Beleid voor leveranciers

Inhoudsopgave

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.01	23-05-2025		Initiële versie	Opzet
0.01	16-06-2025		Akkoord Compliance Office	Beoordeling Compliance
0.70	17-07-2025		Reviews verwerkt	Concept
1.0	19-02-2026		Uitvoeren jaarlijkse review	Concept

Gecontroleerd door

Versie	Datum	Naam	Functie
0.01	03-07-2025		CISO
1.01	10-03-2026		CISO

Geautoriseerd door

Versie	Datum	Naam	Functie
1.00	28-08-2025		CISO
1.01			CISO

Gerelateerde documenten

Documenttitel
IB-maatregelenbaseline
Beleid voor het ISMS
Beleid voor classificatie van informatie
IB-beleid
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	CISO

1 Inleiding

Binnen GGD GHOR Nederland is informatiebeveiliging, inclusief de beveiliging van persoonlijke gezondheidsinformatie, integraal onderdeel van de bedrijfsvoering. Omdat alle ICT-diensten zijn uitbesteed, is dit leveranciersbeleid opgesteld ter borging van vertrouwelijkheid, integriteit, beschikbaarheid en privacy van informatie bij externe dienstverleners.
GGD GHOR Nederland beschikt over een schriftelijk informatiebeveiligingsbeleid, formeel goedgekeurd door het hoogste management en jaarlijks of na een ernstig incident herzien. Dit leveranciersbeleid sluit hierop aan en is opgenomen in contracten met alle externe partijen.

Doel en reikwijdte

Dit beleid geldt voor alle externe leveranciers die systemen, infrastructuur of applicaties beheren of diensten leveren waarbij zij toegang hebben tot informatie(systemen) van GGD GHOR Nederland. De reikwijdte beslaat de volledige levenscyclus: selectie, contractering, uitvoering, wijziging en beëindiging.

Rollen en verantwoordelijkheden voor het beleid voor leveranciers

In onderstaande tabel is de rol- en verantwoordelijkheidsverdeling toegelicht aan de hand van het RACI-model:

- R – Responsible (Uitvoerend verantwoordelijk); Degene(n) die het werk uitvoeren.
- A – Accountable (Eindverantwoordelijk); Degene die eindverantwoordelijk is voor de taak.
- C – Consulted (Geraadpleegd); Experts of belanghebbenden die advies geven.
- I – Informed (Geïnformeerd); Personen die op de hoogte moeten worden gehouden.

Activiteit	Directie	CISO	Service Level Management	Leveranciers	Compliance	Inkoop & Contract management	Privacy
Eigenaar	A	R	I	I	C	I	C
Beleidsvoorbereiding	A	R	C	I	C	C	C
Beleidsbepaling	A	R	I	I	C	I	C
Coördinatie	I	A	C	I	C	R	I
Beleidsinrichting	I	A	R	I	C	R	C
Beleidsuitvoering	I	C	A	R	I	C	I
Beleidscontrole	I	A	C	I	R	C	C

2 Proces

Het waarborgen van informatiebeveiliging in leveranciersrelaties begint met het zorgvuldig opzetten van contracten. Tijdens deze contractmanagementfase worden duidelijke afspraken gemaakt over de verantwoordelijkheden van de leverancier, inclusief specifieke eisen op het gebied van informatiebeveiliging. Deze eisen worden vastgelegd in contracten en Service Level Agreements (SLA's), waarin onder andere wordt bepaald hoe de beschikbaarheid, integriteit en vertrouwelijkheid van data worden gewaarborgd. Ook wordt vastgelegd welke beveiligingsmaatregelen de leverancier moet nemen.

Na het opstellen van het contract volgt het leveranciersmanagement, waarbij de dienstverlening van de leverancier structureel wordt gecontroleerd. Dit houdt in dat de organisatie periodiek beoordeelt of de leverancier nog steeds voldoet aan de afgesproken informatiebeveiligingsmaatregelen. Deze controles kunnen bestaan uit interne en externe audits, het monitoren van prestaties en het evalueren van rapportages over beveiligingsincidenten. Op tactisch niveau speelt het CISO Office een centrale rol bij het beoordelen van de effectiviteit van de getroffen informatiebeveiligingsmaatregelen en het waarborgen dat deze aansluiten bij de bedrijfsbehoeften en het risicoprofiel van de organisatie. Door deze gelaagde aanpak van contractmanagement tot leveranciersmanagement en tactische beoordelingwordt informatiebeveiliging structureel geborgd binnen alle fasen van de leveranciersrelatie.

3 Eisen aan leveranciers

De specifieke technische en organisatorische maatregelen die per leverancier gelden, worden vastgesteld op basis van de BIVP-classificatie en uitgewerkt in de IB-maatregelenbaseline. In contracten en SLA's wordt expliciet verwezen naar dit beleid en de actuele IB-maatregelenbaseline. Tevens zijn generieke eisen voor informatiebeveiliging opgenomen in de vigerende inkoopvoorwaarden zoals de GIBIT. De maatregelen uit de IB-maatregelenbaseline geven invulling aan onder andere de volgende eisen:

Contractuele en organisatorische eisen

- Functionele regievoering op het gebied van informatiebeveiliging is een gedeelde verantwoordelijkheid tussen GGD GHOR Nederland en haar leveranciers, waarbij gezamenlijke afspraken en voortdurende afstemming cruciaal zijn voor het waarborgen van de informatiebeveiliging.
- Voor alle uitbestede IT-infrastructuur en -diensten dient de leverancier aantoonbaar te zorgen voor adequaat capaciteitsmanagement. Dit omvat het proactief monitoren, analyseren en plannen van de benodigde IT-resources om de afgesproken prestaties en beschikbaarheid tijdens de volledige dienstverlening te garanderen.
- Voor alle uitbestede IT-infrastructuur en -diensten dient de leverancier aantoonbaar te zorgen voor adequaat kwetsbaarhedenbeheer. Dit omvat het proactief identificeren, evalueren en mitigeren van technische kwetsbaarheden om de veiligheid en integriteit van de dienstverlening te garanderen.
- In alle overeenkomsten met leveranciers worden eisen op het gebied van informatiebeveiliging opgenomen, passend bij de aard van de dienstverlening.

- Leveranciers zijn verplicht informatiebeveiliging te borgen binnen de gehele ICT-toeleveringsketen, inclusief onderaannemers. Dezelfde beveiligingseisen dienen contractueel te worden opgelegd aan onderaannemers, en naleving moet aantoonbaar zijn.
- Wijzigingen in de dienstverlening die impact kunnen hebben op informatiebeveiliging moeten vooraf worden gemeld, beoordeeld en beheerd.
- Bij het leveren van clouddiensten moet de leverancier kunnen aantonen dat passende beveiligingsmaatregelen zijn getroffen en moet transparantie worden geboden over de locatie en verwerking van data.
- Bij aanvang van de overeenkomst dienen regels voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen te worden vastgesteld.
- Alle processen, procedures en/of voorwaarden voor de informatiebeveiligingsmaatregelen dienen te zijn vastgesteld en afgestemd conform de eisen van GGD GHOR Nederland.
    - Een voorbeeld hiervan is het proces van het intrekken van autorisaties van het personeel van de leverancier.

Technische en operationele beveiliging

- Apparatuur, bekabeling en nutsvoorzieningen dienen fysiek en logisch beveiligd te zijn.
- Apparatuur dient veilig te worden verwijderd of hergebruikt.
- Technische security logging met automatiche real-time monitoring dient geïmplementeerd te zijn.
- Eindgebruikersapparaten moeten adequaat worden beheerd en beveiligd.
- Gegevensbescherming is verplicht, waaronder het wissen van informatie, maskeren van gegevens, voorkomen van datalekken en het maken van back-ups.
- Logging, kloksynchronisatie en het beheer van systeemhulpmiddelen moeten zijn ingericht.
- Alleen geautoriseerde en gecontroleerde software mag op operationele systemen worden geïnstalleerd. Speciale toegangsrechten worden strikt beheerd.
- Netwerkcomponenten moeten beveiligd zijn; netwerksegmentatie en webfilters zijn vereist. Cryptografie, conform huidige best practices, wordt toegepast waar nodig.
- Beveiliging is een integraal onderdeel van de ontwikkelcyclus, inclusief veilige architectuur, veilig coderen, testen van beveiliging en scheiding van ontwikkel-, test- en productieomgevingen.
- Registraties moeten worden beschermd conform het passende classificatieniveau, rekening houdend met het type registratie; authenticatie dient veilig te zijn ingericht. Bescherming tegen malware, beheer van kwetsbaarheden en goed configuratiebeheer zijn verplicht.
- Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.

Ontwikkeling, Testen, Acceptatie en Productie (OTAP)

- De leverancier hanteert een duidelijke fysieke en/of logische scheiding tussen ontwikkel-, test-, acceptatie- en productieomgevingen om ongeautoriseerde toegang en ongewenste wijzigingen te voorkomen.
- In ontwikkel- en testomgevingen wordt uitsluitend gebruikgemaakt van geanonimiseerde of synthetische data; het gebruik van productiegegevens is niet toegestaan. In uitzonderlijke gevallen kan, na toestemming van GGD GHOR Nederland, worden afgeweken van deze eis.
- Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.
- Voor elke overgang tussen OTAP-fasen (bijvoorbeeld van test naar acceptatie of productie) worden verplichte beveiligings- en functionele testen uitgevoerd en aantoonbaar vastgelegd.

- Toegang tot productieomgevingen is strikt beperkt tot geautoriseerd personeel; alle toegangs- en wijzigingsactiviteiten worden gelogd en periodiek geëvalueerd.
- Wijzigingen aan systemen of applicaties worden uitsluitend via een formeel change management-proces doorgevoerd, inclusief risicobeoordeling, goedkeuring en documentatie van de uitgevoerde wijzigingen.
- Implementaties in de productieomgeving worden vooraf afgestemd met GGD GHOR Nederland, bij voorkeur buiten kritieke uren, en voorzien van fallback-scenario's voor snelle terugdraaiing bij incidenten.
- Periodiek worden onafhankelijke audits en evaluaties uitgevoerd op het OTAP-proces, waarbij rapportages en verbetermaatregelen worden gedeeld met GGD GHOR Nederland.

Eisen aan onderaannemers

- Leveranciers zijn verplicht alle relevante beveiligingseisen door te leggen aan hun onderaannemers en moeten zorgen voor aantoonbare naleving in de gehele keten.
- Op verzoek wordt inzicht gegeven in de keten van onderaannemers en hun naleving van de gestelde eisen.

Periodieke rapportages en evaluaties

- Leveranciers leveren periodiek (minimaal jaarlijks, of vaker indien overeengekomen) rapportages aan over de status van informatiebeveiliging, incidenten, uitgevoerde controles en eventuele verbetermaatregelen.
- Tijdens periodieke evaluaties worden prestaties, incidenten en compliance met de gestelde eisen besproken. Indien nodig worden verbetermaatregelen afgesproken en opgevolgd.

Recht op audit

- GGD GHOR Nederland behoudt zich het recht voor om (zelf of door een derde partij) audits uit te voeren bij de leverancier en relevante onderaannemers om naleving van dit beleid en de IB-maatregelenbaseline te controleren.
- Leveranciers dienen volledige medewerking te verlenen aan audits, assessments en het opvragen van relevante documentatie en verklaringen.
- Bevindingen uit audits kunnen aanleiding geven tot aanvullende eisen of corrigerende maatregelen.
- Elke vorm van testen, zoals audits en pentesten, mogen geen gevaar opleveren voor het primaire proces.

4 Zorgspecifieke eisen

Leveranciers die persoonlijke gezondheidsinformatie verwerken, moeten aantoonbaar zorgen voor unieke en betrouwbare identificatie van iedere zorgontvanger. Dit betekent dat systemen en processen zo ingericht zijn dat persoonsverwisseling wordt voorkomen en dat altijd duidelijk is welke gegevens bij welke persoon horen. Dit is essentieel voor zowel patiëntveiligheid als privacybescherming.

Leveranciers van zorgsystemen zijn verplicht om hun systemen zodanig in te richten dat logging plaatsvindt conform de eisen van NEN 7513. Dit houdt in dat alle relevante acties met betrekking tot persoonlijke gezondheidsinformatie – zoals toegang, inzage, wijziging en uitwisseling – volledig en volgens de specificaties van NEN 7513 worden vastgelegd.

Daarnaast dienen leveranciers ervoor te zorgen dat alle getoonde of geprinte gezondheidsgegevens gevalideerd worden voordat deze aan gebruikers of zorgprofessionals worden gepresenteerd. Dit voorkomt fouten en garandeert dat alleen juiste en actuele informatie wordt verstrekt, wat cruciaal is voor het nemen van medische beslissingen en het voorkomen van misverstanden in de zorgketen.

Tot slot moeten leveranciers een grondige analyse en specificatie uitvoeren van de informatiebeveiligingseisen die gelden voor hun systemen en dienstverlening. Dit houdt in dat risico's worden geïnventariseerd, passende beveiligingsmaatregelen worden vastgesteld en dat deze maatregelen aantoonbaar worden geïmplementeerd en onderhouden. Zo wordt de vertrouwelijkheid, integriteit en beschikbaarheid van persoonlijke gezondheidsinformatie structureel geborgd.

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl