Q-link en informatiebeveiliging op basis van NEN 7510

Inleiding

In het kader van informatiebeveiliging zijn onderstaande maatregelen getroffen rondom de Q-link applicatie en alle hierin opgenomen modules. Onder de informatiebeveiliging wordt verstaan: het waarborgen van de beschikbaarheid, vertrouwelijkheid van alle informatie, integriteit van gegevens, zorgen voor onweerlegbaarheid, verantwoordelijkheid, authenticiteit en betrouwbaarheid.
De informatiebeveiliging geldt zowel voor de gegevens van klanten van LENS business software als voor de gegevens die door klanten van LENS business software in Q-link worden vastgelegd. Hiermee voldoet Q-link aan de eisen die gesteld worden in de NEN 7510 Informatiebeveiliging in de zorg.

Vertrouwelijkheid

Dataverkeer
Het dataverkeer tussen de pc van de gebruiker en de servers van LENS business software is door middel SSL (Secure Socket Layer) versleuteld. Eventueel afgetapt dataverkeer kan nooit ontcijferd worden.

Identificatie en authenticatie
Een gebruiker wordt standaard geïdentificeerd door middel van een unieke gebruiksnaam en een wachtwoord. Op het wachtwoord kunnen complexiteitseisen worden toegepast.
Wij adviseren de gebruiker een sterk wachtwoord te kiezen, namelijk een wachtwoord bestaande uit minimaal 8 karakter, waaronder minimaal 1 cijfer en 1 leesteken. De eindgebruiker is zelf verantwoordelijk voor het kiezen en vertrouwelijk omgaan met zijn/haar wachtwoord.
Gebruikersnamen en wachtwoorden die opgevraagd worden bij LENS business software worden uitsluitend via e-mail verstuurd naar een e-mailadres dat reeds in Q-link is opgenomen.

Fysieke toegang
De servers van LENS business software staan in een afgesloten ruimte binnen een datacentrum. Deze ruimte is alleen toegankelijk voor geautoriseerde personen. Deze personen dient te beschikken over een toegangspas, een identiteitsbewijs en moet de locatie en cijfercode van de kast waarin de apparatuur zich bevindt kennen.

Apparatuur
Apparatuur en systemen kunnen op afstand alleen door medewerkers van LENS business software met de juiste bevoegdheden worden beheerd. Gegevens aanwezig op oude apparatuur worden vernietigd.

Geheimhouding
Alle medewerkers van LENS business software die toegang hebben tot gegevens van klanten en tot gegevens opgenomen in Q-link hebben een geheimhoudingsverklaring ondertekend. Deze is in het personeelsdossier opgenomen.

De medewerker zal zich alleen toegang tot de Q-link applicatie verschaffen ten bate van onderhoud of voor inhoudelijke ondersteuning.
Als een medewerker uit dienst treedt, wordt zijn/haar toegang tot systemen en gegevens afgesloten.

Beschikbaarheid

Fysiek
De servers staan in een afgesloten ruimte binnen een datacentrum. Dit datacentrum beschikt over noodstroomvoorzieningen, brandprotectie en redundante dataverbindingen.

Netwerk
De servers beschikken over twee netwerkaansluitingen. Bij uitval van één aansluiting neemt de andere aansluiting het verkeer over. Het datacentrum beschikt over meerdere aansluiting naar het internet.

Server
Iedere server beschikt over twee voedingen die via separate stroomgroepen worden gevoed. Daarnaast is er een noodstroomvoorziening met een UPS en een noodstroomgenerator.

Data
De data wordt gerepliceerd over meerdere harde schijven zodat deze ook bij uitval van een harde schijf beschikbaar blijft.

Herstelprocedure
De herstelprocedure is gedocumenteerd en wordt twee keer per jaar getest.

Integriteit

Database
Iedere Q-link applicatie maakt gebruik van een geïsoleerde, op zich staande database.

Autorisatie en toegangscontrole
Gegevens in Q-link kunnen alleen worden gewijzigd door gebruikers met de juiste bevoegdheden. Identificatie van de gebruiker geschiedt aan de hand van de gebruikersnaam en het wachtwoord.

Applicatie
De applicatie zorgt voor de integriteit van deze gegevens door middel van invoercontrole, opslagcontrole en weergavecontrole.

Onweerlegbaarheid

Logging
Het wijzigen van gegevens door een gebruiker wordt in het systeem vastgelegd.

Verantwoordelijkheid

Licentieovereenkomst
In de licentieovereenkomst is vastgelegd dat de klant zelf verantwoordelijk is voor de inhoud van de gegevens.

Authenticiteit

Certificaat
Door middel van een certificaat wordt de authenticiteit van de webapplicatie en het bijbehorende adres (URL) gewaarborgd.

Betrouwbaarheid

Virusscanner en firewall
De applicaties en systemen worden door middel van virusscanners en firewalls beschermd tegen ongeoorloofde toegang of programmatuur. Alle serverbesturingssystemen worden continu voorzien van de meest recente updates.

Back-up
Van alle gegevens die nodig zijn om een systeem opnieuw volledig werkend op te kunnen bouwen wordt dagelijks een back-up gemaakt. Het slagen van de back-ups wordt dagelijks gecontroleerd. De back-ups worden op ten minste twee locaties opgeslagen en bewaard.

Dataverkeer
Door middel van bewezen technieken als tcp/ip, https en asp.net wordt op elke laag in het dataverkeer van de applicatie de integriteit gecontroleerd.

Applicatieontwikkeling
Bij het ontwerpen en ontwikkelen van applicaties worden altijd de beveiligingsmaatregelen volgens de huidige stand van de techniek opgenomen.
Applicatie-updates worden altijd getest voordat deze worden toegepast.

Applicatie
Elke klant beschikt voor Q-link over een geïsoleerde, op zich staande webapplicatie-omgeving en een eigen database.
Systeembestanden worden beschermd door het besturingssysteem en een virusscanner.

Storingen
Storingen en incidenten worden geregistreerd en jaarlijks geanalyseerd.