NEN 7510 | Informatiebeveiliging in de zorg

Gelderland-Zuid

INFORMATIEBEVEILIGINGSBELEID

Datum:	16 mei 2018	**Classificatie**	Openbaar
Plaats:	Nijmegen	**Versie:**	1.0 DEFINITIEF
Auteur:	Sebastiaan Stevens	**Status:**	Vastgesteld

1 Inhoudsopgave

2 Documenteigenschappen

Rapportdatum: 16 mei 2018
Versie: 1.0 DEFINITIEF

2.1 Document locatie

Dit document is opgenomen in het kwaliteitshandboek (KHB) onder de sectie Beleid.

2.2 Historie

Versie	Datum	Veranderingen	Auteur
0.1	22-04-2018	Eerste opzet	Sebastiaan Stevens
0.2	01-05-2018	Tweede opzet	Sebastiaan Stevens
0.3	02-05-2018	Feedback beleidsadviseur kwaliteit verwerkt	Sebastiaan Stevens
0.9	04-05-2018	Overall revisie	Sebastiaan Stevens
1.0	08-05-2018	Aanvullingen gedragscodes	Sebastiaan Stevens

2.3 Goedkeuring

Dit document heeft de volgende goedkeuringen nodig.

Naam	Rol	Geaccordeerd?	Datum document	Versie
Moniek Pieters Directeur Publieke Gezondheid (DPG) GGD Gelderland-Zuid	Accorderend	Ja, in MT van 14 mei 2018	16-05-2018	1.0

3 Vooraf

Binnen onze organisatie werken we allemaal dagelijks met persoonlijke, gevoelige en/of vertrouwelijke gegevens. Om als betrouwbare partner voor onze cliënten, relaties en collega's te kunnen functioneren vinden wij informatiebeveiliging en bescherming van (persoons)gegevens van essentieel belang.

Hoe wij omgaan met informatiebeveiliging is in het voorliggende document beschreven. Hieraan gerelateerd zijn de meer gedetailleerde procedures, maatregelen en richtlijnen die voor het uitvoeren van het beleid van toepassing zijn. Dit informatiebeveiligingsbeleid beschrijft de richting en ondersteuning zoals deze door ons als managementteam van de GGD Gelderland-Zuid is bepaald.

Omdat wij intensief samenwerken met de Veiligheidsregio Gelderland-Zuid (VRGZ) op het gebied van ICT, informatiemanagement en informatiebeveiliging is het voorliggende beleid afgestemd met de VRGZ. Dit versterkt de integrale samenwerking. Daarnaast voldoet dit beleid aan de vereisten van NEN7510, de informatiebeveiligingsnorm in de zorgsector.

Als management van de GGD Gelderland-Zuid stellen wij de volgende informatiebeveiligingsbeleidspunten vast:

- De informatiebeveiligingsnorm NEN7510 beschouwen wij als uitgangspunt voor het ontwikkelen van richtlijnen die specifiek op de organisatie zijn toegesneden. Op sommige punten kan (gemotiveerd) worden afgeweken van de voorgestelde maatregelen en/of zijn er wellicht aanvullende maatregelen nodig.
- Dit informatiebeveiligingsbeleid is geïntegreerd met ons kwaliteitsbeleid.
- Het uit te dragen informatiebeveiligingsbeleid is vastgelegd in dit document.
- Jaarlijks stellen wij het informatiebeveiligingsplan vast waarin de maatregelen voor dat jaar als doelstelling zijn beschreven.
- Wij zullen actief het beveiligingsbewustzijn van onze medewerkers bevorderen.
- Wij zullen onze medewerkers waar mogelijk voorzien van gereedschappen die onbedoelde schendingen van het informatiebeveiligingsbeleid voorkomen.
- Alle interne[1]- en externe[2] medewerkers van de GGD Gelderland-Zuid conformeren zich aan het Informatiebeveiligingsbeleid.
- Alle medewerkers zijn gehouden gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij afwijkingen hiervan melding te doen.
- Alle onderdelen van dit beleid worden uitgewerkt in concrete richtlijnen en maatregelen, toegesneden op de taken en verantwoordelijkheden van onze medewerkers.
- Periodiek wordt beoordeeld of voor specifieke gegevens of informatiesystemen aanvullende maatregelen noodzakelijk zijn. De naleving van genomen maatregelen wordt periodiek getoetst.
- Het beleid wordt eens per drie jaar herzien en indien nodig tussentijds aangepast.

[1] Werknemer met een dienstverband bij de GGD Gelderland-Zuid
[2] Persoon die (niet) betaalde werkzaamheden voor de GGD Gelderland-Zuid verricht, anders dan met een dienstverband bij de GGD Gelderland-Zuid

Namens het managementteam van de GGD Gelderland-Zuid,

Moniek Pieters
Directeur Publieke Gezondheid

4 Informatiebeveiligingsbeleid GGD

De informatiebeveiligingsdoelstelling is afgeleid van onze missie. Deze luidt:

"*Wij maken ons sterk voor een gezonde regio Gelderland-Zuid. Inwoners helpen wij om gezonde keuzes te maken en om klachten/ziektes te voorkomen. Zodat zij zo lang mogelijk zelfstandig kunnen deelnemen aan de samenleving. Onze speciale aandacht gaat hierbij uit naar kwetsbare groepen.".*

Het bewaken, bevorderen en beschermen van de gezondheid van de inwoners uit onze regio wordt niet alleen zichtbaar in de uitvoering van onze primaire taken. Dit doen we ook door de (persoons)gegevens en (medische) dossierinformatie te bewaken en te beschermen. De drie kernwaarden omgevingsbewust, kwaliteitsgericht en ondernemend vormen het richtsnoer voor al het handelen van de GGD. Op basis van de missie is het mogelijk een meer operationele doelstelling voor Informatiebeveiliging te definiëren:

Alle interne en externe medewerkers van de GGD Gelderland-Zuid handelen bewust (professioneel) ten aanzien van de informatiebeveiligingsaspecten en dragen hierdoor bij aan de betrouwbare partner die de GGD voor haar cliënten en relaties is. We gaan zowel vertrouwelijk als zorgvuldig om met de beschikbare gegevens zodat het (onbedoeld) lekken, niet beschikbaar zijn of onbedoeld wijzigen van deze gegevens wordt voorkomen.[3]

Deze doelstelling heeft betrekking op de organisatie-, technische- en mensaspecten.

4.1 Doel van het beleid

Het beschikken over juiste en betrouwbare informatie is essentieel voor ons succes. Voor een effectieve beveiliging is het noodzakelijk dat gegevens, die aan de basis liggen van informatie, voldoen aan de gestelde eisen ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid. Effectieve beveiliging is te bereiken door te werken met gepaste gedragsregels, in overeenstemming met de wetgeving, navolgen van het vastgestelde beleid en de gewenste richtlijnen uit de praktijk.

Ons informatiebeveiligingsbeleid beschrijft de wijze waarop wij maatregelen nemen en richtlijnen opstellen die van toepassing zijn binnen de GGD Gelderland-Zuid.

Met dit beleid wordt invulling gegeven aan normelement 5.2 'Beleid' uit NEN7510:2017.

[3] Het professioneel en zorgvuldig omgaan met gegevens is nader toegelicht in het privacybeleid.

4.1.1 doelstellingen

De doelstellingen van dit informatiebeveiligingsbeleid zijn:

- Het voldoen aan geldende wet- en regelgeving en de norm NEN7510:2017.
- Het beschermen van alle fysieke en digitale informatiesystemen binnen de GGD Gelderland-Zuid (met inbegrip van, maar niet beperkt tot, alle computers, netwerkapparatuur, software en data) en het beperken van de risico's van diefstal, verlies, misbruik, uitval of beschadiging van deze informatiesystemen.
- De bewustwording creëren met betrekking tot de bekendheid en naleving van alle huidige en relevante interne procedures en richtlijnen, alsmede van wetgeving op het gebied van informatieveiligheid. Met het doel te zorgen dat alle in- en externe medewerkers hun eigen verantwoordelijkheden begrijpen met betrekking tot de bescherming van de vertrouwelijkheid en integriteit van de gegevens die zij behandelen in hun dagelijkse werk.
- Het zorgen voor een veilige en betrouwbare werking van de informatiesystemen voor in- en externe medewerkers en door leveranciers die deze informatiesystemen namens ons beheren.
- De borging ten aanzien van het beheer (exploitatie) van informatiesystemen om onbedoelde wijzigingen, met mogelijke nieuwe risico's, te voorkomen.
- GGD Gelderland-Zuid, als organisatie, te beschermen tegen aansprakelijkheid of schade door het misbruik van haar informatiesystemen en faciliteiten.
- Het zorgen voor een systematiek van incidentenregistratie, analyse en selecteren van gepaste preventieve en corrigerende maatregelen om informatieveiligheid te vergroten.
- Het bieden van een kader voor een adequate continuïteitstrategie om onderbrekingen van activiteiten tegen te gaan en kritieke processen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

4.1.2 Reikwijdte

Dit beleid heeft betrekking op alle door onze organisatie gebruikte gegevens en hieraan gerelateerde informatiesystemen, de fysieke aspecten met betrekking tot deze gegevens, privé-systemen welke zijn aangesloten op het netwerk van de GGD Gelderland-Zuid (bijvoorbeeld laptops van medewerkers) én op software in eigendom van de GGD Gelderland-Zuid of via licentie verkregen.

4.1.3 Uitgangspunten

- De inhoud van dit beleid en de oplegging tot naleving ervan is bekend bij al onze interne en externe medewerkers. Hierom is het onderwerp 'informatiebeveiliging' onderdeel van het inwerkprogramma van nieuwe medewerkers. Daarnaast wordt periodiek, maar minimaal twee keer per jaar op basis van een thema en frequenter indien interne audits hiertoe aanleiding geven, het onderwerp op het (werk-) overleg geagendeerd en besproken.

- Informatiebeveiliging is een continu proces. Daarom is het noodzakelijk periodiek het vastgestelde beleid te herijken. Technologische en organisatorische ontwikkelingen binnen en buiten onze organisatie maken het noodzakelijk om periodiek te beoordelen of wij op adequate wijze de (informatie-)beveiliging waarborgen. Hierom is onze informatiebeveiligingscyclus geïntegreerd in onze kwaliteitscyclus. Onze interne audits maken het hierdoor mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit.
- Wij zijn eigenaar van de informatie die onder onze verantwoordelijkheid wordt geproduceerd, tenzij dit op basis van wettelijke gronden anders is overeengekomen.
- Elke medewerker kent de waarde van informatie en handelt hiernaar. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Het classificeren van gegevens kan hierbij behulpzaam zijn. Zie ook paragraaf 4.3.
- Bij veranderingen, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt het onderwerp informatiebeveiliging zowel in de voorbereiding als in de uitvoering meegenomen.

4.2 Risicoanalyse en continuïteit

Beveiligen gebeurt met een duidelijk beeld voor ogen van de waarde van datgene wat beveiligd wordt. Dat betekent dat bewustzijn van die waarde en van de risico's van mogelijke schade, de grondslag is van dit beleid en daarmee sturend moet zijn in het nemen van maatregelen. Het is onze taak als verantwoordelijke bestuurder en lijnmanagement om ervoor te zorgen dat dit bewustzijn aanwezig is.

4.2.1 Risicoanalyse

Om reproduceerbaar en eenduidig de waarde van informatie(systemen) en gepaste beheersmaatregelen te kunnen bepalen wordt er gebruik gemaakt van een kwalitatieve risicoanalyse om onderbouwd de belangrijkste risico's te identificeren. Wij gebruiken hiervoor de risicomatrix. De risicoanalyse wordt, in beginsel, elke drie jaar herhaald, of tussentijds in het geval van substantiële wijzigingen.

4.2.2 Classificatie informatiesystemen

Elk informatiesysteem binnen onze organisatie heeft een eigenaar[4]. De waarde van de informatiesystemen wordt vastgesteld door de eigenaar o.b.v. een uniforme methodiek voor classificatie. De waarde wordt bepaald door de schade die verlies van beschikbaarheid, integriteit en vertrouwelijkheid toebrengt aan de uitvoering van onze primaire taken op het gebied van publieke gezondheidszorg.

4.2.3 Strategie voor continuïteit

Informatiebeveiliging heeft als doel om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door het management vastgesteld, acceptabel niveau. Ondanks goede beheersmaatregelen kan een incident zich voordoen.

[4] Met eigenaar wordt bedoeld de persoon/functionaris, doorgaans de proceseigenaar, die verantwoordelijk is voor alle aspecten ten aanzien de exploitatie, aanpassingen en toekomstige vervangingen van het systeem.

Voor kritieke ICT-diensten en informatiesystemen is een continuïteitsplan aanwezig. Hierin is opgenomen hoe, in geval van calamiteiten, de getroffen ICT-dienst of het getroffen informatiesysteem, binnen de door ons vastgestelde tijd, operationeel gemaakt kan worden. Continuïteitsplannen worden minimaal één keer per jaar op actualiteit geëvalueerd.

4.3 Informatieclassificatie

Alle informatie binnen onze organisatie wordt geclassificeerd naar één van de vier niveaus van vertrouwelijkheid, zoals in onderstaande tabel is vermeld.

Gegevensclassificatie	Kenmerken van informatie
Openbaar	Deze informatie kent veelal lage eisen ten aanzien van de vertrouwelijkheid en beschikbaarheid en is daardoor voor **iedereen** binnen en buiten de GGD Gelderland-Zuid beschikbaar en toegankelijk.
Bedrijfsvertrouwelijk	Dit betreft de informatie die toegankelijk mag of moet zijn voor alle **medewerkers** van de GGD Gelderland-Zuid. De eisen ten aanzien van vertrouwelijkheid zijn beperkt maar aanwezig.
Vertrouwelijk	Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep gebruikers. De informatie wordt beschikbaar gesteld op basis van het "*need to know*" principe[5]. Schending van deze classificatie kan direct of indirecte schade toebrengen aan de GGD Gelderland-Zuid, onderdelen van de GGD Gelderland-Zuid of personen binnen de GGD Gelderland-Zuid.
Geheim	Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen aan de GGD Gelderland-Zuid, onderdelen van de GGD Gelderland-Zuid of personen binnen de GGD Gelderland-Zuid.

Voor informatie geclassificeerd als 'Bedrijfsvertrouwelijk', 'Vertrouwelijk' of 'Geheim' kunnen, additioneel aan het basis beveiligingsniveau, extra beschermende maatregelen nodig zijn.

4.4 Naleving van wet- en regelgeving

Wij dienen ons te houden aan alle relevante wet- en regelgeving die van toepassing is op het uitvoeren van de dagelijkse werkzaamheden. De relevante wet- en regelgeving is vertaald naar richtlijnen en gedragscodes die van toepassing zijn op al onze medewerkers en voor het overige van toepassing zijn op inhuurpersoneel, stagiaires van de GGD Gelderland-Zuid of derden (zoals leveranciers) die gebruik maken van informatievoorzieningen van de GGD Gelderland-Zuid. Wettelijke voorschriften welke opgevolgd dienen te worden zijn:

- Algemene Verordening Gegevensbescherming[6] (AVG)

[5] Dit principe houdt in dat functionarissen slechts toegang hebben tot die informatie die zij nodig hebben voor het uitoefenen van hun functie.

[6] De AVG is de Europese privacy verordening die per 24 mei 2016 in werking is getreden. De Verordening is vanaf 25 mei 2018 van toepassing.

- Ambtenarenwet
- Archiefwet
- Besluit elektronische gegevensverwerking door zorgaanbieders
- Jeugdwet (JW)
- Meldplicht datalekken
- Nieuwe Wet maatschappelijke ondersteuning (nieuwe Wmo)
- Warenwetbesluit tatoeëren en piercen
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Wet Beroepen in de Individuele Gezondheidszorg (wet BIG)
- Wet Kinderopvang
- Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz)
- Wet op de computercriminaliteit
- Wet op de geneeskundige behandelovereenkomst (WGBO)
- Wet op de lijkbezorging
- Wet Publieke Gezondheid (WPG)

Aanvullend op het voorgaande houden wij ons aan diverse gedragscodes die van toepassing zijn binnen de diverse vakgebieden waarbinnen wij werken. Voorbeelden zijn:

- Gedragscode ambtenaren
- Gedragscode gezondheidsonderzoek
- Beroepscode van Verpleegkundigen en Verzorgenden
  Gedragsregels voor artsen
- Beroepscode jeugdprofessional
- Beroepscode jeugdzorgwerker
- Beroepscode maatschappelijk werker
- Beroepscode pedagoog
- Beroepscode logopedist
- Beroepscode toezichthouder kinderopvang

Daarnaast gelden de afspraken die contractueel zijn overeengekomen met leveranciers.

4.5 Sancties bij inbreuken op het informatiebeveiligingsbeleid

Het beleid is uitgewerkt in verschillende processen, procedures en richtlijnen die van toepassing zijn binnen de GGD Gelderland-Zuid. Bij inbreuk op het informatiebeveiligingsbeleid neemt het management van de GGD Gelderland-Zuid passende maatregelen.

Indien wij worden aangesproken op de overtreding van eigendomsrechten, auteursrechten of overtreding van andere wettelijke bepalingen, zijn de wettelijke en binnen de GGD Gelderland-Zuid geldende regelingen van toepassing. In geval er door het onrechtmatig handelen schade ontstaat, kan de overtreder daarvoor aansprakelijk worden gesteld.

5 Organisatie van de informatieveiligheid

Informatiebeveiliging hebben wij procesmatig ingericht[7]. Dit geldt ook voor de bescherming van persoonsgegevens: het privacybeleid en de naleving ervan. Beide onderwerpen zijn tevens een duidelijk benoemd onderdeel van al onze processen[8]. Informatiebeveiliging is onderdeel van onze kwaliteitscyclus. Aansluitend hierop worden jaarplannen opgesteld, belegd in de organisatie en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen (Plan, Do, Check, Act).

5.1 Actoren

Verschillende actoren in onze organisatie verrichten gezamenlijk de activiteiten binnen het informatiebeveiligings-proces. Elke actor heeft een bepaalde rol binnen het proces. Een goede verdeling van de *taken, bevoegdheden en verantwoordelijkheden* (TBV's) tussen de verschillende actoren is cruciaal voor een effectief en efficiënt procesverloop.

Voor het realiseren van een effectieve informatiebeveiliging onderkennen wij de volgende actoren:

- Management heeft strategische verantwoordelijkheid - besturing
- Het lijnmanagement heeft een tactische verantwoordelijkheid – aansturing en facilitering
- De chief information security officer (CISO) - beheersing en naleving
- De informatiemanager – beleidsontwikkeling en adviseren
- De beleidsadviseur kwaliteit - beleidsontwikkeling en adviseren
- De aandachtsfunctionarissen kwaliteit - kwaliteitsborging
- De interne auditoren - toetsende verantwoordelijkheid
- De medewerker (iedereen) heeft een operationele verantwoordelijkheid - uitvoering
- De functionaris gegevensbescherming (FG) - toezicht privacywetgeving
- De externe partijen, onafhankelijk toetsen en beoordelen

Het management is integraal verantwoordelijk voor het vaststellen van het beleid en de richtlijnen die ten grondslag liggen aan een adequaat systeem van informatiebeveiliging en voor het beoordelen van de efficiëntie en effectiviteit hiervan. Als verantwoordelijke voor het onderwerp informatiebeveiliging is er, binnen het management, een portefeuillehouder informatiebeveiliging aangewezen.

Vanuit de rol van security-officer is deze functionaris verantwoordelijk voor beleidsvorming, controle en registratie, communicatie en voorlichting en stelt verbetervoorstellen op voor de informatiebeveiliging. Dit gebeurt in nauw overleg met de beleidsadviseur kwaliteit.

De beleidsadviseur kwaliteit bewaakt de samenhang met het kwaliteitsmanagementsysteem van onze organisatie. Belangrijke taken vanuit de kwaliteitsadviseur zijn informeren,

[7] Voor de inrichting van het proces zijn het Information Security Management System (ISMS) en het Kwaliteitsmanagementsysteem (KMS) als uitgangspunten genomen.
[8] Of in contracten ondergebracht indien er sprake is van uitbestede (ICT-)diensten.

borging van de integrale kwaliteit en doelmatigheid van onze activiteiten, naleving van wet- en regelgeving en het eigen beleid en het coördineren en uitvoeren van audits om van daaruit te komen tot verbetervoorstellen.

De dagelijkse verantwoordelijkheid berust bij ons lijnmanagement. Zij ziet voortdurend toe op naleving van de vastgestelde richtlijnen. Daarnaast verwachten we van hen de risico's te beoordelen waarmee hun afdeling wordt geconfronteerd.

Elke medewerker (al dan niet in vaste dienst) is gehouden mee te werken aan de informatiebeveiliging. Op individueel niveau is hij verantwoordelijk voor een effectieve informatiebeveiliging van de aan hem toevertrouwde gegevens. Ook wordt van elke medewerker verwacht dat hij eventuele beveiligingsincidenten direct meldt in het registratiesysteem.

5.2 Evaluatie & Controle

Onder controle verstaan we zowel de interne controle door de eigen organisatie als toetsing door een onafhankelijke derde. De toetsing richt zich zowel op het informatiebeveiligingsbeleid als op de maatregelen die uit dit beleid voortvloeien en omvat de volgende drie punten:

1. Juiste naleving van het beleid en de interne werkafspraken.
2. Correcte werking van de beveiligingsorganisatie.
3. Toereikendheid van de vastgestelde beveiligingsmaatregelen gedurende een bepaalde periode.

Onder evaluatie wordt verstaan het nagaan of de kaders van de informatiebeveiliging inhoudelijk nog toereikend zijn. Hierbij worden twee niveaus onderscheiden: de evaluatie van het beleid en de evaluatie van de beheersing van de informatiebeveiliging.

1. De evaluatie van het beleid is een driejaarlijkse heroriëntatie op de beleidsuitgangspunten en of het vastgestelde beleid nog toereikend is.
2. Om ervoor te zorgen dat geïmplementeerde beveiligingsmaatregelen worden nageleefd dient er periodiek te worden gemeten, naast de dagelijkse controle door de chief information security officer. De interne auditoren voeren, op basis van een werkprogramma inclusief uitgewerkte kwaliteitseisen, een audit uit.

5.3 Beheersing van informatieveiligheid

Het organiseren van de informatieveiligheid doorloopt bij ons een cyclisch proces. Door middel van de zogenaamde Plan-Do-Check-Act cyclus wordt gestreefd naar een adequaat niveau van de informatiebeveiliging. De tussentijdse controles of constateringen kunnen aanleiding zijn bij te sturen op de bestaande maatregelen.

De PDCA-cyclus wordt periodiek doorlopen. Deze is geïntegreerd met het kwaliteitsmanagementsysteem (KMS) en de beleidscyclus. Dit betekent dat:

- Het thema informatiebeveiliging jaarlijks terugkomt bij het opstellen van de A3-jaarplannen per afdeling en als resultaat van de halfjaarlijkse directiebeoordeling (PLAN).

- Informatiebeveiliging bij elk project en binnen elke applicatie structureel aan bod komt. Dit is geborgd in onder meer het projectinitiatieproces (DO).

- Informatiebeveiliging 4x per jaar wordt getoetst op de werking in onder meer audits, selfassessments en managementrapportages (CHECK).

- Informatiebeveiliging 2x per jaar wordt geëvalueerd en beoordeeld middels managementreviews per afdeling en de directiebeoordeling (ACT).

Bijlage 1 - Definities

In deze bijlage worden enkele definities nader toegelicht.

Algemene Verordening Gegevensbescherming

De AVG is de Europese privacy verordening die per 24 mei 2016 in werking is getreden. De Verordening is vanaf 25 mei 2018 van toepassing.

Chief information security officer (CISO)

De functionaris binnen de GGD Gelderland-Zuid die is belast met het coördineren van de informatiebeveiligingsactiviteiten.

Continuïteitsplan

Een plan om bij (ernstige) verstoringen de informatievoorziening gericht op het primaire proces, binnen de door de GGD Gelderland-Zuid aangegeven tijd, weer beschikbaar te hebben.

Compliance

Compliance betekent dat de organisatie moet (en wil) voldoen aan de wet- en regelgeving. Het niet voldoen aan compliancy-eisen brengt risico's met zich mee zoals:

- imagoschade die kan worden opgelopen.
- financiële schade in de vorm van boetes of claims.

Fysieke en digitale informatiesystemen

Informatiesystemen met het doel vanuit gegevensbronnen voor een gebruiker relevantie informatie te generen. Dit kan een digitaal systeem (bijvoorbeeld: een applicatie) zijn of een fysiek systeem (bijvoorbeeld: het HRM-dossier in een kast)

Informatiebeveiliging

Het treffen van maatregelen om de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij te waarborgen en de eventuele gevolgen van incidenten te beperken tot een acceptabel, vooraf bepaald niveau.

Informatieveiligheid

Het resultaat van informatiebeveiliging.

Incidentenregistratie

Een systeem, bij voorkeur digitaal, waar meldingen over de informatiebeveiliging in worden geregistreerd zodat de organisatie adequaat kan reageren en de opvolging kan worden gemonitord. Dit wordt daarna opgevolgd in de continue verbetercyclus van de organisatie/zorg en dienstverlening van de organisatie.

ISMS

Het Information Security Management System[9]. Dit is het samenspel van activiteiten gericht op het continue verbeteren van het proces (of processen) gericht op het borgen van de informatiebeveiliging. Door het inrichten van een ISMS behoudt de organisatie grip op het onderwerp Informatiebeveiliging.

Opzet, bestaan en werking

Met opzet wordt bedoeld het beschrijven van processen, procedure, beleidsuitgangspunten et cetera zoals deze binnen de organisatie worden uitgevoerd. Met bestaan bedoelen we het één keer aantoonbaar maken dat deze processen worden beheerst. De werking is het aantoonbaar maken van de beheersing over een bepaalde periode.

[9] Het ISMS is geen ICT-systeem of applicatie maar is gericht op het verbeteren van de kwaliteit van de informatiebeveiligingsprocessen.