# Informatiebeveiligingsbeleid Zorgbalans

**Document kenmerken**

| | |
|---|---|
| **Titel:** | Informatiebeveiligingsbeleid Zorgbalans |
| **Versie:** | 0.4 |
| **Status:** | Onder voorbehoud van wijzigingen vanuit medezeggenschap |

# Inhoudsopgave

# 1 Informatiebeveiliging

## 1.1 Inleiding

Goede informatiebeveiliging is onlosmakelijk verbonden met goede zorg en goed werk. Kwaliteit van zorg en werk is namelijk ook hoe zorgvuldig je als Zorgbalans omgaat met privacygevoelige informatie van onze cliënten en medewerkers. Behalve de kwaliteit wordt ook de continuïteit van zorg en werk direct geraakt als de beveiliging van ICT-systemen niet op orde is en deze daardoor (tijdelijk) uitvallen.

Dit document omschrijft het informatiebeveiligingsbeleid van Zorgbalans en dient als uitgangspunt voor het inrichten van de informatiebeveiliging. Het document is geschreven om de medewerkers van Zorgbalans en andere belanghebbenden op de hoogte te stellen van doelstellingen en processen aangaande informatiebeveiliging. Intern zal het beleid gecommuniceerd worden aan alle medewerkers via MijnZorgbalans. Extern zal het beleid gecommuniceerd worden via de website van Zorgbalans.

## 1.2 Informatiebeveiliging

Bedreigingen van een veilige en betrouwbare informatievoorziening kunnen fysiek van aard zijn, zoals brand en wateroverlast. Maar ook technisch, bijvoorbeeld in de vorm van storingen in programmatuur, apparatuur of de stroomvoorziening. De informatievoorziening kan ook worden bedreigd door (on)opzettelijke fouten en vergissingen of door opzettelijke kwaadaardige acties zoals hacking, phishing, computerfraude, etc.

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die de informatievoorziening van Zorgbalans kunnen schaden, te voorkomen en/of de kans verkleinen en/of eventuele gevolgen te beperken.

## 1.3 Vervlechting informatiebeveiliging en privacy

Eisen omtrent privacy bepalen de omgang met persoonsgegevens. Bescherming van de privacy heeft consequenties voor de voorwaarden waaronder en de manier waarop persoonsgegevens opgeslagen en verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan.

De wet noemt als voorbeelden van verwerking:

> *Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

Hieruit blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy en een zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. De maatregelen die in het kader van informatiebeveiliging worden getroffen, leveren dus een bijdrage aan de bescherming van privacy gevoelige persoonsgegevens.

## 1.4 Relevante wet en regelgeving

De belangrijkste regels voor de omgang met persoonsgegevens in Nederland waren voorheen vastgelegd in de Wet bescherming Persoonsgegevens (Wbp). Echter vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing, de Wbp is daarbij komen te vervallen. Zowel Wbp als AVG verplichten Zorgbalans te zorgen voor een adequate beveiliging van persoonsgegevens.

Zorgbalans is als verwerkingsverantwoordelijke belast met de naleving van de hele AVG en kan daarop aangesproken worden. Hetzelfde geldt voor zogenaamde verwerkers, dit zijn partijen die ten behoeve van Zorgbalans persoonsgegevens verwerken. Dit kan een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan zijn die dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

In de AVG is vastgesteld dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen dienen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Deze verplichting kan worden ingevuld door te voldoen aan de bestaande (Nederlandse en internationale) normen voor informatiebeveiliging. Daarnaast moet er een specifieke verwerkersovereenkomst worden gesloten wanneer er een verwerker in het spel is, bijvoorbeeld in het geval van Medimo, ONS en Verzuimsignaal. Een dergelijke bewerkersovereenkomst regelt de verantwoordelijkheden bij de verwerking van persoonsgegevens als een bedrijf voor de verwerking een ander bedrijf inschakelt.

De NEN 7510 norm is specifiek gericht op de zorgsector en beschrijft maatregelen die zorginstellingen moeten nemen om gegevens van cliënten, medewerkers en hun systemen te beveiligen. De Autoriteit Persoonsgegevens beschouwt voor de zorgsector de NEN 7510 als “een gezaghebbende en sectorale uitwerking” van ‘passende’ technische en organisatorische maatregelen, zoals beschreven in de wet. De Inspectie Gezondheidszorg en Jeugd (IGJ) heeft aangegeven NEN 7510 te hanteren bij het toetsen van de vraag of zorginstellingen de juiste maatregelen treffen voor invoering en handhaving van informatiebeveiliging.

Naast NEN 7510 zijn ook de aanvullingen NEN 7512 en NEN 7513 van belang voor de zorgsector. NEN 7512 ziet toe op de gegevensuitwisseling tussen verschillende partijen, denk aan maatregelen over de identificatie en authenticatie van partijen die gegevens uitwisselen. NEN 7513 ziet toe op logging, zoals maatregelen over het controleren van de rechtmatigheid van toegang tot cliëntendossiers.

Als een zorginstelling de in deze normen aangegeven maatregelen heeft getroffen, wordt daarmee vastgesteld dat de instelling voldoet aan de genoemde wettelijke bepalingen. Om te voldoen aan de NEN 7510 norm heeft de directie van Zorgbalans een informatiebeveiligingsbeleid vastgesteld dat passend is voor het doel van de organisatie.

Verder is het informatiebeveiligingsbeleid een verplichting om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging en tot continue verbetering van het managementsysteem voor informatiebeveiliging.

## 1.5 Risk based

De nieuwe NEN 7510 is risk-based geworden. Dat betekent dat Zorgbalans zelf bij elk risico steeds mag afwegen (en vastleggen) waarbij de cliënt het meest is gebaat. Een risk based aanpak betekent

dat het afdekken van zorgrisico's mag prevaleren boven het afdekken van informatiebeveiligings- en privacy risico's mits dit goed is beargumenteerd (het comply-or-explain principe).

# 2 Doel en reikwijdte Informatiebeveiligingsbeleid

## 2.1 Doel

Informatiebeveiliging richt zich specifiek op de volgende drie aspecten van de informatievoorziening:

1. Beschikbaarheid, de mate waarin gegevens en/of functionaliteiten beschikbaar zijn;
2. Integriteit, gegevens moeten aantoonbaar juist en volledig zijn en de informatiesystemen moeten juiste en volledige gegevens opslaan en verwerken;
3. Vertrouwelijkheid, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die bovenstaande aspecten van de informatievoorziening van Zorgbalans kunnen schaden, te voorkomen en/of de kans te verkleinen en/of eventuele gevolgen te beperken.

Het informatiebeveiligingsbeleid van Zorgbalans is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (cliënt en medewerker) wordt gerespecteerd en Zorgbalans voldoet aan relevante wet- en regelgeving.

## 2.2 Reikwijdte

Het Informatiebeveiligingsbeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Zorgbalans waaronder in ieder geval alle cliënten, medewerkers, stagiairs, mantelzorgers en andere vrijwilligers. Maar ook van personeel dat wordt ingehuurd om diensten te verlenen aan Zorgbalans. Gegevensuitwisseling tussen Zorgbalans en andere organisaties valt ook onder het informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid geldt voor alle toepassingen van Zorgbalans, deze zijn opgenomen in het verwerkingsregister van Zorgbalans. Hieronder valt alle gecontroleerde informatie, die door Zorgbalans zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop Zorgbalans kan worden aangesproken. (b.v. uitspraken van medewerkers in discussies, op (persoonlijke pagina's van) websites en of social media.)

Het Informatiebeveiligingsbeleid geldt voor de geheel of gedeeltelijk, geautomatiseerde / systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Zorgbalans evenals op de daaraan ten grondslag liggende documenten (op papier of in een bestand).

Onder dit beleid vallen ook alle devices (ipads, laptops, telefoons) waarmee geautoriseerde toegang tot het Zorgbalans netwerk verkregen kan worden en/of privacygevoelige informatie bevatten.

## 2.3 Uitgangspunten

Zorgbalans hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging (en privacy) te bereiken:

1. De Raad van Bestuur van Zorgbalans neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt en Zorgbalans voldoet aan alle relevante wet- en regelgeving. De Raad van Bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is de Raad van Bestuur de verwerkings-verantwoordelijke.

2. Bij Zorgbalans is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Zorgbalans om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien mits dit het verlenen van zorg niet in de weg staat.

3. Zorgbalans zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, data-portabiliteit en profilering.

4. Zorgbalans legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister en zal deze up-to-date houden. Zorgbalans voldoet hiermee aan de documentatieplicht.

5. Zorgbalans sluit met alle leveranciers van bedrijfsapplicaties verwerkersovereenkomsten af als zij, in opdracht van Zorgbalans, persoonsgegevens verwerken.

6. Binnen Zorgbalans is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. Zorgbalans medewerkers worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Zorgbalans classificeert informatiesystemen op basis van beschikbaarheid, Integriteit en Vertrouwelijkheid (hoog, midden, laag) in het verwerkingsregister. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Zorgbalans kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

10. Zorgbalans neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die het verlenen van zorg, de privacy en/of de bedrijfsvoering kunnen verstoren. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt, legt Zorgbalans aanvullende afspraken vast over de technische maatregelen.

11. Zorgbalans zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens.

12. Informatiebeveiliging en privacy is bij Zorgbalans een continue proces, waarbij regelmatig (minimaal jaarlijks) de risico's en maatregelen worden geëvalueerd en wordt bekeken of aanpassing gewenst is.

# 3 Managementsysteem voor informatiebeveiliging

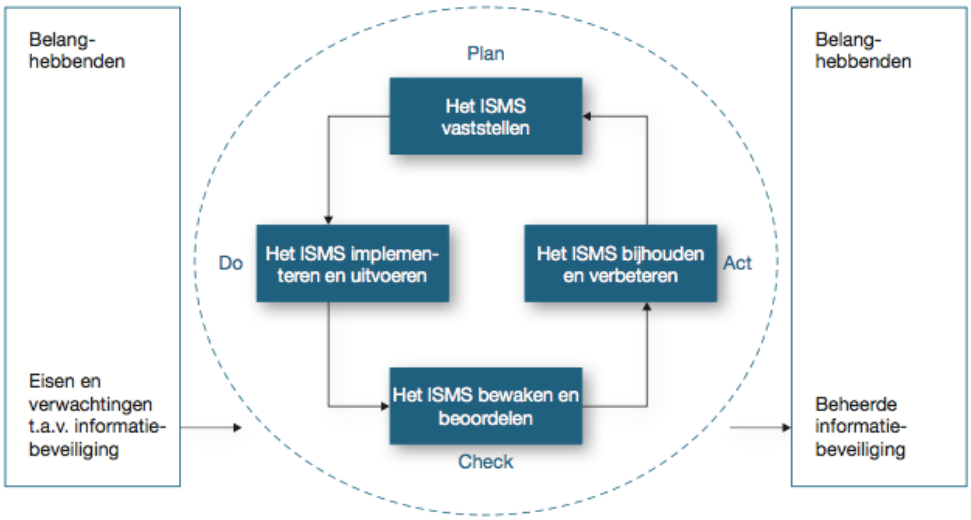
## 3.1 Normatief raamwerk

De NEN 7510 norm geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die Zorgbalans moeten treffen ter beveiliging van de informatievoorziening. Hiervoor geven de normen een normatief raamwerk in de vorm van een managementsysteem voor informatiebeveiliging (ISMS, 'Information Security Management System') dat door Zorgbalans moet worden ingericht.

Door implementatie van het managementsysteem voor informatiebeveiliging inclusief de beheersmaatregelen bij elk van de beheersdoelstellingen in de NEN 7510 kan Zorgbalans voldoen aan de eisen die in een door Zorgbalans uitgevoerde risicobeoordeling zijn vastgesteld. De NEN 7510 geeft daarmee aanwijzingen voor het organisatorisch en technisch inrichten van de informatiebeveiliging. Ze bieden zo een basis voor vertrouwen in de zorgvuldige informatievoorziening bij Zorgbalans en tussen Zorgbalans en de verschillende andere organisaties in de zorg waarmee wordt samengewerkt (bijvoorbeeld Vecozo, ziekenhuizen, apotheken, laboratoria, etc, etc.).

## 3.2 Resultaat garanderen

Het inrichten van een managementsysteem voor informatiebeveiliging (ISMS, 'Information Security Management System') is een continu proces. Om niet te verzaken in maatregelen en processen wordt de PDCA-cyclus aangehouden (PDCA, 'plan, do, check, act'). Deze cyclus geeft structurering in het proces en draagt zorg voor meetbare resultaten.




Plan - het beleid concretiseren

In deze fase wordt gekeken wat er allemaal nodig is voor het inrichten van een ISMS. Een Security Officer (CISO) zal worden aangesteld, de behoeften van belanghebbenden van de organisatie worden

onderzocht en beschreven, de scope wordt opgesteld, verantwoordelijkheden worden vastgelegd en er wordt een methode beschreven voor het uitvoeren van een integrale risicoanalyse.

Do - het beleid implementeren en uitvoeren
Het beleid uit de planfase wordt in zijn werking gezet en de integrale risico analyse wordt uitgevoerd om de waarborging van vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te bepalen. Uit deze analyse komen beheersmaatregelen voort die worden geïmplementeerd. Door implementatie van deze beheersmaatregelen bij elk van de beheers doelstellingen in deze norm kan Zorgbalans voldoen aan de eisen die in een risicobeoordeling zijn vastgesteld.

Check - het beleid evalueren
In deze fase wordt onderzocht of de ingevoerde maatregelen effect hebben gehad. Dit wordt gemeten aan de hand van een interne audit waarbij de Security Officer (CISO) nagaat waar het ISMS verbeterd kan worden.

Act - het beleid verbeteren en actueel houden
In deze laatste fase worden de verbeterpunten uit de interne audit doorgevoerd. Daarna zal de cyclus opnieuw worden doorlopen.

De resultaten van regelmatige risicobeoordeling behoren te worden afgestemd op de prioriteiten en middelen van Zorgbalans.

## 3.3 Overbrengen van belang

Om een goed ISMS in te richten, is het essentieel dat de medewerkers van Zorgbalans ook begrijpen waarom informatiebeveiliging van belang is. Zij zijn tenslotte een groot onderdeel van het ISMS en moeten daarom het belang inzien van een goedwerkend informatiebeveiligingssysteem, ook als dat betekent dat het hun werkzaamheden zal beïnvloeden. Om het bewustzijn van de werknemers te borgen en te vergroten wordt aandacht besteed aan informatieveiligheid bij nieuwe medewerkers, opleidingen en zullen er doorlopend bewustwordingscampagnes worden opgezet.

# 4 Governance

## 4.1 Controle werking en naleving van het beleid

Een belangrijk onderdeel van het organiseren van informatiebeveiliging is het vastleggen van rollen en verantwoordelijkheden. In lijn met het Zorgbalans Zekerheden (3 lines of defense) model zijn de verantwoordelijkheden als volgt belegd:

Medewerkers en leidinggevenden 1e lijn

Bewust van en handelen naar informatiebeveiligingsbeleid.

Security Officer (CISO) 2e lijn

De Security Officer is verantwoordelijk voor het onderhoud en de instandhouding van dit Informatiebeveiligingsbeleid en het managementsysteem voor informatiebeveiliging (ISMS, 'Information Security Management System').

Privacy Officer (PO) 2e lijn

Waar de SO verantwoordelijk is voor het informatiebeveiligingsbeleid is de Privacy Officer verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen Zorgbalans. Daarnaast kan de PO ondersteunen bij het in kaart brengen van de risico's door bijvoorbeeld een Privacy Impact Assessment (PIA) uit te voeren (onderdeel uit de AVG).

Functionaris Gegevensbescherming (FG) 2e lijn

De Functionaris Gegevensbescherming is verantwoordelijk voor het toezicht houden op de naleving van de privacywetten en -regels, het inventariseren en bijhouden van gegevensverwerkingen en het afhandelen van vragen en klachten van mensen binnen en buiten de organisatie. Daarnaast kan de FG ondersteunen bij het ontwikkelen van interne regelingen, het adviseren over privacy op maat én het leveren van input bij het opstellen of aanpassen van gedragscodes.

Directie(beraad) 3e lijn

Het management van Zorgbalans controleert of de Security Officer het ISMS inricht, uitvoert, evalueert en verbetert zoals beschreven in dit document. De Raad van Bestuur is uiteindelijk eindverantwoordelijk voor het informatiebeveiligingsbeleid en de implementatie daarvan binnen Zorgbalans.

Controle Zorgbalans

Een externe audit-organisatie kan Zorgbalans toetsen op het naleven van het beleid / normen.

## 4.2 Contactpersonen

**Privacy Officer (PO)**

Naam: Cora Kunz

Email c.kunz@zorgbalans.nl

Telefoon: 023-8918918

**Functionaris Gegevensbescherming (FG)**

Naam: Cora Kunz

Email c.kunz@zorgbalans.nl

Telefoon: 023-8918918

**Security Officer (CISO)**

Naam: Peter Kuijer

Email p.g.kuijer@zorgbalans.nl

Telefoon: 023-8918596