Beleid voor Informatiebeveiliging 2025 t/m 2027

Inhoud

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
1.00	27-08-2025		Finaliseren	Definitief

Gecontroleerd door

Versie	Datum	Naam	Functie
0.01	03-07-2025		CISO
0.91	27-08-2025		Teamlead Compliance & Audits
0.91	27-08-2025		CIO
1.00	02-02-2026		ISO

Geautoriseerd door

Versie	Datum	Naam	Functie
1.00			CIO
1.01			CIO

Gerelateerde documenten

Documenttitel
IB-Baseline
Beleid voor het ISMS
Beleid voor classificatie van informatie
Beleid voor leveranciers
Beleid voor toegangsbeveiliging
Beleid voor het omgaan met informatie
Taken, verantwoordelijkheden en bevoegdheden voor informatiebeveiliging

Volgende review en/of herziening, plus accordering

Datum	Functie
31-12-2027	CIO

1 Inleiding

Dit document beschrijft het beleid voor informatiebeveiliging binnen GGD GHOR Nederland. Het beleid is gebaseerd op een risicogerichte aanpak en houdt rekening met veranderende organisatiedoelstellingen, nieuwe wet- en regelgeving, relevante standaarden en het actuele dreigingslandschap.

Informatiebeveiliging heeft als hoofddoel het waarborgen van drie kernprincipes: beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Deze principes worden ook wel aangeduid als de BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid).

Dit beleid is officieel goedgekeurd door de Chief Information Officer (CIO) van GGD GHOR Nederland. Het document is publiekelijk beschikbaar en kan actief worden gedeeld met GGD'en, ketenpartners, leveranciers en andere betrokken partijen bij de informatievoorziening.

Scope en doelgroep

Dit beleid is van toepassing op alle vormen van informatie die worden ondersteund of gebruikt binnen de processen van GGD GHOR Nederland. Het beleid geldt gedurende de complete levenscyclus van informatie en informatiesystemen, onafhankelijk van de toegepaste technologie of het karakter van de informatie en ook onafhankelijk van de plaats van deze informatie(systemen) .

Het beleid richt zich op alle medewerkers, gasten, bezoekers en externe relaties van de organisatie. Iedereen die toegang heeft tot informatie of informatiesystemen van GGD GHOR Nederland valt onder de werking van dit beleid.

Opstellen, vaststellen en onderhouden van het informatiebeveiligingsbeleid

Dit informatiebeveiligingsbeleid is ontwikkeld onder verantwoordelijkheid van de Chief Information Security Officer (CISO) en formeel vastgesteld door de Chief Information Officer (CIO) van GGD GHOR Nederland.

Informatiebeveiliging is een doorlopend proces dat continu aandacht vereist. Daarom is het essentieel om het vastgestelde beleid en de uitvoering hiervan periodiek te evalueren. Technologische en organisatorische ontwikkelingen, zowel binnen als buiten onze organisatie, evenals veranderende dreigingslandschappen maken regelmatige beoordeling noodzakelijk. Deze evaluaties bepalen of de informatiebeveiliging nog steeds adequaat is geborgd.

Het informatiebeveiligingsbeleid wordt minimaal eenmaal per jaar beoordeeld en waar nodig geactualiseerd. Daarnaast wordt het beleid herzien wanneer zich een ernstig beveiligingsincident heeft voorgedaan of wanneer er grote organisatorische wijzigingen hebben plaatsgevonden.

2 Informatiebeveiligingsdoelstellingen

In dit hoofdstuk worden de informatiebeveiligingsdoelstellingen van GGD GHOR Nederland uiteengezet. Deze doelstellingen vormen de kern van het informatiebeveiligingsbeleid en geven richting aan de inrichting van onze informatiebeveiliging. Het hoofddoel is het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van risico's door de vertrouwelijkheid, integriteit en beschikbaarheid van onze informatievoorziening te waarborgen.

De in dit hoofdstuk beschreven doelen zijn een directe vertaling van de ambitie en visie van GGD GHOR Nederland. Een robuust informatiebeveiligingsbeleid is essentieel om deze ambities op een veilige en verantwoorde wijze te realiseren en te voldoen aan wettelijke en contractuele eisen.

Dit hoofdstuk beschrijft achtereenvolgens onze ambitie en visie op informatiebeveiliging, de daaruit volgende strategische doelen, en de planning en procedures die we hanteren. Hierin wordt ook vastgelegd hoe wordt omgegaan met situaties die een uitzondering op het vastgestelde beleid vereisen, om zo een consistente en beheerste aanpak te verzekeren.

Ambitie en visie van GGD GHOR Nederland

De missie en dienstverlening van GGD GHOR Nederland is gericht op een veilig en gezond Nederland. Hierbij wordt de volgende ambitie uitgesproken:

- We vergroten gelijke kansen op gezondheid voor iedereen;
- We dragen onze uitgesproken mening uit en beïnvloeden zo de publieke gezondheid;
- We zijn voorbereid op gezondheidsbedreigingen;
- GGD'en en GHOR's bieden een aantrekkelijk werkveld voor goed opgeleide professionals;
- We gebruiken onze data voor een betere publieke gezondheid;
- We zijn voorbereid om de gezondheid te beschermen tijdens rampen en crises.

Dit zijn de principes die als leidraad dienen voor alle activiteiten in verband met informatiebeveiliging.

Strategische doelen voor informatiebeveiliging

GGD GHOR Nederland streeft naar een veilig en gezond Nederland, waarin gelijke kansen op gezondheid voor iedereen centraal staan. Om deze ambitie waar te maken, is het van essentieel belang dat de informatievoorziening binnen de organisatie betrouwbaar, veilig en toekomstbestendig is. Het beschermen van persoonsgegevens, het waarborgen van continuïteit tijdens rampen en crises, en het verantwoord kunnen inzetten van betrouwbare data vormen onmisbare voorwaarden voor het realiseren van de missie en het versterken van het publieke vertrouwen in GGD GHOR Nederland.

De strategische doelstellingen voor en eisen aan de informatiebeveiliging zijn direct afgeleid van deze ambitie en visie. Door te werken aan een veilige en betrouwbare informatievoorziening (eis 1) en het beschermen van persoonsgegevens (eis 2), wordt invulling gegeven aan de randvoorwaarden voor gelijke gezondheidskansen, crisisbestendigheid en een aantrekkelijk werkveld voor professionals.

Het minimaliseren van risico's door menselijk gedrag en het versterken van bewustzijn onder medewerkers dragen bij aan een veilige organisatiecultuur en ondersteunen het aantrekken en behouden van goed opgeleide professionals. Het beheersen van toegang tot informatie, het voorkomen van ongeautoriseerde toegang en het snel detecteren en afhandelen van incidenten zijn essentieel voor het beschermen van de publieke gezondheid en het waarborgen van continuïteit, ook

in tijden van crisis. Door leden en projecten actief te ondersteunen en een coördinerende rol te vervullen in het informatiebeveiligingsbeleid, draagt het CISO Office bij aan kennisdeling en versterking van de gehele publieke gezondheidszorg.

De eisen aan informatiebeveiliging:

1. Het waarborgen van veilige en betrouwbare informatievoorziening, bedrijfsmiddelen en processen;
2. Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.

Voor het voldoen aan de bovenstaande eisen zijn de volgende IB-doelstellingen geformuleerd door het CISO Office:

1. Het minimaliseren van risico's door menselijk gedrag;
2. Het beheersen van de toegang tot informatie en tot informatiesystemen;
3. Het voorkomen van ongeautoriseerde toegang door kwaadwillende en/of onbevoegden;
4. Het detecteren, identificeren en reageren op incidenten en datalekken;
5. Het ondersteunen, wanneer gevraagd en wanneer mogelijk, van haar leden en projecten bij informatiebeveiligingsvraagstukken;
6. Het spelen van een coördinerende rol bij planning, uitvoering, rapporteren en evalueren van informatiebeveiligingsbeleid.

De vertaling van deze strategische doelen naar de praktijk vindt plaats door het formuleren van jaarlijkse doelstellingen, waaraan concrete Key Performance Indicators (KPI's) zijn verbonden. Hiermee wordt de voortgang en het succes van ons informatiebeveiligingsbeleid gemonitord. Deze tactische doelen en KPI's zijn gedocumenteerd en beschikbaar in het Information Security Management System (ISMS).

ISMS

Ter ondersteuning van het CISO Office en het realiseren van deze doelstellingen, is een Information Security Management System (ISMS) ingericht. Dit ISMS fungeert als het gestructureerde raamwerk van beleid, processen en procedures dat helpt om informatiebeveiliging systematisch te borgen en continu te verbeteren volgens de Plan-Do-Check-Act cyclus. Het ISMS biedt de concrete handvatten om de door het CISO Office geformuleerde doelen te implementeren, zoals het inrichten van toegangsbeheer en het opzetten van een incident response proces. Bovendien zorgt het ISMS ervoor dat de informatiebeveiliging aantoonbaar en controleerbaar wordt, wat essentieel is voor het voldoen aan wettelijke en contractuele eisen, zoals de AVG, en het beheerst reduceren van risico's tot een acceptabel niveau.

Gedeelde verantwoordelijkheid

Het realiseren van de geformuleerde informatiebeveiligingsdoelstellingen is een gezamenlijke inspanning die de gehele organisatie omvat. Hoewel het CISO Office een coördinerende en sturende rol heeft in het opstellen en evalueren van het beleid, ligt de uiteindelijke verantwoordelijkheid voor een veilige informatiehuishouding niet exclusief bij dit team. Informatiebeveiliging is een integraal onderdeel van de dagelijkse werkzaamheden en vereist de actieve betrokkenheid van zowel managers als medewerkers. Managers dragen de verantwoordelijkheid om het beleid binnen hun teams uit te dragen en toe te zien op de naleving ervan, terwijl iedere medewerker de plicht heeft om zorgvuldig en bewust om te gaan met de informatie en systemen die zij gebruiken. Alleen door deze gedeelde

verantwoordelijkheid te omarmen, kan GGD GHOR Nederland de risico's effectief minimaliseren en haar missie op een veilige en betrouwbare manier uitvoeren.

3 Het organiseren van informatiebeveilging

De eindverantwoordelijkheid voor informatiebeveiliging bij GGD GHOR Nederland ligt bij de algemeen directeur van GGD GHOR Nederland. Hij heeft deze verantwoordelijkheid gedelegeerd aan de Chief Information Officer (CIO) van GGD GHOR Nederland. De CIO heeft de operationele verantwoordelijkheid voor de besturing, inrichting en bewaking van informatiebeveiliging gedelegeerd aan de CISO.

De CIO is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het bestuur en de leden van de vereniging Publieke Gezondheidzorg Nederland. Hierbij rapporteert hij of zij tevens over de mate waarin invulling is gegeven aan het uitwerken van tactische beleidsonderwerpen die aanvullend zijn op het strategische beleid.

De directeur zal erop toezien dat elke leidinggevende en werknemer bekend is met het beleid en hiernaar werkt. Ter vergroting van de bewustwording rondom het onderwerp Informatiebeveiliging worden updates geplaatst op het intranet.

Leiderschap en betrokkenheid

De CIO toont leiderschap en betrokkenheid met betrekking tot informatiebeveiliging door:

1. Het informatiebeveiligingsbeleid goed te keuren;
2. Te bewerkstelligen dat de informatiebeveiligingsdoelstellingen worden vastgesteld en passend zijn met de strategische richting van GGD GHOR Nederland;
3. Te bewerkstelligen dat de eisen van het managementsysteem voor informatiebeveiliging in de processen van GGD GHOR Nederland worden geïntegreerd;
4. Te bewerkstelligen dat de voor het managementsysteem voor informatiebeveiliging benodigde middelen beschikbaar zijn;
5. Het belang van doeltreffend informatiebeveiligingsmanagement en van het voldoen aan de eisen van het managementsysteem voor informatiebeveiliging te communiceren;
6. Te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resultaten behaalt;
7. Leidinggevenden en medewerkers aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging;
8. Continue verbetering te bevorderen;
9. Andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

De CISO is verantwoordelijk voor het inrichten en onderhouden van het informatiebeveiligingsmanagementsysteem van GGD GHOR Nederland en rapporteert over de effectiviteit van informatiebeveiliging binnen GGD GHOR Nederland en haar omgeving aan de CIO. De CIO wordt op de hoogte gehouden van de ontwikkelingen op het gebied van informatiebeveiliging door middel van jaarlijkse management reviews en regelmatige overleggen.

Verantwoordelijkheden voor de beheersmaatregelen

GGD GHOR Nederland legt de verantwoordelijkheid voor de beheersmaatregelen voor het ISMS bij diverse functionarissen. Een gedetailleerd overzicht van welke functionaris verantwoordelijk is voor

welke specifieke beheersmaatregel, is opgenomen in het document "Taken, verantwoordelijkheden en bevoegdheden".
De verantwoordelijkheden zijn op strategisch, tactisch en operationeel niveau belegd om een integrale aanpak te garanderen. Zo is de algemeen directeur, samen met de CIO, verantwoordelijk voor het tonen van leiderschap en betrokkenheid vanuit de top van de organisatie. De CIO heeft een brede, sturende rol in het vaststellen van het beleid, de operationele planning en het beschikbaar stellen van middelen. De CISO is de proceseigenaar van het ISMS en daarmee primair verantwoordelijk voor de risicobeoordeling, het opstellen van de beveiligingsdoelstellingen en de monitoring van de prestaties. Essentiële ondersteunende taken, zoals het verhogen van competentie en bewustzijn, zijn belegd bij HRM en Communicatie. De details van deze toewijzing zijn, zoals gezegd, te vinden in het document "Taken, verantwoordelijkheden en bevoegdheden".

Cultuur

Het is van groot belang dat het informatiebeveiligingsbeleid en de hieruit volgende principes en richtlijnen bekend zijn bij alle betrokkenen binnen GGD GHOR Nederland. De inrichting van informatiebeveiliging draagt bij aan de weerbaarheid van GGD GHOR Nederland.

Leidinggevenden bevorderen een cultuur waarbij nut en noodzaak van informatiebeveiliging wordt uitgedragen. De leidinggevenden van GGD GHOR Nederland geven duidelijke richting aan informatiebeveiliging en demonstreren dat zij het belang van informatiebeveiliging ondersteunen en zich hierbij betrokken voelen, door onder andere het uitdragen en handhaven van het informatiebeveiligingsbeleid.

Bewustzijn en verantwoordelijkheden medewerkers

GGD GHOR Nederland biedt een bewustwordingsprogramma aan alle medewerkers van GGD GHOR Nederland. Dit programma omvat het regelmatig maken van een e-learning en het uitvoeren van aanvullende interventies om het niveau van bewustwording te verhogen. Dit programma heeft een verplicht karakter. Verder worden medewerkers op de hoogte gebracht van het gewenste gedrag op het gebied van veilig omgaan met informatie door middel van een gedragscode waarvoor zij tekenen bij het in dienst treden.

Medewerkers zijn verplicht om (vermoedens van) beveiligingsincidenten direct te melden bij het SOC. Dit kan via SOC@GGDGHOR.nl of via 030-7024830. Incidenten kunnen variëren van datalekken, malwarebesmettingen en ongeautoriseerde toegang tot verstoringen van systemen of processen. Het SOC registreert alle meldingen en start direct een eerste analyse om de aard en impact van het incident vast te stellen.

4 Inrichting en beheersing van informatiebeveiliging

Om de in het vorige hoofdstuk gestelde doelen te realiseren, is een doordachte structuur en een helder raamwerk voor beheersing essentieel. Dit hoofdstuk beschrijft de fundamentele uitgangspunten die GGD GHOR Nederland hanteert voor de praktische inrichting en de dagelijkse beheersing van haar informatiebeveiliging.

We beginnen met de basis: het gebruik van een gestandaardiseerde IB-Baseline die als fundament dient voor al onze beveiligingsinspanningen. Vervolgens wordt de scope verbreed naar onze samenwerkingsverbanden, waarbij de principes van ketenverantwoordelijkheid worden toegelicht om de veiligheid ook buiten onze eigen organisatie te waarborgen. Tot slot wordt ingegaan op een cruciale interne beheersmaatregel: de scheiding van taken, die de integriteit van onze processen waarborgt. Samen vormen deze elementen het raamwerk waarbinnen we onze informatie op een consistente en veilige manier beheren.

Gebruik van baselines

GGD GHOR Nederland gebruikt marktstandaarden voor informatiebeveiliging en gaat uit van een 'baseline' van maatregelen, aangevuld met dreiging-gebaseerde maatregelen. Hiervoor wordt gebruik gemaakt van de zogeheten 'IB-Baseline'. Deze set van maatregelen bestaat uit technische, organisatorische en fysieke maatregelen om dreigingen te mitigeren, en is voortgekomen uit beleidsprincipes, standaarden en best-practices, vertaald naar een concrete uitwerking om het doel van de maatregelen te bereiken. De IB-Baseline is de bron voor de eisen die worden opgelegd aan leveranciers, programma's en projecten en is op te vragen bij het CISO Office.

Aangezien GGD GHOR Nederland haar volledige IT heeft uitbesteed, is het essentieel om te benadrukken dat de organisatie zelf geen technische beheersmaatregelen implementeert. Onze rol is het definiëren van de vereiste beveiligingseisen via de IB-Baseline; de daadwerkelijke technische inrichting en het beheer zijn volledig belegd bij onze gespecialiseerde IT-leveranciers. De naleving van deze eisen wordt geborgd via ons leveranciersmanagementproces en de afspraken die worden gemaakt in het kader van ketenverantwoordelijkheid.

Ketenverantwoordelijkheid

GGD GHOR Nederland ondersteunt de informatiebeveiliging van de publieke gezondheidszorg door zowel gevraagd als ongevraagd, haar klanten, ketenpartners en leveranciers zowel proactief als reactief te adviseren over informatiebeveiliging.

Het organiseren van adequate informatiebeveiliging draagt bij aan een integrale (keten)verantwoordelijkheid voor GGD GHOR Nederland. Informatiebeveiliging wordt daarom bepaald op ketenniveau, rekening houdend met de informatieclassificatie. Afspraken met leveranciers moeten passen binnen de besturing van de keten.

Aan leveranciers en ketenpartners die operationeel uitvoering geven aan het beheer, de ontwikkeling of de ondersteuning van de informatievoorziening, worden dezelfde informatiebeveiligingseisen gesteld als die GGD GHOR Nederland zelf hanteert. Deze eisen zijn opgenomen in het Programma van Eisen bij nieuwe aanbestedingen.

Iedere overeenkomst of convenant is voorzien van een informatiebeveiligingsparagraaf waarin wordt verwezen naar het proces van IT-risicobeheersing en de daaruit voortvloeiende activiteiten. Het is de verantwoordelijkheid van de CISO om hier inhoudelijke afstemming over te vinden met de contractpartij(en) via de verantwoordelijken voor Inkoop- en Leveranciersmanagement binnen GGD GHOR Nederland.

Scheiding van taken

Om belangenconflicten en fraude te voorkomen, is het essentieel om functiescheiding toe te passen binnen de organisatie. Dit houdt in dat kritische taken en verantwoordelijkheden bewust worden verdeeld over verschillende medewerkers en afdelingen. Door deze scheiding wordt voorkomen dat één persoon of afdeling volledige controle heeft over een proces, waardoor de kans op fouten, misbruik of ongewenste beïnvloeding aanzienlijk wordt verkleind. Functiescheiding draagt daarmee bij aan transparantie, controleerbaarheid en een integere bedrijfsvoering.

Binnen het kader van informatiebeveiliging zorgt het team Identity & Access Management (IAM) ervoor dat geautoriseerde gebruikers toegang hebben tot systemen en gegevens, in overeenstemming met hun functies en verantwoordelijkheden. De uitvoering van functiescheiding is belegd bij het team IAM, dat verantwoordelijk is voor de inrichting en het beheer van toegangsrechten. Door deze integrale aanpak ondersteunt IAM de toepassing van functiescheiding en draagt het bij aan het minimaliseren van beveiligingsrisico's. Team IAM valt onder de afdeling Beheer & Ondersteunen (B&O).

De functioneel beheerders, welke ook vallen onder de afdeling B&O, zorgen voor de autorisaties van gebruikers binnen een systeem.

5 Monitoring

Iedere medewerker, ingehuurde kracht of andere persoon die namens GGD GHOR Nederland werkzaamheden uitvoert, is verplicht om een geheimhoudingsverklaring en gedragscode te ondertekenen. Deze documenten leggen de nadruk op het zorgvuldig, integer en vertrouwelijk omgaan met alle gegevens van GGD GHOR Nederland en haar klanten, inclusief persoonsgegevens en gevoelige informatie over de volksgezondheid.

In het kader van de Europese NIS2-richtlijn en nationale wetgeving ter bevordering van de digitale weerbaarheid, voert GGD GHOR Nederland structurele monitoring uit op het gebruik van haar informatiesystemen. Deze monitoring is gericht op het vroegtijdig detecteren van afwijkend of potentieel kwaadaardig gedrag, ongeautoriseerde toegang en incidenten die kunnen duiden op beveiligingsinbreuken of niet-naleving van interne beleidsregels. Voor deze monitoring wordt gebruikgemaakt van een Security Information and Event Management (SIEM)-systeem dat loggegevens, toegangsactiviteiten en systeemhandelingen continu analyseert.

De inzet van monitoring vindt plaats binnen duidelijke juridische en ethische kaders. De scope, aard en intensiteit van de monitoring zijn afgestemd met de Ondernemingsraad, in lijn met de beginselen van proportionaliteit en subsidiariteit. Medewerkers worden geïnformeerd over deze maatregelen via het informatiebeveiligingsbeleid en het privacyreglement.

Onregelmatigheden, zoals inloggen vanaf ongebruikelijke locaties, buiten kantoortijden of door andere dan de bevoegde gebruiker, worden gesignaleerd en onderzocht.
Alle relevante loggegevens en vastgelegde handelingen worden bewaard conform de toepasselijke wetgeving, met een bewaartermijn van maximaal vijf jaar, tenzij wettelijke of contractuele verplichtingen een langere termijn vereisen.

De uitvoering van dit hoofdstuk is belegd bij het Security Operations Center (SOC), dat valt onder de afdeling B&O.

6 Overige beleidsdocumenten

Ter verdere invulling van de informatiebeveiliging van GGD GHOR Nederland zijn aanvullende, specifieke beleidsdocumenten ontwikkeld en gedocumenteerd. Deze documenten behandelen gedetailleerde aspecten van informatiebeveiliging die specifieke aandacht vereisen binnen de organisatie.

Beleid voor het omgaan met informatie

Dit beleidsdocument beschrijft de fundamentele regels en verantwoordelijkheden voor alle medewerkers bij het dagelijks hanteren van informatie binnen GGD GHOR Nederland. De lezer kan hierin praktische richtlijnen verwachten voor het zorgvuldig aanmaken, bewerken, opslaan, delen en vernietigen van informatie. Specifieke aandacht gaat uit naar het correct omgaan met vertrouwelijke en privacygevoelige gegevens, zoals persoonsgegevens.

Doelgroep: Dit beleid is van toepassing iedereen die toegang heeft tot informatie van GGD GHOR Nederland.

Beleid voor classificatie van informatie

In dit document wordt het raamwerk vastgelegd voor het waarderen en beveiligen van informatie op basis van de gevoeligheid voor de organisatie. De lezer vindt hierin een officieel classificatieschema met duidelijke niveaus (bijvoorbeeld openbaar, intern, vertrouwelijk, zeer vertrouwelijk). Per niveau worden de eisen beschreven ten aanzien van vertrouwelijkheid, integriteit, beschikbaarheid en privacy (BIV-P). Het beleid legt de verantwoordelijkheid voor het classificeren van informatie bij de informatie-eigenaar en beschrijft de procedures voor het labelen en periodiek herzien van de classificatie.

Doelgroep: Primair gericht op informatie-eigenaren, applicatiebeheerders en het management. Secundair is het relevant voor alle medewerkers die informatie creëren, zodat zij deze op de juiste wijze kunnen classificeren en behandelen.

Beleid voor toegangsbeveiliging

Dit beleid waarborgt dat toegang tot informatiesystemen, applicaties en data uitsluitend wordt verleend aan geautoriseerde personen op basis van de principes 'need-to-know' en 'least privilege'. De lezer kan in dit document de uitgangspunten en regels vinden voor het beheren van de logische en fysieke toegang. Het beschrijft het volledige proces voor het aanvragen, verlenen, wijzigen, periodiek controleren en intrekken van toegangsrechten. De basis voor autorisatie is altijd de functie of taak van de medewerker.

Doelgroep: Dit beleid is relevant voor alle gebruikers van IT-middelen, leidinggevenden (in hun rol als autorisatieverlener), IT-beheerders, applicatie-eigenaren en de HR-afdeling.

Beleid voor leveranciers

Aangezien GGD GHOR Nederland nagenoeg haar volledige IT-infrastructuur en -beheer heeft uitbesteed, is dit beleid van cruciaal belang. De verantwoordelijkheid voor de bescherming van onze informatie blijft immers bij de organisatie, ook wanneer de verwerking door externe partijen wordt uitgevoerd. Dit document beschrijft de beheersmaatregelen om de risico's te mitigeren die ontstaan

door de toegang van leveranciers tot de informatie en systemen van GGD GHOR Nederland. De lezer kan hierin de informatiebeveiligingseisen vinden die worden gesteld aan leveranciers en die contractueel moeten worden vastgelegd. Het beleid omvat de gehele levenscyclus van een leveranciersrelatie: van de selectie en screening tot de contractering, de monitoring tijdens de dienstverlening en de veilige beëindiging van de relatie.

Doelgroep: Primair bedoeld voor de afdeling inkoop, contractmanagers, projectleiders en iedere medewerker die verantwoordelijk is voor het aansturen of beheren van een leverancier.

Beleid voor het ISMS

Dit beleidsdocument fungeert als het overkoepelende raamwerk voor het managementsysteem voor informatiebeveiliging (ISMS). Het beschrijft de structuur en aanpak waarmee GGD GHOR Nederland haar informatiebeveiliging beheerst, controleert en continu verbetert, conform de eisen van normen zoals de ISO 27001 en de NEN 7510. De lezer vindt hierin de structuur van het ISMS, de vastgestelde rollen en verantwoordelijkheden (zoals die van de CISO), de processen voor risicomanagement, interne audits en directiebeoordelingen. Het document legt de basis voor alle andere onderliggende beleidsdocumenten.

Doelgroep: Voornamelijk gericht op de directie, het management, de CISO (Chief Information Security Officer), security officers en (interne en externe) auditors.

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl