Informatiebeveiligingsbeleid

Inleiding

Als zorginstelling is Profila Zorg verantwoordelijk voor goede en veilige zorg aan haar cliënten. Bij het uitvoeren van deze taak staat het leveren van kwaliteit voorop. Om deze kwaliteit aan de cliënten en andere betrokkenen te kunnen bieden, is een veilige opslag, verwerking en uitwisseling van gegevens essentieel. De beveiliging van gegevens moet zijn gewaarborgd ongeacht de vorm, dus zowel handmatig, bijvoorbeeld in cliëntendossiers en MDO verslagen, als geautomatiseerd, denk aan het gebruik van het elektronisch cliëntendossier, internet en e-mail.

Naast het zorgvuldig beheren van cliëntgegevens, dient ook het beheer van bedrijfsgegevens en medewerker gegevens zorgvuldig te gebeuren. Daar waar externen, zoals toeleveranciers, werken binnen Profila Zorg, dienen zij zich te houden aan het informatiebeleid van de organisatie.

Een veilige opslag van informatie is van essentieel belang voor de continuïteit van de bedrijfsvoering van de organisatie. Zowel op papier als geautomatiseerd zijn wij bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Onze organisatie en onze informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren.

Doel

Dit document beschrijft het beleid van Profila Zorg met betrekking tot de beveiliging van privacy gevoelige en bedrijfseconomische informatie.
Dit beleid is vastgelegd in het onderhavige document dat door de Raad van Bestuur is vastgesteld. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging binnen de organisatie.

Definitie van informatiebeveiliging
Informatiebeveiliging wordt als volgt gedefinieerd:
Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen.

Opgemerkt wordt dat informatiebeveiliging een samenhangend stelsel van maatregelen omvat. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen, niet los van elkaar worden getroffen, maar in onderlinge samenhang staan.

Het stelsel van beveiligingsmaatregelen heeft tot doel een blijvend niveau van beveiliging te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd.

Doelstelling informatiebeveiligingsbeleid
Het opstellen van het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen Profila Zorg vast te leggen zodat we voldoen aan de NEN-norm 7510, Informatiebeveiliging in de zorg (hoofdstuk 5 Beveiligingsbeleid en hoofdstuk 6 Organiseren van informatiebeveiliging).

Informatiebeveiliging is gericht op het realiseren van een optimaal niveau van beveiliging. Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten. Daarnaast is het opstellen van informatiebeleid een zorgvuldige afweging tussen optimale veiligheid, praktische haalbaarheid en werkbaarheid. Misschien helaas, is het zo dat de NEN 7510 geen blauwdruk heeft ontwikkeld voor wat 'goede informatiebeveiliging' is. Informatiebeleid vraagt van ons als zorgaanbieder steeds weer afwegingen te maken. De systeembeheerder van Profila Zorg speelt hierin een belangrijke rol.

Doelstelling informatiebeveiliging
Informatiebeveiliging richt zich op de volgende drie aspecten van de informatievoorziening:

- Beschikbaarheid, de informatie moet op de gewenste momenten beschikbaar zijn;
- Integriteit, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- Vertrouwelijkheid, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Reikwijdte

Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie van Profila Zorg. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van Profila met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

Inhoud

1. Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen Profila Zorg worden de volgende uitgangspunten gehanteerd:

- Profila Zorg voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
    - Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG)
    - Wet Bescherming Persoonsgegevens (WBP)
    - Wet Geneeskundige Behandelingsovereenkomst (WGBO)
    - Wet Bijzondere Opname Psychiatrische Ziekenhuizen (BOPZ)
- Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle bedrijfsonderdelen van Profila Zorg hebben hiertoe verantwoordelijkheden voor informatie-beveiliging toegewezen en vastgelegd. De in hoofdstuk 4 beschreven organisatie van informatiebeveiliging vormt hierbij de leidraad.
- Wanneer (onderdelen van) Profila Zorg samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
- De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van Profila Zorg zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
- Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
- Profila Zorg voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren.
- Profila Zorg beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
- Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de Raad van Bestuur een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de CAO.
- Alle onderdelen van Profila Zorg hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
- Alle onderdelen van Profila Zorg hebben maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, etc.) vormen hiervan een belangrijk onderdeel.
- Alle onderdelen van Profila Zorg hebben maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
- Bij de ontwikkeling en aanschaf van informatiesystemen wordt in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan informatiebeveiliging.
- Alle onderdelen van Profila Zorg hebben adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
- Als onderdeel van het beleidsproces voor informatiebeveiliging wordt binnen Profila Zorg door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
- Alle onderdelen van Profila Zorg beschikken over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.

2. Organisatie van informatiebeveiliging

In dit hoofdstuk wordt de organisatie van informatiebeveiliging binnen Profila Zorg beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft.

De organisatie van informatiebeveiliging wordt beschreven volgens de volgende invalshoeken:

- Het niveau van de beveiligingstaken, waarbij onderscheid wordt gemaakt naar strategische en operationele informatiebeveiliging
- Generieke rollen voor informatiebeveiliging, waarbij de rollen van eigenaar, functioneel beheerder, applicatiebeheerder, technisch beheerder en gebruiker worden onderscheiden
- Rollen en functies voor informatiebeveiliging binnen Profila Zorg.

2.1 Strategisch en operationeel niveau

In het onderstaande overzicht wordt een indeling van activiteiten met betrekking tot informatiebeveiliging gepresenteerd, waarbij het niveau van de activiteiten als onderscheidend criterium is gehanteerd.

Niveau	Activiteit	Verantwoordelijke	Documentatie
Strategisch	Beleidsvorming en planning	Management team	Informatiebeveiligingsbeleid Profila Zorg brede richtlijnen Informatiebeveiligingsplan
Operationeel	Uitvoering	Systeembeheerder	Operationele procedures per eenheid

Op strategisch niveau vindt de beleidsvorming met betrekking tot informatiebeveiliging plaats. Het management team is verantwoordelijk voor deze beleidsvorming. De beleidsvorming wordt vastgelegd in het Informatiebeveiligingsbeleid en nader uitgewerkt in Profila Zorg brede richtlijnen zoals de Gedragsregels voor informatieveiligheid.

De uitvoering van activiteiten met betrekking tot informatiebeveiliging vindt plaats op operationeel niveau. Eerstverantwoordelijke voor deze activiteit is de systeembeheerder van Profila Zorg.

2.2 Rollen en functies voor informatiebeveiliging

Veel onderdelen binnen onze organisatie zijn bij informatiebeveiliging betrokken. In dit informatiebeveiligingsbeleid worden de verantwoordelijkheden van de volgende functies en rollen beschreven:

- Portefeuillehouder informatiebeveiliging: MT
- Lijnmanagement
- Coördinator informatiebeveiliging
- Kwaliteitsmedewerker
- Hoofd HR
- Hoofd Facilitaire dienst
- Ondernemingsraad
- ICT/ systeembeheer

Portefeuillehouder informatiebeveiliging: management team
Door het management team is voor informatiebeveiliging een portefeuillehouder aangewezen: de manager bedrijfsvoering. De verantwoordelijkheid voor informatiebeveiliging omvat:

- Het vaststellen van organisatiebreed informatiebeveiligingsbeleid en daaruit voortvloeiende richtlijnen
- 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.

Lijnmanagement
Het lijnmanagement, bestaande uit regiomanagers, teamleiders en hoofden zijn 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 eigenaar is. Het lijnmanagement wordt hierbij ondersteund door de systeembeheerder.

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, beoordelingen etc.
- Afhandelen van vertrouwelijke informatiebeveiligingsincidenten.

Coördinator Informatiebeveiliging
De systeembeheerder van Profila Zorg is tevens de coördinator informatiebeveiliging en vormt een aanspreekpunt inzake informatiebeveiliging voor het management en de eigen medewerkers van het eigen organisatieonderdeel.
Op hoofdlijnen omvat deze beschrijving de volgende verantwoordelijkheden:

- Planvorming, het beheren van het informatiebeveiligingsplan en hieruit voortvloeiende decentrale richtlijnen en procedures
- Coördinatie en registratie, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging binnen de eigen organisatie-eenheid
- Communicatie en voorlichting, het stimuleren van het beveiligingsbewustzijn bij management en medewerkers
- Evaluatie en advies, het adviseren van de leiding van de eigen organisatie-eenheid over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen het organisatieonderdeel.

Afdeling Kwaliteit
De verantwoordelijkheid van afdeling kwaliteit is als volgt:

- De kwaliteitsmedewerker is verantwoordelijk voor het continu verbeteren van (bedrijfs)processen. Dit gebeurt door het toetsen van richtlijnen, processen en beleid binnen de instelling door het uitvoeren van interne audits en het formuleren van verbeteracties. Dit geldt ook wat betreft richtlijnen over de Wet Bescherming Persoonsgegeven en het beleid mbt informatiebeveiliging. De bevindingen van interne audits worden gerapporteerd aan de Raad van Bestuur.
- Afdeling kwaliteit is ervoor verantwoordelijk om het informatiebeveiligingsbeleid periodiek onder de aandacht van medewerkers te brengen door het op de aftekenlijst beleidsdocumenten te plaatsen en wijzigingen in het beleid te communiceren aan medewerkers middels het kwaliteitsplan per afdeling.
- Afdeling kwaliteit beheert alle beleidsdocumenten binnen Profila Zorg, dus ook het beleid mbt informatiebeveiliging. Dit betekent dat beleidsdocumenten jaarlijks geëvalueerd en bijgesteld worden. Hiertoe worden de verschillende verantwoordelijken en inhoudsdeskundigen uitgenodigd.

Hoofd HR
De verantwoordelijkheid van HR is als volgt:

- Het hoofd van de afdeling HR is verantwoordelijk voor het beheer van het personeelsbeleid van Profila Zorg. Er is een relatie tussen personeelsbeleid en informatiebeveiliging, onder andere daar waar het de indienstneming en het ontslag van personeel betreft. Dit dient op een zorgvuldige manier te geschieden met de waarborging van een goede informatiebeveiliging. Hiertoe bewaakt het hoofd HR samen met de systeembeheerder, de samenhang tussen personeelsbeleid en informatiebeveiliging.
- De afdeling HR is ervoor verantwoordelijk dat elke medewerker bij indienstneming de Gedragscode informatiebeveiliging ondertekent.
- De afdeling HR is ervoor verantwoordelijk dat het onderwerp van informatiebeveiliging opgenomen is in de jaargesprekken met medewerkers.
- De afdeling HR is verantwoordelijk voor het beheer van de toegangsrechten tot informatie voor medewerkers.

Hoofd Facilitaire Dienst
Het hoofd facilitaire dienst is verantwoordelijk voor het beveiligingsbeleid van Profila Zorg. Er is een relatie tussen beveiligingsbeleid en informatiebeveiliging, bijvoorbeeld daar waar het de beveiliging van locaties, werkplekken en computerruimten betreft. Het hoofd facilitaire dienst bewaakt, samen met de systeembeheerder, de samenhang tussen het beveiligingsbeleid en informatiebeveiliging.

Ondernemingsraad
De OR wordt geïnformeerd over de hoofdlijnen van beleid en de daaruit voortvloeiende richtlijnen en maatregelen met betrekking tot informatiebeveiliging. Daarnaast worden specifieke richtlijnen met betrekking tot informatiebeveiliging die een directe relatie hebben met het persoonlijke gedrag van het personeel ter beoordeling aan de OR voorgelegd. Dit geldt met name voor de Gedragscode informatiebeveiliging van Profila Zorg.

ICT / systeembeheer
ICT en systeembeheer is geoutsourced en wordt verzorgd door Unica Schutte. Door middel van een SLA is Unica Schutte verantwoordelijk voor:

- het verzamelen van informatie over potentiële ICT-beveiligingsincidenten en beveiligingslekken
- het centraal registreren van (potentiële) ICT-beveiligingsincidenten
- het analyseren en beoordelen van de aard, omvang en oorzaak van het ICT-beveiligingsincident
- het organiseren van de evaluatie van de afhandeling van ICT-beveiligingsincidenten
- het adviseren van de staande organisatie over de te nemen preventieve en herstelacties bij ICT-beveiligingsincidenten van beperkte omvang
- het adviseren van de calamiteitenorganisatie over de te nemen preventieve en herstelacties bij ICT-beveiligingsincidenten van grote omvang
- het informeren en instrueren van de direct betrokkenen over de uit te voeren preventieve en herstelacties
- het centraal informeren van gebruikers over (potentiële) ICT-beveiligingsincidenten
- het coördineren van de uitvoering van preventieve en herstelacties.

Als extern bedrijf legt Unica Schutte verantwoording af aan de systeembeheerder van de Facilitaire dienst.

4. Verantwoordelijkheden

De Raad van Bestuur is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid op het MT van juli 2010 vastgesteld.
De systeembeheerder van Profila Zorg is verantwoordelijk voor het naleven van het informatiebeveiligingssysteem conform professionele standaarden en het bijwerken van dit beleid.
Het lijnmanagement is verantwoordelijk voor toezicht op de naleving van dit beleid en de richtlijnen. Hierover vindt geen rapportage plaats.