



Informatiebeveiligingsbeleid

Qics B.V.

Datum : 17 februari 2023
Documentnr : INTQ-2038835178-65/ v4.0
Auteur : Mark Velthuijsen

Inhoudsopgave

1. Introductie	3
1.1. <i>Inleiding</i>	3
1.2. <i>Informatie- en privacy beveiligingsbeleid Qics</i>	3
1.3. <i>Doelstellingen informatiebeveiliging en privacy</i>	3
1.4. <i>Verantwoordelijkheid informatie-en privacy beveiligingsbeleid</i>	4
1.5. <i>Algemene toelichting</i>	4

1. Introductie

1.1. Inleiding

Dit document beschrijft het door Qics B.V. ("organisatie") gehanteerde informatiebeveiligingsbeleid met betrekking tot onze software, services, interne processen en medewerkers.

Het document heeft als doel om onze klanten en andere belanghebbenden te informeren over de maatregelen die wij genomen hebben om de veiligheid van de gegevens van onze klanten zo goed als mogelijk te waarborgen.

1.2. Informatie- en privacy beveiligingsbeleid Qics

Qics helpt zakelijke dienstverleners en dienstverleners in de zorg met het stroomlijnen van bedrijfsprocessen op het gebied van planning, urenregistratie en facturatie.

Als directie van Qics B.V. (hierna te noemen: Qics) hechten we grote waarde aan een goede informatiebeveiliging. We streven ernaar om te borgen dat alle informatie die wij verzamelen, produceren, uitwisselen en opslaan op een adequate wijze wordt beveiligd. Ons informatiebeveiligingsbeleid is erop gericht om de gegevens die wij gebruiken zo goed mogelijk te beschermen. Ter uitvoering van dit beleid zullen wij ervoor zorgen:

- Dat gegevens, zowel interne informatie als afkomstig van derde partijen, vertrouwelijk worden behandeld;
- Dat de integriteit van de gegevens gewaarborgd blijft;
- Dat onze informatiesystemen zodanig zijn ingericht dat zij in voldoende mate beveiligd zijn tegen beveiligingsrisico's;
- Dat wij de relevante wet- en regelgeving op het gebied van gegevensbeveiliging en privacy naleven;
- Dat de continuïteit van onze dienstverlening gewaarborgd blijft door het handhaven van een effectief Business Continuity Plan (BCP);
- Dat medewerkers voldoende bewust zijn van het belang van een goede informatie- en privacybeveiliging;
- Dat wij voldoende maatregelen nemen om onze informatiesystemen te beschermen tegen ongeoorloofde toegang en misbruik;

Naast deze eisen zijn wij gehouden aan de geldende wet- en regelgeving (zoals AVG). Met de documentatie in ons Information Security Management System (ISMS), dat is ingericht conform ISO-27001:2017 en NEN 7510:2017, zijn we in control en tonen wij aan op welke wijze wij aan wet- en regelgeving voldoen.

Qics is ISO-27001 en NEN-7510 gecertificeerd. Deze certificering en de bijbehorende verklaring van toepassing zijn beschikbaar op onze website.

1.3. Doelstellingen informatiebeveiliging en privacy

1. Leveren van veilige en betrouwbare clouddiensten aan onze klanten en eindgebruikers, zodat deze met vertrouwen onze SaaS software kunnen gebruiken om hun data veilig te verwerken.
2. Bieden van een veilige werkomgeving aan onze medewerkers die ze in staat stelt om professionele diensten uit te voeren voor onze klanten.
3. Voldoen aan de contractuele eisen van onze partners en klanten op het gebied van informatieveiligheid en gegevensuitwisseling. Onderdeel hiervan is de ambitie om voor mei 2022 de ISO 27001 en NEN 7510 certificeringen te hebben behaald.
4. Voldoen aan de wettelijke eisen met betrekking tot privacy en informatiebeveiliging en onze klanten helpen om aan hun wettelijke eisen te kunnen voldoen bij het gebruik van onze software.

Concrete informatie- en privacybeveiligingsdoelstellingen zijn opgenomen in ons managementsysteem.

1.4. Verantwoordelijkheid informatie-en privacy beveiligingsbeleid

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld. De rol van Information security officer is belegd binnen de Qics organisatie. De security officer is verantwoordelijk voor het onderhoud van het informatie- en privacybeveiligingsbeleid. Hij is ook verantwoordelijk voor het onderhoud en de implementatie van het informatiebeveiligingsplan en bijbehorende maatregelen. Qics is zich bewust dat regelmatig onderhoud aan het ISMS noodzakelijk is. Onder andere bij wijzigingen binnen de organisatie, resultaten van (interne) audits, risicoafwegingen en ontwikkelingen op het gebied van wet- en regelgeving, zal Qics de impact op het ISMS bepalen en eventueel benodigde aanpassingen doorvoeren.

1.5. Algemene toelichting

De beveiliging wordt als volgt gedefinieerd:

"Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit, vertrouwelijkheid en privacy van informatie en informatiesystemen."

Opgemerkt wordt dat informatie- en privacybeveiliging een samenhangend stelsel van maatregelen omvat. Dit betekent dat de verschillende maatregelen die samen de informatiebeveiliging vormen niet los van elkaar, maar in onderlinge relatie met elkaar staan.

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

Informatie- en privacybeveiliging is gericht op het realiseren van een optimaal niveau van beveiliging. Dit optimum wordt bereikt door een zorgvuldige afweging van de risico's.

Namens Qics B.V.

17 februari 2023 te Katwijk



Mr. Velthuisen

Technisch directeur