Procesnaam	Informatiebeveiligingsbeleid
Onderdeel van (hoofd)proces	(be)sturend proces > Intern beleid kwaliteit van zorg en veiligheid
Document (proces) eigenaar	Hendrikx H., Geneesheer Directeur
Document beheerder	Beheer handboek kwaliteit
Schrijver van het document	Huygens Tholen V., Adviseur diff. Adviseur A, Zi, Zo, KV, VG
Status van het document	Schrijven
Versie	1
Beleidsthema/ interne beleidsregel	
Ingangsdatum	18 april 2016
Einddatum	7 maart 2018
Trefwoorden/zoektermen	informatiebeveiligingsbeleid, informatie, beveiliging, informatiebeveiliging

Informatiebeveiligingsbeleid Vincent van Gogh

Inhoud

1.0 Inleiding en context

Voor u ligt het beleidsdocument informatiebeveiliging van Vincent van Gogh voor GGZ. Als zorginstelling is Vincent van Gogh verantwoordelijk voor patiëntenzorg. Het leveren van kwaliteit staat bij het uitvoeren van deze taak voorop. Om deze kwaliteit aan de patiënten en andere betrokkenen te kunnen bieden, is een betrouwbare informatievoorziening essentieel. De betrouwbaarheid van de informatievoorziening moet zijn gewaarborgd ongeacht de vorm, dus zowel handmatig, bijvoorbeeld in de patiëntenstatus en ontslagbrieven, als geautomatiseerd, denk aan het gebruik van het elektronisch patiëntendossier, internet, eHealth en e-mail. Uitgebreide aandacht voor de beveiliging van de opslag, verwerking en uitwisseling van informatie is continu vereist.
Dit beleid is gebaseerd op en volgt relevante wet- en regelgeving in de zorg (o.a. NEN 7510, WBP, WGBO, Wet op datalekken).

Niet vrijblijvend…
Voor een effectieve informatiebeveiliging is de medewerking van alle medewerkers en zorgverleners vereist. Een goede informatiebeveiliging is een verplichting voor iedereen. Het onderhavige document vormt een basis voor communicatie naar de medewerkers toe en geeft aan welk informatiebeveiligingsbeleid Vincent van Gogh wenst te voeren.

2.0 Belanghebbenden

Het informatiebeveiligingsbeleid is van toepassing op alle geledingen en vestigingen van Vincent van Gogh en op de gegevensuitwisseling binnen Vincent van Gogh en met andere organisaties.

Het informatiebeveiligingsbeleid is van toepassing op/richt zich op alle medewerkers van Vincent van Gogh, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

- Alle interne en externe partijen die in opdracht van Vincent van Gogh bemoeienis hebben met dataverwerking, databeheer en of dataopslag.
- Alle door Vincent van Gogh ingehuurde leveranciers, bureaus en of medewerkers niet in loondienst.

3.0 Beleid

3.1 Doelstelling informatiebeveiligingsbeleid:

Het doel van informatiebeveiligingsbeleid is het waarborgen van de beschikbaarheid, exclusiviteit en integriteit van de informatievoorziening binnen de zorg- en ondersteunende processen/diensten.
Het beleid vormt de leidraad voor alle betrokkenen bij informatiebeveiliging binnen Vincent van Gogh.

3.2 Waarom dit beleid?

Vincent van Gogh streeft naar het leveren van veilige en steeds betere zorg. Dit doen we door onder andere opvolging en uitvoering te geven aan professionele standaarden, externe wet- en regelgeving van overheid en branche- of belangenorganisaties en interne regels en afspraken (compliance).
Compliance moet vooral leiden tot betere en veiligere zorg en heeft ook een duidelijke relatie met risicobeheersing op de verschillende resultaatgebieden van onze organisatie. Een toename van onder andere digitale informatieverwerking, mogelijke risico's inbreuk, verlies van informatie, wijziging in relevante wet- en regelgeving voor de zorg vormen een noodzaak voor het opstellen van informatiebeveiligingsbeleid.

3.3 Hoe wordt vorm gegeven aan het beleid?

- Uitgangspunten voor ons informatieveiligheidsbeleid:
- Informatiebeveiliging is voorwaarde scheppend voor veilige informatie-uitwisseling, verwerking en opslag van onder andere zorggegevens.
- De zorg mag door informatiebeveiliging niet onnodig verstoord worden.
- De kosten van beveiligingsmaatregelen zijn:
  - in balans met de waarde van de te beschermen informatie en informatieverwerking.
  - in balans met de risico's waartegen ze beschermen.
- Ons informatieveiligheidsbeleid richt zich op de volgende aspecten:
- Mens (medewerker)
  Iedere medewerker van Vincent van Gogh is bewust van zijn/haar verantwoordelijkheid voor het nemen en uitvoeren van passende maatregelen binnen de gestelde informatiebeveiligingskaders.
- Organisatie
  Vincent van Gogh voorziet in een organisatie waarmee invulling en uitvoering gegeven wordt aan het informatieveiligheidsbeleid.
  Iedere informatieverwerkingstoepassing ten behoeve van zorgprocessen en ondersteunende diensten heeft een verantwoordelijk eigenaar.
  We werken voor iedere informatieverwerkingstoepassing met een test- en operationele omgeving die van elkaar zijn gescheiden.
- Techniek
  Techniek wordt zowel binnen als ook buiten Vincent van Gogh voor GGZ (uitbesteden door externe partners) beheerd, onderhouden en uitgevoerd.

Met onze externe partners waar Vincent van Gogh voor GGZ afspraken mee heeft in het kader van gegevensverwerking stellen wij Service Level Agreements (SLA) op waarin de veiligheidseisen, zoals Vincent van Gogh voor GGZ deze heeft vastgesteld, worden geborgd.

3.4 Wat levert het beleid op?

Mens (medewerker)

- Medewerkers van Vincent van Gogh zijn zich bewust van het veilig (be)handelen van informatie en tonen dit in de wijze waarop zij met informatie omgaan.
- Er is een Vincent van Gogh gedragscode afgeleid van het informatieveiligheidsbeleid.

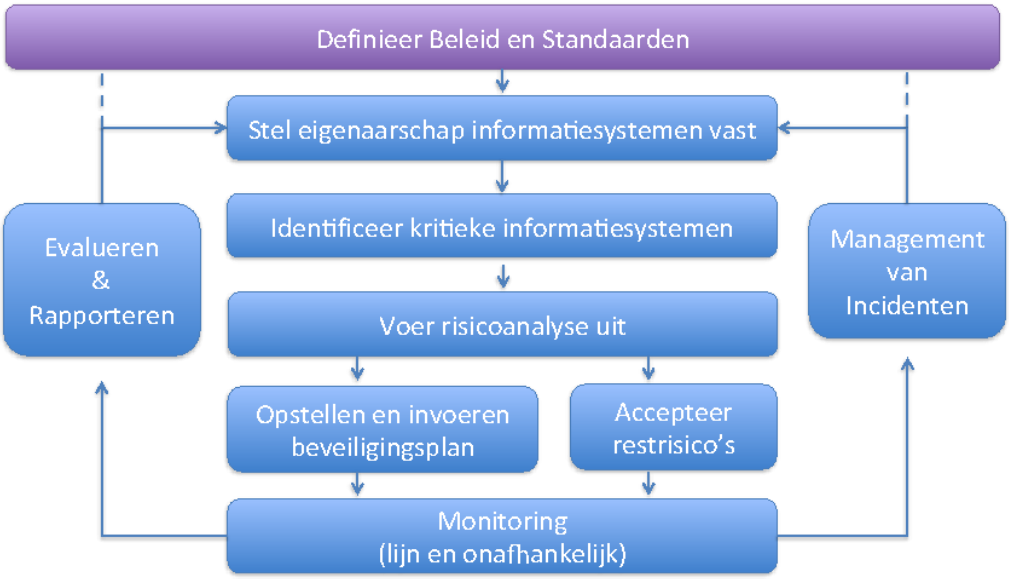
Organisatie

- Er is een functionaris / medewer**ker verantwoordelijk voor de coördinatie van informatiebeveiliging binnen Vincent** van Gogh.
- Er is een mogelijkheid om op te schalen naar een hogere hiërarchisch verantwoordelijke***.***
- De opzet, het bestaan en de verwerking van de informatiebeveiligingsmaatregelen worden periodiek geaudit.
- Overtredingen van de informatiebeveiligingsmaatregelen door de medewerkers en of derden worden getoetst en indien nodig worden passende maatregelen getroffen.
- Vincent van Gogh meldt datalekken binnen 72 uur bij de Autoriteit Persoonsgegevens.
- De opzet, het bestaan en de verwerking van de informatiebeveiligingsmaatregelen worden periodiek geëvalueerd***.***
- Aandacht voor informatiebeveiliging bij ontwikkeling, innovatie en beheer van informatiesystemen (verplichte toepassing van een Privacy Impact Assessment (PIA)***)***.

Techniek

- Met alle contractuele partners in het kader van gegevensverwerking is een verplichte verwerkersovereenkomst.
- Er is een mechanisme om beveiligingsincidenten te rapporteren en af te handelen**.**
- Binnen Vincent van Gogh wordt uitsluitend legale software en hardware gebruikt.
- Binnen Vincent van Gogh wordt alleen gebruik gemaakt van software en hardware die de bedrijfsprocessen ondersteunen.
- Technische applicaties gericht op verwerken en opslag van informatie voldoen aan de door Vincent van Gogh vastgestelde eisen voor informatieveiligheid.
- Iedereen die gebruik maakt van systemen van Vincent van Gogh is uniek identificeerbaar.
- De techniek ondersteunt het informatieveiligheidsbeleid.

4.0 Proces van informatiebeveiliging:



Nr.	Stap	Actie	Eigenaar	Wanneer
1	Definiëren van beleid en standaarden	Ontwikkelen, opstellen en vaststellen van VvG-informatieveiligheidsbeleid	Geneesheer Directeur	April 2016
2	Vaststellen van eigenaarschap informatiesystemen	Inventariseren van informatiesystemen en beleggen van eigenaarschap • Proceseigenaar • Systeemeigenaar • Infrastructuureigenaar	Manager Shared Service Center & Geneesheer Directeur	Juni 2016
3	Identificeren van kritieke informatiesystemen	Identificeren en vaststellen van kritieke informatiesysteem	Informatiesysteemeigenaren, manager Shared Service Center & Geneesheer Directeur	Juli 2016
4, 5 en 6	Uitvoeren van risicoanalyse	Risico's identificeren, analyseren en opstellen van contingency plan	Informatiesysteemeigenaren	Oktober 2016
7	Monitoring	Auditen op uitvoering geven aan informatie-veiligheidsbeleid en contingency plan	Geneesheer directeur en adviseur Kwaliteit&Veiligheid	Jaarlijks aan te vangen per 1 jan. 2017
7	Monitoring	Verzamelen van informatieveiligheids-incidentmeldingen	Geneesheer directeur	Op basis van melding
8	Evalueren en Rapporteren	Reflecteren op en analyseren van monitoringsresultaten en aanbieden van rapportage aan bestuursteam	Geneesheer directeur	2 maal per jaar
9	Management van incidenten	Opvolging geven aan informatieveiligheids-incidenten (procedure melden datalek)	Geneesheer Directeur	Op basis van melding

4.1 Organisatie informatiebeveiliging Vincent van Gogh voor GGZ:

Uitgangspunten voor de organisatie van informatiebeveiliging:

- De toewijzing van taken, verantwoordelijkheden en bevoegdheden vindt zodanig plaats dat er voorkomen wordt dat er zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingsmaatregelen achterwege blijft.

De onderstaande tabel is een onderverdeling in activiteiten en verantwoordelijkheden met betrekking tot informatiebeveiliging.

Niveau	Activiteit	Verantwoordelijk
Strategisch	Beleidsvorming	Raad van Bestuur
Tactisch	Planning	Management
Operationeel	Uitvoering	Zelfsturende teams

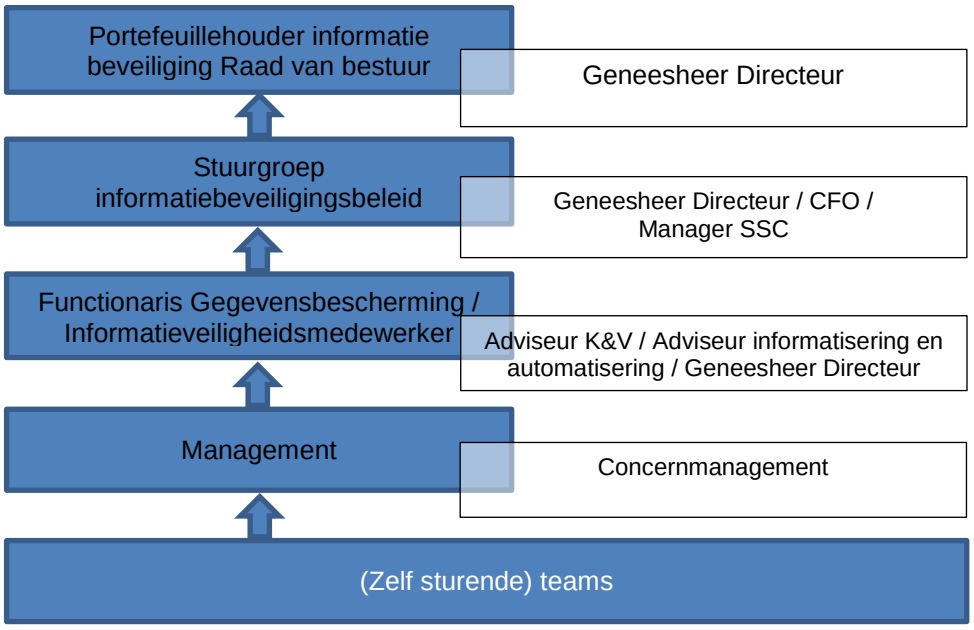
Binnen Vincent van Gogh voor GGZ is de informatiebeveiliging gekoppeld aan rollen en functies in de organisatie. Hierbij wordt onderscheid gemaakt in de onderstaande rollen:

- **Portefeuillehouder informatiebeveiliging Raad van Bestuur**
  De Raad van Bestuur is eindverantwoordelijk voor alle activiteiten binnen Vincent van Gogh en hiermee dus ook voor de informatiebeveiliging. De verantwoordelijkheden omvatten:
  - Vaststellen van informatiebeveiligingsbeleid en daaruit voortvloeiende richtlijnen
  - Toezien op naleving van informatiebeveiligingsbeleid
  - Het evalueren van informatiebeveiligingsbeleid.
- **Stuurgroep informatiebeveiligingsbeleid**
  De stuurgroep adviseert de Raad van Bestuur met betrekking tot informatiebeveiliging. De stuurgroep is verantwoordelijk voor de activiteiten, ondersteuning en bewaking van de realisatie en naleving van het informatiebeveiligingsbeleid en de daarbij behorende richtlijnen, procedures.
- **Functionaris Gegevensbescherming / Informatieveiligheidsmedewerker**
  Deze medewerker is op operationeel niveau verantwoordelijk voor:
  - Aanspreekpunt inzake informatiebeveiliging;
  - het beheer van het instellingsbrede informatiebeveiligingsbeleid en hieruit voortvloeiende richtlijnen en procedures;
  - het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij management, medewerkers en derden betrokken bij gegevensverwerking;
  - het adviseren van de stuurgroep, management en andere leidinggevenden over informatiebeveiliging bij ontwikkeling, innovatie en beheer van informatiesystemen;
  - het adviseren over de te nemen preventieve en herstelacties bij beveiligingsincidenten;
  - het informeren en instrueren van de direct betrokkenen over de uit te voeren preventieve- en herstelacties;
  - het centraal informeren van gebruikers over potentiële beveiligingsincidenten;
  - uitvoeren van een Privacy Impact Assessment.

- **Management**
  De verantwoordelijkheden van het management omvat onder andere de volgende zaken:

  Kaderstellend:
  - Positieve en actieve houding ten aanzien van informatiebeveiliging.
  - Naleving en uitdragen van informatiebeveiligingsmaatregelen.
  - Faciliteren van het Computer Emergency Response Team (CERT)
    Het Computer Emergency Response Team is verantwoordelijk voor:
  - Directe respons bij computer (ICT) calamiteiten met verhoogd risico voor informatieverlies (datalek);
  - Audit: **Informatiebeveiliging is een vast onderdeel in de jaarlijkse uit te voeren interne** audits, waarbij aandacht uit dient te gaan naar naleving en borging van informatiebeveiligingsbeleid.

  Operationaliseren:
  - Diverse overlegvormen;
    Voor overleg, coördinatie en afstemming op gebied van informatiebeveiliging zijn diverse overlegvormen belegd. In deze overlegmomenten worden ontwikkelingen, activiteiten, incidenten enz. met betrekking tot informatiebeveiliging besproken;
  - Controle en rapportage via P&C-cyclus (operationele controle op naleving van informatiebeveiligingsbeleid);
  - Aandacht in werkoverleg (het organiseren en coördineren van de evaluatie en afhandeling van beveiligingsincidenten);
  - Het verzamelen, analyseren, beoordelen en registreren van informatie over potentiële ICT-beveiligingsincidenten en beveiligingslekken.



4.2 Identificeren van kritieke informatiesystemen:

Voor welke processen en onderliggende informatiesystemen moet een risicoanalyse worden uitgevoerd. De beveiligingseisen aan het bedrijfsproces en onderliggende applicaties worden geïnventariseerd met behulp van onderstaande tabel;

Betrouwbaarheidseis	Geen criterium	Wenselijk	Belangrijk	Essentieel
Beschikbaarheid	Er hoeven geen garanties te worden gehaald	Een enkele keer uitval is aanvaardbaar	Nauwelijks uitval gedurende de openingstijden	Slechts in uitzonderlijke gevallen niet operationeel
Vertrouwelijkheid	Gegevens hoeven niet te worden afgeschermd	Gegevens uitsluitend ter inzage voor een bepaalde groep	Gegevens uitsluitend toegankelijk voor direct betrokkenen	Bedrijfsbelangen worden ernstig geschaad indien niet ge-autoriseerden toegang krijgen
Integriteit	Geen extra integriteitsbescherming	Bedrijfsproces tolereert enkele fouten	Een zeer beperkt aantal fouten is toegestaan	Bedrijfsproces eist foutloze informatie

Gedetailleerde kennis van de bedrijfsprocessen en de onderliggende informatiesystemen is essentieel, overwegingen en toelichting op keuzes bij afwijkende eisen worden per informatiesysteem vastgelegd, hierbij rekening houdend met de eisen aan de processen en het belang van informatiesystemen voor die processen, wordt vastgesteld welke betrouwbaarheidseisen moeten worden gesteld ten aanzien van:

Beschikbaarheid:	De mate waarin informatie en informatiesystemen op de juiste momenten beschikbaar zijn voor gebruikers.
Integriteit	De mate waarin de juistheid en volledigheid van informatie is gewaarborgd.
Vertrouwelijkheid	De mate waarin informatie alleen toegankelijk is voor degenen die hiervoor gerechtigd zijn.

Het beoordelen van het belang van informatie voor het bedrijfsproces in termen van beschikbaarheid, integriteit en vertrouwelijkheid heeft tot doel concreter eisen te kunnen formuleren en beter in staat te zijn de afweging voor het soort risico en maatregelen te maken. Daar waar een applicatie op één van de aspecten van informatie: beschikbaarheid, integriteit en/of vertrouwelijkheid scoort is een aanvullende risicoanalyse noodzakelijk.

4.3 Risicoanalyse:

Bedrijfsimpact Analyse / Privacy Impact Assessment

Vincent van Gogh onderzoekt privacyrisico's van een nieuw (projectmatig) initiatief in een vroeg stadium op een gestructureerde en heldere manier. Dit doen wij middels een Privacy Impact Assessment (PIA). Met de PIA verplicht Vincent van Gogh zich om op tijd na te denken over vragen als:

- wat is de impact van het beoogde project op de privacy van de betrokkenen (de mensen van wie persoonsgegevens verwerkt worden)?;
- wat zijn de risico's voor de betrokkenen en voor de organisatie?;
- of is er, gegeven de doelstellingen van het project, ook een aanpak mogelijk die minder gevolgen heeft voor de privacy?

Een PIA dient bij te dragen aan:

- meer privacy bewustzijn;
- meer vertrouwen van onze patiënten en werknemers in hoe hun persoonsgegevens verwerkt en hun privacy gerespecteerd wordt;

- een betere communicatie over privacy en de bescherming van persoonsgegevens;
- voldoen aan wet- & regelgevingen van toezicht en handhaving;
- Een betere kwaliteit van gegevens;
- Een betere dienstverlening;
- Een betere besluitvorming.

4.4 Opstellen en invoeren van een Informatiebeveiligingsplan:

Op basis van de risicoanalyse wordt een beveiligingsplan opgesteld voor de concrete invoering van de vastgestelde tegenmaatregelen. De tegenmaatregelen worden uitgewerkt door zowel deskundigen van het te analyseren proces als deskundigen op het gebied van informatiebeveiliging en ICT.
Voor het benoemen van de maatregelen wordt de volgende werkwijze gehanteerd:

1. Vaststellen welke maatregelen noodzakelijk zijn per beschreven risico. Hierbij wordt tevens aangegeven of de maatregel al bestaat (vanuit bijvoorbeeld het standaard beveiligingsniveau);
2. Opstellen van een overzicht van alle benodigde maatregelen inclusief de nog te implementeren maatregelen;
3. In samenspraak met de verantwoordelijk manager wordt een rangorde opgesteld van de in te voeren maatregelen. Daarbij zijn de eerder bepaalde prioriteit en de geraamde kosten van de maatregel van belang;
4. Benoemen van alle relevante restrisico's en acceptatie hiervan door de eigenaar. Het management van het bedrijfsonderdeel beoordeelt de mogelijke consequenties van de restrisico's en initieert eventueel een aanpassing van het informatiebeveiligingsplan.

Het komt voor dat maatregelen groter zijn dan het uitvoeren van één of meerdere individuele acties. In dat geval neemt de eigenaar in het informatiebeveiligingsplan een actie op om een projectvoorstel op te stellen voor de invoering van de betreffende maatregel. Dit projectvoorstel wordt via de hiervoor ingerichte structuren binnen Vincent van Gogh voor GGZ als regulier project ingediend.

4.5 Accepteren van restrisico's:

Met het doorvoeren van maatregelen worden de risico's niet in alle gevallen volledig weggenomen. Maatregelen zijn vaak enkel gericht op het verkleinen van de kans, dan wel de impact van het risico. Daarom is na invoering van een maatregel een revisie van het risico en het bijbehorende restrisico noodzakelijk. De inschatting van het restrisico wordt door de eigenaar opgenomen in het beveiligingsplan. Het accepteren van alle restrisico's gebeurt door de eigenaar. Daarnaast rapporteert deze wel over de risico's die middel, dan wel hoog zijn geclassificeerd. Alle hoge restrisico's worden ter verificatie voorgelegd aan de Raad van Bestuur als onderdeel van de risicoanalyse. De eigenaar van de applicatie blijft te allen tijde verantwoordelijk voor alle risico's en de mogelijke consequenties. Terugkoppeling vanuit de Raad van Bestuur, kan eventuele aanpassing van het informatiebeveiligingsplan initiëren.

4.6 Monitoren, evalueren en rapporteren:

Vincent van Gogh gaat preventief en pro-actief om met informatiebeveiliging. Essentieel daarbij is de inrichting van een adequate managementrapportage aan de hand waarvan het management informatiebeveiliging monitort, evalueert en (be)stuurt.

4.7 Management van incidenten:

Vincent van Gogh kent een bestaande procedure voor het melden van incidenten (melden van onbedoelde gebeurtenissen / VIM). De melder kan incidenten tijdens de

registratie en/of classificatie een onbedoelde gebeurtenis als informatiebeveiligings-incident (met als specifieke variant datalek) classificeren. Wanneer een incident gekenmerkt wordt als informatiebeveiligingsincident en/of datalek dan worden procedureel de volgende aspecten geborgd:

- Is er sprake van een informatie beveiligingsincident, dan wordt de medewerker Informatiebeveiliging en de aviseur Kwaliteit en Veiligheid direct geïnformeerd (op basis van een e-mail notificatie met een koppeling naar het gemelde incident in het meldsysteem);
- Is (eveneens) sprake van een datalek, dan wordt de Geneesheer Directeur direct geïnformeerd (op basis van een e-mail notificatie met een koppeling naar het incident in Veilig Incidenten Melden).
- Over alle informatiebeveiligingsincidenten wordt gerapporteerd.

Incident respons:
Ten behoeve van incidenten betrekking hebbende op (een vermoeden van) datalek wordt uitvoering gegeven aan het calamiteitenprotocol datalekken.
Zoals alle verander- en verbeterprocessen binnen Vincent van Gogh worden deze processen cyclisch doorlopen. Hiertoe hanteren wij de zogenaamde PDCA-cyclus (Plan, Do, Check en Act).

5.0 Bijbehorende procedures/werkinstructies

De procedures met betrekking tot het beleid worden niet opgenomen in het beleidsdocument zelf.

6.0 Definities/bronnen

Wat	Omschrijving
Bedrijfscontinuïteitsplanning	Een proces dat voorziet in de totstandkoming van een document waarin de bedrijfsrisico's worden vastgelegd zodanig dat het gebruikt kan worden in het geval van een calamiteit.
Bedrijfscontinuïteitsplan	Het document dat voorziet in alle vereiste informatie waarmee Vincent van Gogh zich ervan kan verzekeren dat zij in staat is om kritieke processen (activiteiten) te hervatten in het geval dat zich een crisis of calamiteit voordoet.
Bedrijf kritieke processen / functies / systemen	De primaire bedrijfsfuncties, veelal op basis van geautomatiseerde systemen, die uitgeoefend moeten blijven worden om de dienstverlening naar patiënten voortgang te kunnen geven.
Beperkte Service (SDO)	Service Delivery Objective: de beperkte dienstverlening die binnen een vastgelegde tijdsperiode opgestart kan worden om kritieke processen in beperkte omvang te kunnen leveren.
Bedrijfs Impact Analyse	Het proces dat voorziet in het verzamelen van de minimale eisen ten aanzien van het herstel van die activiteiten noodzakelijk voor de totstandkoming van de bedrijfsdoelstelling. Zulks in het geval van een calamiteit.
Calamiteit	Een ernstig incident met aanzienlijke directe en/of gevolgschade. Vanuit ICT systemen gaat het om een aanzienlijke kans op onbeschikbaarheid van systemen die kritieke processen ondersteunen.
Calamiteiten Emergency Respons Team (CERT)	Het team dat verantwoordelijk is voor het beperken van de gevolgen van een incident en het herstel, voortkomende uit niet beschikbaar zijn van systemen als gevolg van een calamiteit of verstoring anderzijds.

Datalek	Een datalek is een bijzonder soort informatiebeveiligingsincident. We spreken van een datalek als een onbedoelde verwerking op gegevens plaats heeft gevonden. Denk hierbij aan gegevens die in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Maar ook gegevens die zijn kwijtgeraakt of onbedoeld zijn gewijzigd. Het kan gaan om een inbreuk op informatie of informatiedragers (netwerk, datadragers zoals mobiele en vaste apparatuur, papieren dossiers). Een datalek is het gevolg van een beveiligingsprobleem. De inbreuk kan door personen (wachtwoord misbruik, diefstal of vermissing van datadragers) of door andere mogelijke inbreuken (virusaanval, hacking, phishing, etc.) plaatsvinden. In het geval van **persoonsgerelateerde informatie** (medewerkers en patiënten) is het calamiteitenprotocol datalekken inclusief meldplicht van toepassing.
Disaster Recovery Plan (gedeeltelijk herstelplan)	Een plan dat beschrijft hoe herstel vanuit de calamiteit naar een aanvaardbaar dienstverleningsniveau wordt bereikt, op basis waarvan het proces in ieder geval weer plaats kan vinden.
Impact	De aard en ernst van de gevolgen voor de organisatie die zich voordoen als een bepaald risico zich verwezenlijkt.
Incident	Een situatie waarin een bekend of onbekend risico zich verwezenlijkt, waardoor wordt afgeweken van het normale dienstverleningsniveau.
Informatiebeveiligingsincident	Een incident waarbij de beschikbaarheid, vertrouwelijkheid of integriteit (juistheid) van gegevens in het gevaar komt of te kort schiet.
Kritieke Prestatie Indicator (KPI)	Variabelen die prestaties van ondernemingen weergeven.
Privacy Impact Assessment (PIA)	Beoordeling die tot doel heeft de risico's van een bepaalde verwerking van persoonsgegevens voor de betrokkenen in kaart te brengen en om waar nodig maatregelen te nemen.
Recovery Time Objective (RTO)	De tijd vanaf het moment dat een calamiteit wordt uitgeroepen tot het tijdstip dat de kritieke bedrijfsprocessen weer volledig operationeel moeten zijn, zodanig om substantiële verliezen te voorkomen.
Recovery Point Objective (RPO)	Een Recover Point Objective (RPO) geeft aan hoeveel data er maximaal verloren mag gaan bij een calamiteit.
Reguliere Service	De dienstverlening die geleverd wordt in een normale situatie, zonder dat er verstoringen zijn of op het moment dat alle verstoringen als gevolg van een calamiteit opgeheven / teniet zijn gedaan.
Resources / middelen	De middelen die nodig zijn om diensten en/of producten te kunnen leveren. Middelen zijn geld, activa (middelen), technologie en de meest belangrijke: mensen.
Restoration Plan (volledig herstelplan)	Een plan dat beschrijft hoe herstel tot het oorspronkelijke (volledige) en overeengekomen niveau van dienstverlening wordt bereikt.
Risico	Effect van onzekerheid op het behalen van doelstellingen.
Risico Management	Het proces van het beheersen van risico's, bestaande uit definiëren en analyseren van risico's en het benoemen van tegenmaatregelen om de risico's te beperken, waarbij (nog steeds) aan de ondernemingsdoelstelling(en) invulling kan worden gegeven.