INFORMATIEBEVEILIGINGS-BELEID

Eigenaar	Directeur services
Datum	22 april 2020
Versie	2020.1.1 definitief
Vastgesteld DO	Ja, april 2020
Vastgesteld RvB	Ja, april 2020
Ter advies COR	Besproken en goedgekeurd op 22 april 2020

INHOUDSOPGAVE

REVISIEHISTORIE

Versie	Datum	Auteur	Inhoud wijziging
1.0	9 juni 2017	Martine van de Merwe	Eerste vastgestelde versie
1.1	28 februari 2018	Peter van der Zwan	Wijzigingen in verband met AVG
1.2	31 mei 2018	Peter van der Zwan	Privacybeleid aangescherpt, rollen beschreven
2020.1.0	Januari 2020	Marc Been Sieuwert van Otterloo	Meerdere wijzigingen vanwege verbetering opzet ISMS
2020.1.1	22 april 2020	Sieuwert van Otterloo	Datum goedkeuring COR toegevoegd

DISTRIBUTIE

Versie	Datum	Doelgroep	Medium
1.0	Juni 2017	Alle medewerkers	MijnIdB
1.1	Maart 2018	Projectgroep AVG	Email
1.2	Mei 2018	Regiegroep Informatieveiligheid en Privacy	
1.3	Februari 2019	Strategisch IV Overleg	Email
2020.1	Januari 2020	Directie Overleg	

1. ONDERWERP EN TOEPASSINGSGEBIED

1.1. INLEIDING

Ipse de Bruggen levert zorg aan mensen met een verstandelijke of meervoudige handicap. De dienstverlening van Ipse de Bruggen is gericht op het begeleiden, verzorgen en behandelen van cliënten. Hiervoor werken er deskundige en betrouwbare zorgprofessionals op basis van visie en vertrouwen.
Het waarborgen van de privacy van cliënten is hierbij heel belangrijk. Voor ongestoorde zorgverlening is continue beschikbaarheid van informatie noodzakelijk. Cliënten en zorgverleners wisselen (bij voorkeur digitaal) informatie uit die veelal medisch en persoonlijk, dus vertrouwelijk is. Voor het vertrouwen is het van cruciaal belang dat deze informatieverwerking en -uitwisseling veilig gebeurt.

Naast de noodzaak van toegankelijke en betrouwbare informatie voor goede zorgverlening aan cliënten zijn andere redenen om informatie te beveiligen:

- Intrinsieke motivatie om de privacy van cliënten te waarborgen.
- Vertrouwen van cliënten en andere interne en externe relaties.
- Uitvoeren van het manifest. In het manifest van Ipse de Bruggen uit 2015 worden vertrouwen en betrouwbaarheid benoemd. Daarbij gaat het erom dat cliënten erop kunnen vertrouwen dat er zorgvuldig met hun gegevens wordt omgegaan. Voor het leveren van goede zorg is beschikbaarheid van juiste en volledige informatie noodzakelijk.
- Zorgplicht. Verzekeraars hebben een zorgplicht voor het leveren van kwalitatief goede, bereikbare en tijdige zorg. Om dat als zorginstelling te kunnen leveren moet informatie juist, volledig en beschikbaar zijn.
- Belangrijk in de keten. Uitwisselen van informatie in de keten moet veilig gebeuren en de uitgewisselde informatie moet juist en volledig zijn.
- Risicobeheersing. Als informatie niet juist, tijdig en volledig beschikbaar is levert dat risico's voor de cliëntveiligheid. Als de vertrouwelijkheid wordt geschonden levert dat privacyverlies op voor de betrokkene en imagoschade voor de organisatie. Bij overtreding van wet- en regelgeving is er risico op boetes.
- Verbetering van gegevensuitwisseling. Maatregelen zorgen voor verbetering van de gegevenskwaliteit en waarborgen van de vertrouwelijkheid.
- Concurrentiepositie. Als informatiebeveiliging aantoonbaar op orde is, kan dat onderscheidend werken.
- Efficiënter werken. Maatregelen voor betere gegevenskwaliteit of efficiëntere uitwisseling kunnen fouten voorkomen en processen versnellen.
- Technische noodzaak. Het invoeren van bepaalde technische oplossingen dwingt tot het maken van keuzes op het gebied van informatiebeveiliging.
- Wetgeving. Diverse toepasselijke wet- en regelgeving schrijft informatiebeveiliging voor.

Ipse de Bruggen werkt met een risicogerichte aanpak van informatiebeveiliging. Er is een managementsysteem voor informatiebeveiliging ingericht dat Ipse de Brugge continu zal verbeteren. Dit management kan worden afgekort tot ISMS, dat staat voor 'Information Security Management System'. Het ISMS is opgezet volgens NEN 7510-1:2017, de norm voor informatiebeveiliging in de zorg.

1.2. TOEPASSINGSGEBIED

Het informatiebeveiligingsbeleid en bijbehorend managementsysteem voor informatiebeveiliging van Ipse de Bruggen heeft als toepassingsgebied(scope):

> De activiteiten voor levering van advies, begeleiding, behandeling, ondersteuning en zorg aan cliënten en de informatiesystemen, netwerken, fysieke omgeving en mensen die deze activiteiten ondersteunen.

Het beleid richt zich op eigen medewerkers, personeel niet in loondienst, cliënten, ouders, wettelijk vertegenwoordigers, vrijwilligers en personeel dat door derden wordt ingezet om diensten te verlenen aan Ipse de Bruggen en cliënten

Het informatiebeveiligingsbeleid bevat de managementafspraken tussen de Raad van Bestuur en proceseigenaren van Ipse de Bruggen. Aanvullend (operationeel) beleid is uitgewerkt in het **Informatiebeveiligingshandboek**.

2. TERMEN EN DEFINITIES

Informatiebeveiliging is een samenhangend stelsel van maatregelen dat zich richt op de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

Beschikbaarheid	De mate waarin een object (informatie, IT-dienst of IT-middel) continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.
Integriteit	De mate waarin het object (gegevens, IT-dienst of IT-middel) in overeenstemming is met de beoogde werkelijkheid (juist, tijdig, volledig).
Vertrouwelijkheid	De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruikmaken van een object (IT-dienst of IT-middel) of toegang hebben tot een object (creëren, wijzigen, verwijderen of lezen van gegevens).

Andere termen

Informatie	Informatie is voor dit beleid gedefinieerd als alle uitingsvormen (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, cd, dvd, beeldscherm et cetera) en alle informatieverwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen).
Informatiebeleid	Geheel van visies, uitspraken en voorschriften die richting geven aan de ontwikkeling en inrichting van de informatie-huishouding.
Informatiebeveiligingsbeleid	Geheel van visies, uitspraken en voorschriften die richting geven aan maatregelen alsmede procedures en processen die de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie binnen een organisatie garanderen. Informatiebeveiliging gaat vooral om mensen en processen. Het is meer dan ICT, computers en automatisering
Informatievoorziening (IV)	Het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie. Binnen Ipse de Bruggen is de afdeling IV onderdeel van de directie Services.
Maatregel	Technische en organisatorische voorzieningen om risico's te beheersen.
Risico	Het product van de kans op een ongewenste gebeurtenis en het (geschatte) effect waarmee deze op kan treden

3. LEIDERSCHAP

De Raad van Bestuur is eindverantwoordelijk voor het ISMS en draagt zorg voor opzetten en instandhouden van het informatiebeveiligingsbeleid.

De Raad van Bestuur zal hiervoor het volgende doen:

a) informatiebeveiligingsdoelstellingen vaststellen die aansluiten bij het manifest van Ipse de Bruggen;

b) de eisen van het ISMS in de processen van de organisatie integreren;
c) ervoor zorgen dat de benodigde middelen voor het inrichten, implementeren, onderhouden en continu verbeteren van het ISMS beschikbaar zijn;
d) het belang van doeltreffend informatiebeveiligingsmanagement en de eisen aan een ISMS uitdragen;
e) bewerkstelligen dat het ISMS zijn beoogde doelstellingen behaald;
f) mensen aansturen om een doeltreffend ISMS te realiseren;
g) continue verbetering bevorderen;
h) directeuren en managers ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

De Raad van Bestuur verbindt zich tot de implementatie en het beheer van richtlijnen, procedures en maatregelen met als doel het bewaken en continue verbeteren van de informatiebeveiliging.

4. DOELSTELLING INFORMATIEBEVEILIGING

Het doel van het informatiebeveiligingsbeleid is aantoonbaar te voldoen aan wettelijke eisen, contractuele afspraken en redelijke verwachtingen van betrokkenen op het gebied van informatiebeveiliging en daarmee het risico op schade of informatiebeveiligingsincidenten te minimaliseren.

Dit doel is in het Informatiebeveiligingshandboek uitgewerkt in meetbare doelstellingen en performance-indicatoren (KPI's).

5. PLANNING

Ipse de bruggen voert een risico-analyse uit om de gevolgen van bedreigingen te analyseren en op grond hiervan een passend beveiligingsniveau te bepalen. Risico's en kansen worden geïnventariseerd en aangepakt op basis van een risico- en kansenregister. Dit register wordt minimaal jaarlijks bijgewerkt. De risiscomanagement-methode is verder uitgewerkt in het Informatiebeveiligingshandboek.

In het Informatiebeveiligingshandboek is eveneens bepaald op welke manier:

- te treffen maatregelen gepland, geïntegreerd en geïmplementeerd zullen worden;
- de doeltreffendheid van deze maatregelen zal worden geëvalueerd;
- informatiebeveiligingsrisico's zullen worden beoordeeld;
- informatiebeveiligingsrisico's zullen worden behandeld.

6. ONDERSTEUNING

Ipse de Bruggen zal ervoor zorgen dat de personen die zich met informatiebeveiliging bezighouden over voldoende scholing, opleiding of ervaring beschikken en als deze ontbreekt de nodige aanvullende competente personen contracteren.

Het is belangrijk dat het informatiebeveiligingsbeleid en de hieruit volgende principes en richtlijnen bekend zijn bij alle betrokkenen binnen Ipse de Bruggen. De Security Officer is verantwoordelijk voor de communicatie rondom het beleid. Het bevorderen van het beveiligingsbewustzijn bij management en medewerkers vormt een belangrijk aandachtspunt bij deze communicatie en de Raad van Bestuur en directeurs spelen hier een actieve rol in.

Het ISMS en alle bijbehorende gedocumenteerde informatie zal worden bijgehouden in een daarvoor geschikte online omgeving, en zal op diverse wijzen bekend gemaakt worden aan belanghebbenden.

7. UITVOERING

De volgende onderdelen zijn nader uitgewerkt in het Informatiebeveiligingshandboek en de Raad van Bestuur zal voor de uitvoering middelen beschikbaar stellen, deelverantwoordelijkheden aangeven en de effectiviteit bewaken:

- Operationele planning en beheersing;
- Risicobeoordeling door (lijn)management;
- Behandelen van informatiebeveiligingsrisico's.

8. EVALUATIE VAN DE PRESTATIES

De Raad van Bestuur definieert metrieken en doelstellingen voor het monitoren, meten, analyseren en evalueren van de doeltreffendheid van het ISMS. De Security Officer is verantwoordelijk voor het maken van analyses en rapporteren over de werking van het ISMS.

De interne auditor van Ipse de Bruggen stelt het interne auditprogramma vast, is verantwoordelijk voor uitvoering en rapportage van de resultaten.

Minimaal eens per jaar zal de Raad van Bestuur dit informatiebeveiligingsbeleid evalueren met oog op continue verbetering. De Security Officer zal het beleid aandragen voor evaluatie. Bij de beoordeling van het beleid wordt gekeken of ontwikkelingen in de organisatie (zoals wijzigingen aan de IT-infrastructuur) en de omgeving (zoals nieuwe risico's en wet- en regelgeving) aanpassing van het beleid noodzakelijk maken. Ook worden in- en externe signalen en incidentrapporten beoordeeld om vast te stellen of aanpassing van het beleid nodig is. Uiteraard is het medewerkers toegestaan om ook gedurende het jaar verbeteractiviteiten uit te voeren.

Afwijkingen van het ISMS zullen worden geregistreerd en conform NEN 7510 worden behandeld. In het Informatiebeveiligingshandboek is beschreven op welke wijze correctieve acties worden getroffen en gemonitord.

BIJLAGE A – ROLLEN

Alle bedrijfsonderdelen binnen onze organisatie zijn bij informatiebeveiliging betrokken. In deze bijlage worden de verantwoordelijkheden die horen bij verschillende rollen beschreven.

De Raad van Bestuur wordt voor uitvoering van dit beleid ondersteund door twee teams:

- Informatiebeveiliging & Privacy kernteam – IB&P team (privacy officer, security officer, informatie architect, technisch architect, adoptiecoach)
- Privacy en Informatiebeveiligings-Team PIT (IB&P kernteam + directeur services)

PORTEFEUILLEHOUDER INFORMATIEBEVEILIGING

De Raad van Bestuur is eindverantwoordelijk voor alle activiteiten binnen Ipse de Bruggen en dus ook voor informatiebeveiliging. Binnen het bestuur is een portefeuillehouder informatiebeveiliging aangewezen. De portefeuillehouder is vanuit het bestuur verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid.

De bestuursverantwoordelijkheid voor informatiebeveiliging omvat:

- het vaststellen van dit informatiebeveiligingsbeleid;
- het toezien op de naleving van het informatiebeveiligingsbeleid door de organisatieonderdelen;
- het evalueren van de toepassing en werking van het informatiebeveiligingsbeleid op basis van rapportages over informatiebeveiliging.

De Directeur Services kan door de portefeuillehouder gemandateerd worden om organisatiebrede richtlijnen voor informatiebeveiliging op te stellen die voortkomen uit dit bestuurlijke informatiebeveiligingsbeleid.

PROCESEIGENAREN

Ipse de Bruggen kent verschillende bedrijfsonderdelen die worden aangestuurd door directeuren. De directeuren zijn de proceseigenaren en op grond daarvan verantwoordelijk voor het voeren van regie over de activiteiten binnen hun bedrijfsonderdelen en het beschikbaar stellen van de juiste mensen en middelen voor uitvoeren van het beleid. Ook zullen proceseigenaren als risico-eigenaar of maatregel-eigenaar moeten optreden of eigenaren aanwijzen.

Het voeren van regie betekent dat directeuren verschillende lijnmanagers aansturen. Zie ook de beschrijving hieronder van Lijnmanagement.

SECURITY OFFICER

Bij Ipse de Bruggen is de (Information) Security Officer de spin in het web met betrekking tot informatiebeveiliging. Op hoofdlijnen omvat deze rol de volgende verantwoordelijkheden:

- toezicht houden op de naleving van de wet- en regelgeving, normen en standaarden met betrekking tot informatieveiligheid binnen Ipse de Bruggen;
- beleidsvorming, het beheren van het Ipse de Bruggen-brede informatiebeveiligingsbeleid en de hieruit voortvloeiende Ipse de Bruggen-brede richtlijnen en procedures, waaronder het informatiebeveiligingshandboek;
- controle en registratie, het bewaken van het niveau van informatiebeveiliging binnen Ipse de Bruggen;
- aanspreekpunt voor incidenten, de afhandeling, registratie en evaluatie hiervan;
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij management en (tijdelijke) medewerkers (in duidelijke en begrijpelijke taal);

- evaluatie en advies, het adviseren van de Raad van Bestuur en andere leidinggevenden over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen Ipse de Bruggen.

LIJNMANAGEMENT

Het management van de diverse bedrijfsonderdelen is verantwoordelijk voor de inrichting en uitvoering van de primaire en secundaire bedrijfsprocessen.

De verantwoordelijkheid voor de bedrijfsprocessen omvat ook de beveiliging van de informatie en de ICT-infrastructuur waarvan het organisatieonderdeel eventueel zelf (risico)eigenaar is. Het lijnmanagement kan hierbij een beroep doen op advies en ondersteuning door de Security Officer.

De verantwoordelijkheid van het lijnmanagement omvat onder andere de volgende taken:

- positieve en actieve houding ten aanzien van informatiebeveiliging;
- fungeren als voorbeeldfunctie;
- toezicht houden op de naleving van Informatiebeveiligingsmaatregelen;
- medewerking verlenen aan verbeteracties;
- autoriseren van medewerkers;
- informatiebeveiliging behandelen in werkoverleg en beoordelingen;
- afhandelen van vertrouwelijke informatiebeveiligingsincidenten.

EIGENAAR SYSTEEM / APPLICATIE

De eigenaar van een systeem/applicatie is verantwoordelijk voor het functioneren en de ontwikkeling van een systeem / applicatie. De eigenaar is vaak de persoon die verantwoordelijk is voor het proces dat een systeem / applicatie ondersteunt. Hij beschikt over het budget voor beheer, onderhoud en verniewing, en stelt de prioriteiten. Hij is derhalve ook verantwoordelijk voor de maatregelen met betrekking tot informatiebeveiliging en risicomanagement. Als uitvloeisel hiervan stelt hij bijvoorbeeld ook de autorisatiematrix vast voor de applicatie.

FUNCTIONEEL BEHEERDER

De functioneel beheerder is namens de systeemeigenaar verantwoordelijk voor de continuiteit en het optimaal functioneren van het betreffende systeem / applicatie (kwaliteit). Hij richt zich op de inrichting en het beheer van de applicatie, ondersteuning van de gebruikers en beheer van de functionele documentatie. De functioneel beheerder heeft een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit. Concrete taken zijn problem- en change management, afhandeling incidenten, autorisatiebeheer, begeleiden acceptatietesten, incident management en documentbeheer.

MEDEWERKER

Alle medewerkers moeten zorgvuldig omgaan met informatie, zeker als het persoonsgegevens betreft of zorginformatie.

Namens de Raad van Bestuur zal er gezorgd worden voor passende en begrijpelijke instructies en voor trainingen en informatiemateriaal dat past bij de functie. Medewerkers moeten instructies voor informatiebeveiligingsbeleid naleven, trainingen volgen, meewerken aan de uitvoering van het beleid en incidenten en afwijkingen melden.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid.

De betrokkenheid van medewerkers vertaalt zich naar hun eigen handelen en in communicatie naar clienten en hun vertegenwoordigers.

LEIDINGGEVENDE

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het Informatiebeveiligingsbeleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen, bijvoorbeeld in werkoverleggen en beoordelingen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde beveiligingsonderwerpen.

BIJLAGE B – AANVULLENDE DOCUMENTATIE

Het Ipse de Brugge informatiebeveiligingsbeleid is verder uitgewerkt in de volgende documenten:

- Verklaring van toepasselijkheid (een overzicht van van toepassing zijnde beheersmaatregelen)
- Informatiebeveiligingshandboek
- Privacybeleid Ipse de Bruggen
- Privacyreglementen (Privacyreglement Cliënten en Privacyreglement Medewerkers)
- Regeling aanvaardbaar gebruik ICT bedrijfsmiddelen
- Procedures en werkdocumenten, zoals genoemd in het Informatiebeveiligingshandboek