematische wijze interne en externe invloeden betrokken (o.a. markt- en effectonderzoek). < naam instelling > neemt deel aan tal van samenwerkingsverbanden, ondervindt toetsing door haar financiers en door meerdere toezichthoudende instanties en is onderhevig aan overvloedige wet- en regelgeving. Specifieke ontwikkelingen op het gebied van de informatiebeveiliging worden vanuit de Adviesgroep Informatiebeveiliging gevolgd, en zonodig in de beleidsvorming en -uitvoering verwerkt.
Een belangrijke 'trechtering' van externe invloeden wordt ook gevormd door de certificering conform het Harmonisatiemodel Kwaliteitstoetsing Zorgsector (HKZ) en de NEN-ISO/IEC 27001. Door middel van certificatieonderzoek en het op certificering aansluitende herhalingsonderzoek verzekert < naam instelling > zich van een permanente vorm van externe toetsing. Aanbevelingen uit (pre)certificatieonderzoek worden rechtstreeks vertaald naar nieuwe (jaar-)plannen en zonodig meerjarenbeleid.
Gedurende het jaar is het eerder regel dan uitzondering, dat actuele ontwikkelingen worden ingevlochten in de interne auditgesprekken en de overleggen van het managementteam.

Afspraken die over het inspelen op dergelijke ontwikkelingen worden gemaakt, worden net als het reguliere beleid gemonitored door het auditteam in het kader van de Planning & Control.

P&C Cyclus: de directiebeoordeling
De directiebeoordeling is de jaarlijkse evaluatie of beoordeling van het kwaliteitsmanagementsysteem. Als input voor deze beoordeling worden minimaal de volgende elementen ingebracht:

- *analyse van de uitkomsten van de Prestatiemeter. De prestatiemeter is het geheel van prestatie-indicatoren die in hun samenhang door de Raad van Bestuur maatgevend worden geacht voor de kwaliteit van < naam instelling > . In de reguliere beleidscyclus worden deze indicatoren telkens voorzien van normwaarden. De prestatiemeter wordt bij elke directiebeoordeling geëvalueerd;*
- *de periodieke verslaglegging van het interne auditteam;*
- *klachten, incidenten en gedwongen ontslagen;*
- *resultaten medewerkerstevredenheidsonderzoek;*
- *de verslaglegging van het externe auditteam in het kader van de follow up van het HKZ-certificatieonderzoek;*
- *de procedures voor corrigerende en preventieve maatregelen. Een corrigerende maatregel is gericht op het wegnemen van de oorzaak van een geconstateerde afwijking. Een preventieve maatregel probeert bij voorbaat een oorzaak van een mogelijk toekomstig probleem weg te nemen;*
- *interne en externe veranderingen die van invloed kunnen zijn op het kwaliteitsmanagementsysteem.*

< naam instelling > meent met het toegepaste kwaliteitsmanagementsysteem (P&C-cyclus) een geïntegreerde procesbenadering te hebben waarmee alle zorg- en ondersteunende processen, inclusief de informatiebeveiligingsprocessen, systematisch worden beheerst en verbetert.

6 Risicomanagement

6.1 Inleiding

Beveiligingsrisico's met betrekking tot informatie en de ondersteunende processen, systemen en netwerken moeten structureel worden onderzocht. Op deze manier wordt inzicht verkregen in de actuele en specifieke risico's en kunnen bewust keuzes worden gemaakt over de te nemen maatregelen.
In dit hoofdstuk wordt het raamwerk en de door < naam instelling > gevolgde onderzoeksmethode voor risicoanalyse beschreven.

6.2 Doelstelling risicoanalyse

De risicoanalyse beoordeelt op een systematische wijze de schade als gevolg van het optreden van een bedreiging voor < naam instelling > en de waarschijnlijkheid dat een dergelijke bedreiging zich voordoet. Hierbij wordt rekening gehouden met de gevolgen voor de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatievoorziening in het licht van de aanwezige bedreigingen.

Het ISMS heeft als doel het, op basis van een beoordeling van bedrijfsrisico's, vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging. Een belangrijk onderdeel van het management systeem is de risicoanalyse.

Wat is het doel van een risicoanalyse?
- inzicht te krijgen in (mogelijke) risico's en gevolgen van incidenten op de bedrijfsvoering;
- inzicht te krijgen in de kans op bedreigingen en kwetsbaarheden;
- bewust keuzes te maken over hoe om te gaan met risico's (accepteren, vermijden, overdragen of
  verminderen);
- inzicht, beleid en maatregelen actueel te houden.

6.3 Risicoanalyse raamwerk

Voor de inventarisatie van risico's maakt < naam instelling > gebruik van de SPARK-methode[3]. De methode is een gestructureerd instrument om de risico's met betrekking tot informatie en de ondersteunende processen, systemen en netwerken te onderzoeken. De methode is eveneens een hulpmiddel bij het selecteren van passende beveiligingsmaatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en bedrijfsvoering te garanderen.

De SPARK-methode bestaat uit 4 fasen. In *fase 1* wordt de impact op bedrijfsprocessen en hieraan
gerelateerde informatiesystemen van de consequentie van het verliezen van informatie (in termen van

[3] SPARK: Simplified Process for Analyzing Risks by KPMG

beschikbaarheid, integriteit en vertrouwelijkheid) bepaald. Op basis van deze inventarisatie wordt het
informatiesysteem geclassificeerd. Voor systemen met een middelhoog en hoog ingeschat risico wordt verdergegaan met *fase 2*. In deze fase worden de bedreigingen en kwetsbaarheden door middel van vragenlijsten geïnventariseerd en onderzocht.
Op basis van de relevante bedreigingen worden in *fase 3* beveiligingsmaatregelen geselecteerd. Bij deze selectie wordt gebruik gemaakt van referentiemaatregelen. Hierdoor zijn concrete aanknopingspunten voorhanden voor het treffen van passende beveiligingsmaatregelen.
In de laatste, 4e fase wordt periodiek geëvalueerd in hoeverre de risicobeoordeling, impactanalyse en beveiligingsmaatregelen actueel en juist zijn.

De door < naam instelling > gehanteerde SPARK-methode is schematisch weergegeven in figuur 2. De ononderbroken pijlen in de figuur geven de vereiste vervolgstappen aan en de onderbroken pijlen de mogelijke vervolgstappen. Voor laag-risicosystemen wordt geen verdere risicoanalyse uitgevoerd.

6.4 Risicoanalyse

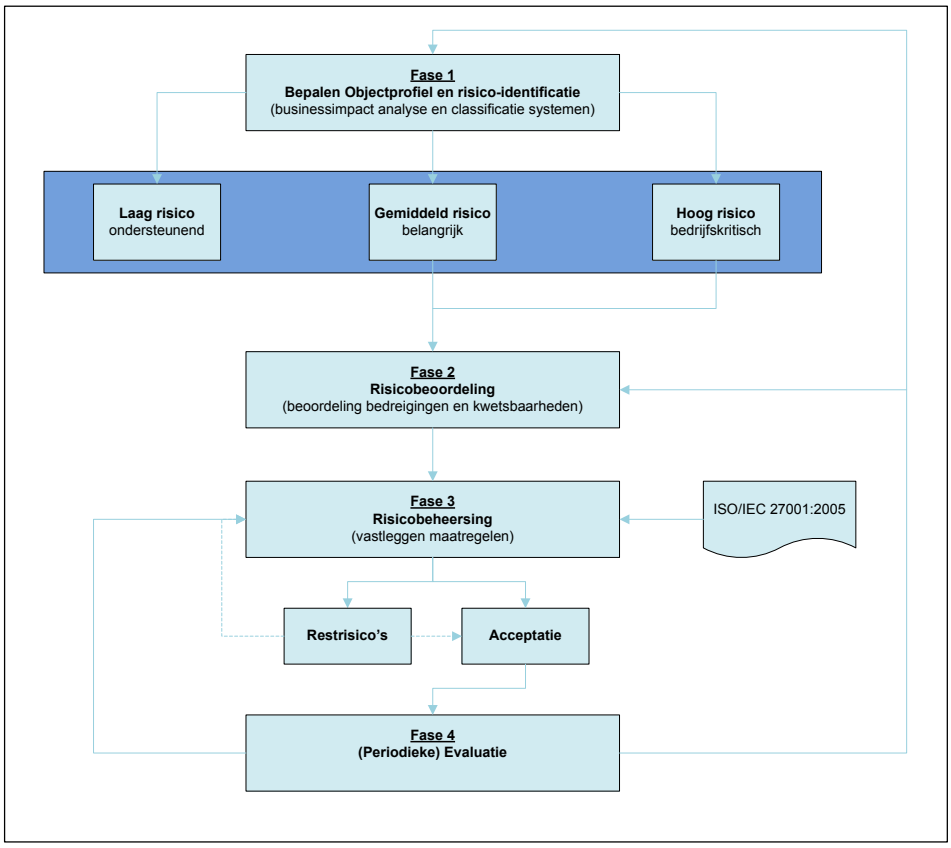
Onderstaand worden de 4 fasen binnen het proces van risicoanalyse zoals toegepast bij < naam instelling > uitgebreid beschreven.

Fase 1:
In deze fase wordt het objectprofiel en de risico-identificatie bepaald. Voor de geautomatiseerde systemen (i.c. User, Exact, SDB, telefonie) zijn aan medewerkers van de diverse (zorg-)disciplines vragen gesteld om helder te krijgen *hoe* afhankelijk het zorgproces is van deze geautomatiseerde systemen. De vragen zijn gericht op de drie kwaliteitskenmerken van informatie:
- beschikbaarheid (gevolgen als een systeem langer dan een week niet beschikbaar is);
- integriteit (gevolgen van foutieve invoer of ongeautoriseerde invoer);
- vertrouwelijkheid (gevolgen van openbaarmaking van informatie).

De impact van de geautomatiseerde systemen wordt ingeschat op basis van de antwoordmogelijkheden:
- voortbestaan in gevaar (*catastrofaal*)
- serieuze schade (*ernstig*)
- significante schade (*matig*)
- beperkte schade (*gering*)
- verwaarloosbare schade (*onbelangrijk*)

Om de mate van impact te bepalen zijn de criteria omschreven in Bijlage 3: *Indeling impact*

Op basis van de uitkomsten kunnen de systemen worden geclassificeerd:
- *hoog*: het systeem is kritiek voor de bedrijfsvoering;
- *medium*: het systeem is belangrijk voor de administratieve bedrijfsvoering;
- *laag*: het systeem is ondersteunend aan de bedrijfsvoering.



Figuur 2 – schema risicoanalyse (SPARK-methode)

Fase 2:

In deze fase vindt de risicobeoordeling plaats. Voor de verschillende systemen wordt middels het beantwoorden van een aantal vragen door medewerkers uit de diverse bedrijfsonderdelen bepaald wat de afhankelijkheden en kwetsbaarheden zijn van deze systemen. Hierdoor wordt de kans bepaald dat bepaalde bedreigingen zich voordoen. De vragen gaan over drie kwaliteitskenmerken van informatie: beschikbaarheid, integriteit en vertrouwelijkheid.

- *beschikbaarheid*
  - kans op een ernstige calamiteit
  - kans op een systeemstoring
  - kans op verstoring van bedrijfsprocessen
  - kans op onacceptabele verlaging van systeemperformance
  - kans op een denial-of-service
  - kans op aantasting door kwaadaardige code/scripts
- *integriteit*
  - kans op invoerfouten door gebruikers
  - kans op bedieningsfouten door onkundige medewerkers
  - kans op ongeautoriseerd gebruik
  - kans op ongeautoriseerde wijziging van bestanden
  - kans op aantasting door spoofing
  - kans op ongeautoriseerde wijziging berichtenverkeer
- *vertrouwelijkheid*

- kans dat onbevoegde inzicht in print-outs en informatie
- kans van verstrekken gevoelige informatie aan onbevoegden
- kans op ongeautoriseerde fysieke toegang
- kans op ongeautoriseerde logische toegang
- kans op afluisteren berichtenverkeer
- kans op in verkeerde handen vallen berichtenverkeer

Bij de beantwoording van de vragen wordt rekening gehouden met een 'worst-case scenario'. De gestelde vragen naar de mate van risicobeoordeling worden beantwoord met:
- waarschijnlijk
- zeer goed mogelijk
- mogelijk
- onwaarschijnlijk
- onmogelijk.

Fase 3:
In deze fase zijn op basis van de uitkomsten van fase 1 en fase 2 de te treffen maatregelen bepaald. Op basis van de classificatie van de impact van het systeem op de bedrijfsvoering van < naam instelling > , gekoppeld aan de kwetsbaarheid van het systeem voor bepaalde bedreigingen worden passende beveiligingsmaatregelen getroffen. Door gebruik te maken van vragenformulieren wordt op systematische wijze een oordeel gevormd over de belangrijkste beveiligingsonderwerpen. Om deze gestructureerdheid ook bij de selectie van maatregelen tot uitdrukking te brengen, maakt SPARK gebruik van de Code voor Informatiebeveiliging. SPARK biedt hiermee ondersteuning bij de classificatie van informatiesystemen, de analyse van risico's, de keuze van te implementeren maatregelen en een automatische koppeling van maatregelen aan risico's.
De relevante en toepasbare beheersdoelstellingen en -maatregelen zijn vervolgens gedocumenteerd in de Verklaring van Toepasselijkheid. Naast de uitkomsten van de risicoanalyse wordt de relevantie van de beheersdoelstellingen getoetst aan het beleidskader en de geldende wet- en regelgeving.

Fase 4:
In de laatste fase wordt geëvalueerd in hoeverre de risicobeoordeling en impactanalyse actueel en juist zijn. Jaarlijks stelt < naam instelling > vast in hoeverre de maatregelen de risico's (nog) afdoende afdekken. De geregistreerde incidentmeldingen, interne audits, gesignaleerde externe ontwikkelingen vanuit de de Adviesgroep Informatiebeveiliging en de periodieke managementrapportage vormen een belangrijke bron van informatie om de veiligheidsrisico's te volgen, en zonodig opnieuw te beoordelen. Naast een periodieke evaluatie van de risicoanalyse gebeurt dit ook tussentijds in het geval van veranderingen.

Bijlage 1 **Termen en definities**

Bedrijfsmiddel	alle middelen die noodzakelijk zijn om de dienstverlening van < naam instelling > richting cliënten te kunnen garanderen
Beschikbaarheid	zekerstellen dat gegevens en informatiediensten op de gewenste momenten beschikbaar zijn voor gebruikers
Informatiebeveiliging	samenhangend stelsel van organisatorische en technische maatregelen, in de juiste kosten/nut verhouding, om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade als gevolg van desondanks optredende verstoringen te beperken. Naast vertrouwelijkheid, integriteit en beschikbaarheid van informatie kunnen ook andere eigenschappen, zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid een rol spelen
Informatiebeveiligingsgebeurtenis	vastgestelde status van een systeem, dienst of netwerk die duidt op een mogelijke overtreding van het beleid voor informatiebeveiliging of een falen van beveiligingsvoorzieningen, of een tot dan toe onbekende situatie die relevant kan zijn voor beveiliging
Informatiebeveiligingsincident	afzonderlijke gebeurtenis of een serie ongewenste of onverwachte informatiebeveiligingsgebeurtenissen waarvan het waarschijnlijk is dat ze nadelige gevolgen voor de bedrijfsvoering hebben en een bedreiging vormen voor de informatiebeveiliging
Informatievoorziening	geheel van informatiesystemen dat tot doel heeft te voorzien in de informatiebehoefte van een organisatie
Integriteit	het waarborgen dat gegevens niet ongecontroleerd worden gewijzigd of verloren gaan
Management systeem voor	dat deel van een managementsysteem dat

informatiebeveiliging (ISMS)	op basis van een beoordeling van bedrijfsrisico's, tot doel heeft het vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging
Overblijvende risico's	overblijvend risico na risicobehandeling
Risicoaanvaarding	besluit een risico te aanvaarden
Risicoanalyse	systematisch gebruik van informatie om bronnen te identificeren en de risico's in te schatten
Risicobehandeling	proces van keuze en implementatie van maatregelen om risico's te verlagen
Risicobeheer	gecoördineerde activiteiten om een organisatie sturing te geven en te bewaken met betrekking tot risico's
Risicobeoordeling	algeheel proces van risicoanalyse en risico-evaluatie
Risico-evaluatie	proces waarin het ingeschatte risico wordt afgewogen tegen vastgestelde risicocriteria om te bepalen in welke mate het risico significant is
Verklaring van Toepasselijkheid (VvT)	gedocumenteerde verklaring die de beheersdoelstellingen en beheersmaatregelen beschrijft die relevant en toepasbaar zijn op het ISMS van de organisatie.
Vertrouwelijkheid	het beschermen van gegevens tegen onbevoegde kennisname

Bijlage 2 **Verklaring van Toepasselijkheid**

Verklaring van Toepasselijkheid

De Raad van Bestuur van <naam instelling> zet in op het voor < * > voldoen aan de NEN-ISO/IEC 27001:2005 (nl) norm voor informatiebeveiliging vanuit het bewustzijn, dat ICT en zorg onlosmakelijk met elkaar verweven zijn geraakt. Zorgverlening is niet langer denkbaar zonder ICT en goede zorgverlening kan niet meer zonder informatieverkeer en informatievoorzieningen die adequaat beveiligd zijn.

Eind 2008 is < naam instelling > gestart met toetsing van het bestaande kwaliteitsmanagementsysteem vanuit de optiek van risicomanagement. Op deze wijze zijn en worden op systematische wijze en op alle beleidsterreinen risico's in kaart gebracht, die voorheen mogelijk onderbelicht waren. Eén daarvan is het cluster van risico's dat samenhangt met de voor de zorgverlening benodigde adequate, vertrouwelijke en betrouwbare informatie. Hoewel de informatiebeveiligingsmaatregelen bij < naam instelling > grosso modo gelijke tred hebben gehouden met de kwantitatieve en kwalitatieve uitbreiding van de ICT door de jaren heen, is systematische borging ervan door middel van het informatiebeveiligingssysteem door de Raad van Bestuur hoog op de agenda gezet.

Informatiebeveiliging is een verantwoordelijkheid voor de gehele organisatie van < naam instelling > , waarbij de algehele eindverantwoordelijkheid berust bij de Raad van Bestuur van < naam instelling > . De wijze waarop < naam instelling > met zijn informatiebeveiligingssysteem toewerkt naar certificering is vastgelegd in het document **Management Systeem voor Informatiebeveiliging** van juni 2012.

*
Bestuurder

Datum: …….

Plaats: ……

Bijlage 3 **Indeling impact**

Klasse	*Omschrijving*
Catastrofaal (A)	- onvermogen om afgesproken zorgverlening < naam instelling > voor zeer lange tijd te continueren - treft een zeer groot gedeelte van de business (meer dan 60%) - heeft zeer grote impact op de beschikbaarheid/vertrouwelijkheid/ integriteit van informatie en/of informatiesystemen - erkenning < naam instelling > wordt ingetrokken door ministerie VWS (CIBG) - oplegging van handhavingsmaatregel door Inspektie voor de Gezondheidszorg (IGZ) - negatieve externe publiciteit voor < naam instelling > - financiële schade < naam instelling > is > 250.000 euro per dag
Ernstig (B)	- onvermogen om afgesproken zorgverlening < naam instelling > voor langere tijd te continueren - treft een groot gedeelte van de business (20% - 60%) - heeft grote impact op de beschikbaarheid/vertrouwelijkheid/integriteit van informatie en/of informatiesystemen - erkenning < naam instelling > wordt tijdelijk ingetrokken door CIBG - plaatsing van < naam instelling > onder (verscherpt) toezicht door IGZ - negatieve interne publiciteit voor < naam instelling > - financiële schade voor < naam instelling > is tussen de 50.000 euro en 250.000 euro per dag
Matig (C)	- tijdelijke verstoring dienstverlening die buiten de afgesproken te leveren zorg of buiten de verwachtingen van de business valt - heeft beperkte impact op de beschikbaarheid / vertrouwelijkheid / integriteit van informatie en/of informatiesystemen - < naam instelling > krijgt een waarschuwing van VWS (CIBG) m.b.t. de erkenning - treft een beperkt gedeelte van de business (minder dan 20%) - negatieve interne publiciteit beperkt voor < naam instelling >

	- financiële schade voor < naam instelling > is tussen de 10.000 euro en 50.000 euro per dag
Gering (D)	- verstoring van de dienstverlening valt binnen de afgesproken service levels of binnen de verwachtingen van de business - treft een zeer beperkt gedeelte van de business (meerdere eindgebruikers) - heeft nauwelijks impact op de beschikbaarheid/vertrouwelijkheid/ integriteit van informatie en/of informatiesystemen - financiële schade voor < naam instelling > is tussen de 1.000 euro en 10.000 euro per dag
Onbelangrijk (E)	- incidenten, met kleine impact op één of enkele eindgebruikers - geringe financiële schade (< 1.000 euro per dag)