SilverCloud Zorg IoT

Beleid voor kwaliteit en informatiebeveiliging met specifieke (zorg) beheersmaatregelen

INHOUD

1 VOORWOORD

Bij SilverCloud staat kwaliteit in dienstverlening en zorgvuldig omgaan met informatieveiligheid en dataprivacy hoog in het vaandel. Dit is niet alleen een kwestie van processen en technische maatregelen maar ook, specifiek, van bedrijfscultuur en persoonlijke motivatie.

Een tweede culturele waarde binnen ons bedrijf is transparantie en daarom delen wij graag met u ons “kwaliteit en informatiebeveiligingsbeleid” zoals die ook gedeponeerd is voor de ISO 9001, ISO 27001 en NEN 7510 certificeringen.

Op het gebied van kwaliteit- en informatiebeveiliging zijn altijd verbeteringen en aanpassingen mogelijk op basis van gewijzigd inzicht, nieuwe technologieën, nieuwe eisen en wensen en wettelijke maatregelen, wij waarderen uw “feedback” en garanderen u dat we deze ter harte nemen.

Namens alle medewerkers van SilverCloud hartelijk dank voor uw getoonde vertrouwen.

4 CONTEXT VAN DE ORGANISATIE

In de context beschrijven wij de in- en externe issues waar SilverCloud mee te maken heeft. Deze issues kunnen de kwaliteit en informatiebeveiliging beïnvloeden en wegen wij mee in onze risicobeoordeling en ons informatiebeveiligings-beleid.

4.1 Interne inrichting

4.1.1 Strategie

De directie heeft nagedacht over de diensten die zij wil verlenen en de doelgroep van klanten aan wie deze diensten geleverd (gaan) worden. Binnen de diensten zijn drie hoofdlijnen te herkennen:

- Cloud werkplekken: het aanbieden van flexibele Cloud werkplekken aan de klant met volledig beheer vanuit SilverCloud (dienst staat bekend als BrainOnline);
- Zakelijke telefonie: het leveren van telefonie oplossingen en slimme vergaderruimtes
- Netwerk en IoT: Het beheren van het volledige netwerk van klanten en het hierin uitbreiden van de dienstverlening met IoT oplossingen.

Commercieel worden er binnen de aanwezige diensten drie vormen gehanteerd voor het afsluiten van overeenkomsten:

- Abonnementen: bieden van een volledige oplossing aan de klant tegen een vast tarief per maand;
- Wederverkoop: hardware en internetverbindingen, waarbij SilverCloud als tussenpersoon optreedt. De klant sluit een overeenkomst af met SilverCloud, waarbij SilverCloud de dienst inkoopt en wederverkoopt en de facturatie verzorgt. Ondersteuning wordt verzorgd door de originele leverancier;
- Managed service: maatwerk ondersteuningscontracten voor het beheren van specifiek omschreven onderdelen. Belangrijk hierin voor de klant is het principe van ‘single point of contact’

De klantgroep van SilverCloud is als volgt te omschrijven:

SilverCloud Computing:

- Organisaties, die de keuze maken voor SilverCloud Computing op basis van nabijheid en de mogelijkheid voor afname van Cloud werkplekken
- Organisaties die de keuze maken voor SilverCloud Computing om betaalbare oplossingen te bieden voor zakelijke telefonie

SilverCloud Zorg IoT:

- Organisaties, die de keuze maken voor SilverCloud Zorg IoT om beheer te voeren over de IoT oplossingen die gekozen worden. Specifiek is hier een keuze gemaakt voor medische organisaties die gebruik willen maken van IoMT (internet of Medical Things) oplossingen

4.1.2 Cultuur

SilverCloud kent een open en platte structuur, werkzaamheden worden intern op basis van passendheid bij de persoon neergelegd en eventuele problemen worden via de korte communicatielijnen snel naar boven gehaald en opgelost.

4.1.3 Beschikbare middelen

SilverCloud beschikt over een gedeeltelijke eigen inventaris met hierin onder andere de kantooromgeving (bureaus, desktops etc.) en de server infrastructuur in het datacentrum in Dronten en een gedeeltelijk beheerde inventaris van klanten. Tijdens het schrijven van dit document beschikt SilverCloud over voldoende middelen om alle diensten te kunnen verlenen en ook in de toekomst aanvullende diensten te kunnen leveren.

Issues die spelen zijn:

- Beheer van apparatuur van klanten wordt minder, klanten willen liever een totaaloplossing waarin zij ook de hardware leasen en betalen voor het beheer en onderhoud;
- Eigen servers en hardware is nog passend voor SilverCloud, hier wordt geen grote investering verwacht.

4.1.4 Informatieverwerking

SilverCloud krijgt in haar eigen processen te maken met een grote stroom aan data, zowel eigen data als data die in beheer is van klanten. Verantwoordelijkheid voor de eigen data ligt bij de directie, data van klanten kan ook onder deze verantwoordelijkheid komen te vallen afhankelijk van de diensten die verleend worden.

4.2 Externe inrichting

4.2.1 Externe ontwikkelingen

Externe ontwikkelingen die voor SilverCloud van belang zijn bestaan uit onder andere het steeds volwassener worden van cloudoplossingen wat maakt dat het onderscheidend zijn op dit vlak steeds belangrijker wordt. Ook de verdere integratie van zakelijke telefonie met oplossingen als MS Teams en andere sociale media heeft de laatste tijd een vlucht genomen, zeker de afgelopen tijd als gevolg van de corona maatregelen. Dit heeft ook geleid tot de aanvraag van andere hardware om bijvoorbeeld videoconferencing mogelijk te maken.

Belangrijke ontwikkeling in het veld van IoT is de interesse die hiervoor is binnen de medische wereld. SilverCloud Zorg IoT heeft meerdere connecties binnen de medische wereld en ziet de interesse in Internet of Medical Things toenemen. Onderdeel hiervan is ook track & tracing van medische hulpmiddelen en de mogelijke aansluiting die hierin kan worden gevonden op het nieuwe Convenant Medische Hulpmiddelen.

4.2.2 Normen en richtlijnen

Binnen de wereld van SilverCloud vindt op het gebied van wet- en regelgeving op dit moment niet heel veel plaats. De omgang met privacy is sinds invoering van de AVG per 2018 al onder de aandacht en

blijft deze aandacht de komende jaren ook nog wel vragen. Op het gebied van richtlijnen is de NCSC één van de partijen die veel richtlijnen publiceert waar SilverCloud gebruik van maakt. Ook brancheverenigingen als Zorg & ICT en ISC2 zijn een bron van informatie op dit vlak.

Het werkzaam zijn op een markt van zorginstellingen brengt ook met zich mee dat SilverCloud op de hoogte wil zijn van de wetten en regels die daar van toepassing zijn en de manier waarop wij hier in onze dienstverlening aan tegemoet kunnen komen. Specifiek gaat het hier om de toepasselijke normen binnen de NEN 7510 en de hierin ondersteunende normen als de NEN 7512 en 7513 over gegevensuitwisseling en logging in de zorg.

4.2.3 Wetgeving

Op het gebied van kwaliteit en informatiebeveiliging hebben wij te maken met de volgende relevante normen en wetgeving:

Afkorting	Wetgeving
Gw	Grondwet
	Administratiewet
	Meldplicht datalekken
AVG	Algemene Verordening Gegevensbescherming
Aw	Auteurswet
TCw	Telecommunicatiewet
	Domeinnaamwet
wCC	Wet Computer Criminaliteit
ISO 27001	ISO 27001:2017
NEN 7510	NEN 7510
ISO 27002	ISO 27002:2017
ISO 9001	ISO 9001:2015
Covid-19	Richtlijnen vanuit het RIVM voor de omgang met Corona

Via onder andere onze zorgklanten zijn wij op de hoogte van de volgende wet- en regelgeving die voor hen van toepassing is:

Afkorting	Wetgeving
WGBO	Wet Geneeskundige Behandelovereenkomst
WKKGZ	Wet Kwaliteit, klachten en geschillen zorg
	Besluit elektronische gegevensverwerking door zorgaanbieders
	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
NTA 7516	Richtlijn veilig mailen in de zorg
CE	Richtlijnen rondom CE markering van (onder andere) apparatuur
	Convenant Medische Technologie
NEN 7512	Richtlijn veilig delen van data
NEN 7513	Richtlijn logging in zorginstellingen

4.2.4 Contractuele verplichtingen

In de contracten met klanten en leveranciers wordt afhankelijk van het type klant al aandacht besteed aan kwaliteit en informatieveiligheid. Een aantal klanten stelt in offerte trajecten al vragen over de inrichting van informatieveiligheid en eisen certificering om op objectieve wijze de kwaliteit van de dienstverlening zeker te stellen.

Klanten in het MKB-segment vragen bij de start van ondersteuning nog niet vaak om garanties op gebied van kwaliteit en/of informatieveiligheid, met deze klanten worden SLA afspraken gemaakt en is de dienstverlening ook meer kritisch voor hun eigen processen. De SLA dient in dit geval ter bescherming van beide partijen en het verduidelijk van de diensten die voor een bepaald bedrag worden geleverd.

5 ZORGSPECIFIEKE TOEVOEGING

SilverCloud Zorg IoT werkt in toenemende mate voor zorginstellingen. Hierop zijn een aantal zorg specifieke toevoegingen van toepassing. In de regel beschikken wij niet over zorginformatie. Organisaties, medewerkers en andere relevante partijen kunnen het informatiebeveiligingsbeleid inzien.

5.1 Zorgspecifieke eisen

De noodzaak van gezondheidsinformatiebeveiliging is bijzonder groot. Steeds meer data wordt uitgewisseld. Daarbij gaat het niet alleen om patiëntinformatie, maar ook om werkwijzen (protocollen) en ondersteunende documenten. Het is van belang dat deze informatie voor alle partijen betrouwbaar is.

Het beschikbaar stellen van deze informatie, de integriteit ervan en uiteraard het bewaken van de vertrouwelijkheid zijn belangrijke doelen van gezondheidsinformatiebeveiliging.

Door de aard van onze werkzaamheden werken de medewerkers van SilverCloud bijna altijd in de omgeving en onder de verantwoordelijkheid van de instelling.

De dienstverlening op het gebied van IoMT richt zich op het beheer van (Medische) hulpmiddelen en facilitaire ondersteuning zoals klimaatbeheersing en niet direct op Zorg als primair proces. Hierdoor is de impact van wetgeving in verband met naleving beperkt.

De belangrijkste eisen van wet- en regelgeving en contractuele eisen, waaronder eisen met betrekking tot de bescherming van persoonlijke gezondheidsinformatie en de wettelijke en ethische verantwoordelijkheden van zorgverleners omvatten de geheimhouding. Wij hanteren het beleid dat zorginformatie niet in ons bezit mag komen en informatie niet buiten de eigen omgeving gebracht mag worden door ons. Hierbij moeten wij de beveiligingsniveaus voor vertrouwelijkheid en integriteit handhaven.

Informatiebeveiligingsincidenten melden wij altijd via de meldingssystemen van de klant, waarbij een beroep kan worden gedaan op de directie van SilverCloud om incidenten te bespreken of bespreekbaar te maken bij de klanten.

Onze oplossingen zijn vrijwel altijd ondersteunend aan de primaire processen, waardoor er geen vitale processen en systemen zijn in de zorg (‘vitaal’ wil zeggen dat het falen ervan nadelige gevolgen kan hebben voor cliënten). Uiteraard kan er wel sprake zijn van ongemak, wat wij ook altijd proberen te voorkomen.

5.2 Beleidsregels voor maatregelen

5.2.1 Verantwoordelijkheden

De Quality & Security Officer is verantwoordelijk voor het beheer van zorginformatie en neemt maandelijks deel aan het werkoverleg wat dient als informatiebeveiligingsforum. Indien noodzakelijk zal de Quality & Security Officer ook deelnemen aan overleg bij opdrachtgevers.

5.2.2 Scheiding van taken

SilverCloud scheidt, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden zoveel mogelijk op basis van need to know om de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.

5.2.3 Risico's in projectbeheer

Daar waar SilverCloud onder eigen verantwoordelijkheid een project in de zorg uitvoert (als hoofdaannemer) voorzien wij ook in een Quality & Security Officer die binnen het project de informatiebeveiliging op zich neemt.

5.2.4 Screening

Het screeningsbeleid van SilverCloud houdt rekening met de specifieke eisen die voor zorginstellingen gelden. Wij screenen sollicitanten op adres, referenties en vragen een VOG-verklaring. Daarnaast moet de kandidaat over de juiste competenties beschikken.

5.2.5 Arbeidsovereenkomst en functie-inhoud

In de regel verwerken wij geen zorginformatie. Maar als dat toch gebeurt dan zullen wij de verantwoordelijkheden hiervan schriftelijk vastleggen in een functieomschrijving of een aanvulling maken op de functiebeschrijving.

5.2.6 Bewustzijn

Medewerkers van SilverCloud die werken met zorginformatie zijn verplicht jaarlijkse hun kennis op peil te houden hetgeen zal worden gefaciliteerd door de directie.

5.2.7 Verwerkende systemen

Als wij zorginformatie verwerken dan zullen wij de informatie verwerkende systemen in een aparte categorie opnemen in de assetlijst en ook als een aparte groep classificeren. Indien nodig worden hiervoor eigenaren en aanvullende gebruiksvoorwaarden vastgesteld.

5.2.8 Teruggeven bedrijfsmiddelen

Alle medewerkers moeten bij uit dienst treden informatie van de eigen systemen verwijderen en bedrijfsmiddelen inleveren. Dit speelt in het bijzonder voor verwerkers van zorginformatie. Hierbij zullen wij extra zorgvuldigheid betrachten in verband met de hogere classificatie eisen.

5.2.9 Classificatie

Alle zorginformatie classificeren en behandelen wij per definitie als vertrouwelijk.

5.2.10Labelen

Alle zorginformatie die wij verwerken of waarvoor wij systemen ontwikkelen wordt door ons gelabeld met Vertrouwelijk.

5.2.11Media

Alle media met zorginformatie zijn versleuteld tijdens opslag en vervoer en alleen toegankelijk met gebruikersnaam, wachtwoord en indien technisch mogelijk met multifactor authenticatie.

5.2.12Toegangsbeveiliging

Indien wij persoonlijke gezondheidszorginformatie gaan verwerken zullen wij richtlijnen opstellen voor de toegangsbeveiliging tot deze informatie. De gebruikers die hierbij betrokken zijn zullen daarvoor geregistreerd worden onder vermelding van een aparte categorie. Wanneer iemand deze informatie niet meer nodig heeft, wordt de toegang tot de persoonlijke gezondheidsinformatie beperkt of beëindigd.

5.2.13Apparatuur

Onze apparatuur bevat geen zorg specifieke informatie. Niettemin zullen wij apparatuur die gebruikt is binnen zorginstellingen extra nauwkeurig behandelen wanneer deze gerepareerd, verwijderd of doorgegeven moet worden aan een (nieuwe) collega.

5.2.14Bedrijfsvoering

In de bedrijfsvoering wordt voor wijzigingen in systemen met zorginformatie voorzien in een formele wijzigingsprocedure. Bij de ontwikkeling, het testen, accepteren en in productie nemen van producten zien wij toe op een duidelijk scheiding van deze fasen.

5.2.15Evaluatie

Het informatiebeveiligingsbeleid zal minimaal één keer per jaar getoetst worden op effectiviteit waarbij wijzigingen in de zorgcontext worden meegenomen.

5.2.16Back-up

Indien wij informatie gaan beheren zullen wij in overleg met de opdrachtgever de zorginformatie veiligstellen door middel van back-ups.

5.2.17Interne audits

Interne audits op zorginformatie worden uitbesteed, zodat de kwaliteit hiervan gewaarborgd is en de auditinformatie niet gemanipuleerd kan worden.

5.2.18Acceptatietests

In beheercontracten nemen wij specifieke waarborgen, waaronder acceptatiecriteria op voor veilige updates en patches.

5.2.19Leveranciers

Zorginformatie wordt conform wettelijke eisen in het daartoe bestemde land opgeslagen. Met leveranciers worden overeenkomsten gesloten die voorzien in de juiste waarborgen.

5.2.20Incidentenmanagement

Indien er bij incidenten persoonlijke zorginformatie betrokken is zullen wij de persoon in kwestie daarover informeren evenals de betreffende zorginstelling indien het incident mogelijk negatieve gevolgen heeft gehad of kan hebben.

5.2.21Privacy

Indien wij persoonsgebonden informatie verwerken, dan beheren wij ook de grondslag voor de verwerking in de vorm van een toestemmingsverklaring.

5.2.22 Transport van data

SilverCloud Computing hanteert onderstaand beleid in het transport van data tenzij met leveranciers of klanten andere afspraken zijn gemaakt.

Informatiesoort	Toegestaan communicatie/ transport middel
Contracten (klant, leveranciers)	Docusign, e-mail
Klantdata (data van de klant)	Opgeslagen in Exact en gekoppeld met Autotask
Back-up klantendata	Altijd versleuteld
E-mail persoonsgebonden	HTTPS/TLS 1.2
E-mail niet persoonsgebonden	HTTPS/TLS 1.2
Wachtwoorden klanten	In de virtuele kluis (1Password) worden wachtwoorden opgeslagen die nodig zijn voor de uitvoering van de dienstverlening. Alleen geautoriseerd personeel heeft toegang
Fileshare dienstverlening voor klanten	Altijd versleuteld

6 COMMUNICATIE EN LEIDERSCHAP

6.1 Communicatie

Het beleid wordt binnen en buiten de organisatie aan de relevante personen gecommuniceerd.

6.2 Evaluatie

Jaarlijks wordt het beleid geëvalueerd conform de operationele planning.

6.3 Rollen, verantwoordelijkheden en bevoegdheden

Leiderschap op het gebied van kwaliteit en informatiebeveiliging betekent dat we alert zijn, waar mogelijk het goede voorbeeld geven en elkaar helpen en aanspreken op ongewenst gedrag. Hierbij heeft het management een voorbeeldfunctie, maar ook van medewerkers wordt een proactieve houding verwacht. Op hoofdlijnen gelden hierbij de volgende verantwoordelijkheden:

6.3.1 Alle functies

- Nemen kennis van het beleid en de (gedocumenteerde) beheersmaatregelen en passen dit toe
- Spreken elkaar aan op ongewenst gedrag en melden incidenten
- Nemen actief deel aan awareness campagnes, trainingen en instructies

6.3.2 Quality & Security Officer

- Bewaakt dat het KISMS aan ISO 27001, NEN 7510 en ISO 9001 voldoet.
- Organiseert audits en voorziet in rapportages.
- Identificeert eisen uit o.a. wetgeving, contracten en certificeringsnormen.
- Adviseert en ondersteunt bij het bewaken van vervaldata, risicoanalyses, dataclassificatie, oorzaakanalyses, calamiteitenoefeningen en systeemevaluaties.
- Meten, analyseren en sturen bij op basis van KPI’s, audits en incidentmeldingen.
- Verbeteren maatregelen op grond van risico(her)beoordelingen en oorzaakanalyses.

6.3.3 Systeembeheerder/ Support engineer

- Delen kennis over informatiebeveiliging binnen het team
- Signaleren en melden afwijkingen in systemen proactief

6.3.4 Directie

- Stelt kwaliteit en IB-doelstellingen en -beleid vast en vervult een voorbeeldfunctie.
- Draagt het beleid uit en stelt middelen beschikbaar.
- Evalueert de prestaties en streeft naar continue verbetering.
- Signaleren risico’s/nemen deel aan risicoanalyses en implementeren beheersmaatregelen.
- Vervullen een voortrekkersrol bij het verbeteren van bewustzijn.

6.4 Leiderschap

De directie draagt de eindverantwoordelijkheid voor het managementsysteem en zet zich persoonlijk in voor de doeltreffendheid ervan. Bij het werken aan en concretiseren van de beleidsuitgangspunten heeft de directie van SilverCloud zelf een actieve rol en is zij maximaal betrokken.

De directieverantwoordelijkheden hierbij betreffen:

- bewerkstelligen dat het beleid en de bijbehorende doelstellingen zijn vastgesteld en maximaal aansluiten bij de strategie van het bedrijf;
- zorgdragen dat de organisatie voldoet aan geldende wet- en regelgeving;
- bewerkstelligen dat de eisen van het managementsysteem in de bedrijfsvoering van SilverCloud zijn geïntegreerd;
- bewerkstelligen dat de voor het managementsysteem benodigde middelen beschikbaar zijn;
- het belang van een effectief managementsysteem en het voldoen aan de eisen communiceren;
- bewerkstelligen dat het managementsysteem de beoogde resultaten behaalt;
- het aansturen van de medewerkers en deze ook te ondersteunen om een bijdrage te leveren aan het managementsysteem;
- het bevorderen van het proces van continu verbeteren;
- het ondersteunen van managementfuncties om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.