



Beleidsverklaring

D0008-20221217

Auteur: Management van SecuDoc B.V.

Inhoudsopgave

Inhoudsopgave	2
De organisatie	3
Informatiebeveiliging	3
Toepassingsgebied	3
<i>Mensen</i>	<i>3</i>
<i>Processen</i>	<i>3</i>
<i>Plekken/locaties.....</i>	<i>3</i>
<i>Platformen en toepassingen</i>	<i>3</i>
Verantwoordelijkheden	4

De organisatie

SecuDoc zorgt ervoor dat iedereen de mogelijkheid heeft om veilig bestanden te versturen, ontvangen én ondertekenen. Ook kan je veilig berichten versturen, vooral handig voor zorginstellingen die snel en veilig medische gegevens moeten sturen.

Bovenstaande beschrijft wel waarom het zo van belang is dat SecuDoc handelt naar de ISO 27001 en de NEN 7510 norm. We hebben de verantwoordelijkheid om veilig, integer en vertrouwelijk met (zorg-gerelateerde) informatie om te gaan van directe en indirecte belanghebbenden. In dit beleidsdocument omschrijven wij in hoofdlijnen hoe we ervoor zorgen dat SecuDoc het maximale onderneemt en blijft ondernemen om informatiebeveiliging te garanderen.

Informatiebeveiliging

Het doel van informatiebeveiliging is het waarborgen van de bedrijfscontinuïteit en het minimaliseren van bedrijfsschade door het voorkomen en minimaliseren van de impact van bedrijfsincidenten. Bedrijfsmiddelen, processen en alle overige interne en externe SecuDoc activiteiten moeten de volgende drie elementen als kernwaarde hebben, namelijk het waarborgen:

1. **Vertrouwelijkheid**, ofwel: informatie beschermen tegen ongeoorloofde openbaarmaking
2. **Integriteit**, ofwel: informatie beschermen tegen ongeoorloofde of accidentele wijziging(en)
3. **Beschikbaarheid**, ofwel: informatie op de juiste momenten aan de juiste personen toegankelijk maken voor het realiseren van bedrijfsdoelstellingen.

Om aan de gestelde norm en de geformuleerde doelstellingen te voldoen hanteert SecuDoc een managementsysteem voor informatiebeveiliging, het zogeheten ISMS.

Toepassingsgebied

Mensen

- Medewerkers van de organisatie (inclusief directie, inhuur, oproepkrachten en stagiairs)

Processen

- Ontwikkelp proces
- Hosting en technische exploitatie
- Administratie en verkoop
- Gebruikersondersteuning

Plekken/locaties

- Kantoorlocatie (Velperweg 27, 6824BC te Arnhem)
- Thuiswerk- en telewerklocaties van medewerkers

Platformen en toepassingen

- Netwerk- en telediensten (lokaal)
- Externe cloudplatformen (Office 365)
- Interne cloudplatformen en eigen beheerde servers
- Ingekochte software

Verantwoordelijkheden

Om aan de gestelde norm te voldoen en om de gestelde doelstellingen te behalen en continu te verbeteren zijn er een aantal verantwoordelijkheden geformuleerd. Deze gelden voor diverse betrokkenen van SecuDoc. De verantwoordelijkheden waaraan SecuDoc voldoet en waar betrokkenen zich aan moet houden zijn:

1. De directie/management heeft dit informatiebeveiligingsbeleid goedgekeurd;
2. De dagelijkse verantwoordelijkheid voor en de contacten met externe organisaties voor de naleving van de wettelijke eisen, met inbegrip van de bescherming van gegevens, berusten bij het management van SecuDoc;
3. Alle belanghebbenden hebben de plicht om de middelen, inclusief fysieke locatie, hardware, software, systemen en informatie (alle bedrijfsgerelateerde informatie), die zij onder hun hoede hebben, te beschermen en elke vermoede inbreuk op beveiliging onmiddellijk te melden;
4. Het naleven van informatiebeveiligingsprocedures zoals uiteengezet in de diverse beleids- en richtlijndocumenten wordt geaccepteerd als onderdeel van de standaardwerkzaamheden binnen de organisatie. SecuDoc zet zich hard in voor het opleiden van medewerkers en verstrekt alle beschikbare educatie en documenten aan haar medewerkers. Mochten er zaken niet worden nageleefd dan leidt dit tot disciplinaire maatregelen;
5. Aan alle wettelijke en reglementaire vereisten wordt voldaan en regelmatig op wijzigingen gecontroleerd door het management;
6. Er is een managementsysteem wat betreft informatiebeveiliging (ISMS). Dit wordt onderhouden, getest en regelmatig herzien om bedrijfscontinuïteit en handhaven (PDCA-cyclus);
7. Het informatiebeveiligingsbeleid en de beleidsbepaling worden regelmatig herzien en kan door het management worden gewijzigd om de blijvende levensvatbaarheid, toepasbaarheid en naleving van wetgeving te waarborgen en om de informatiebeveiliging systemen voortdurend te verbeteren;
8. De directie/management stuurt erop aan dat er wordt voldaan aan de geldende wet- en regelgeving en dat middels het informatiebeveiligingsmanagementsysteem continu verbetering wordt bewerkstelligd.
9. Maatregelen zijn genomen om technische naleving te borgen, zoals het uitvoeren van interne en externe audits in het kader van ISO 27001 en NEN 7510.

Middels deze verantwoordelijkheden neemt SecuDoc de informatiebeveiliging van haar zelf en haar stakeholders uiterst serieus. Mochten er vragen zijn of verdere opmerkingen over deze bepaling dan kan er altijd contact worden opgenomen via onderstaande contactgegevens.

SecuDoc B.V.
Velperweg 21
6824 BC, Arnhem
0243010201
info@secudoc.nl

Namens de directie van SecuDoc,



Nicolaj Nijenhuis