

1. Beveiliging

Bij de ontwikkeling van Konnect zijn hoge eisen gesteld aan de mate van beveiliging. Dit heeft er toe geleid dat beveiliging in alle onderdelen van het portaal is doorgevoerd. Het ouderportaal heeft een strikte toegangsbeveiliging, waardoor de kinderopvang organisatie bepaalt welke ouders en medewerkers toegang hebben. Daarnaast is het internetverkeer beveiligd op dezelfde bewezen veilige manier als bijvoorbeeld bij internetbankieren en worden de gegevens in het ouderportaal beveiligd opgeslagen.

Hieronder is een kort overzicht gegeven van de belangrijkste maatregelen die in het kader van de beveiliging genomen zijn.

1.1. Toegangsbeveiliging

Op basis van een gebruikersnaam en wachtwoord wordt bepaald of de gebruiker toegang krijgt tot het systeem. Indien een gebruiker meer dan vijf keer met een verkeerd wachtwoord heeft geprobeerd in te loggen, wordt de gebruiker voor een bepaalde periode geblokkeerd, om misbruik te voorkomen. Elke foutieve inlogpoging wordt vastgelegd om misbruik te detecteren.

Elke gebruiker heeft een zelf gekozen wachtwoord, dat minimaal uit 6 karakters bestaat en alleen bekend is bij de gebruiker. Het wachtwoord is onleesbaar in de database opgeslagen, zodat ook beheerders nooit inzicht hebben in het gekozen wachtwoord van de gebruiker.

1.2. Autorisatie

Elke gebruiker heeft een of meer rollen in Konnect. Op basis van de rollen die de gebruiker heeft, wordt bepaald welke functies de gebruiker mag uitvoeren.

Met betrekking tot de autorisatie worden de volgende uitgangspunten gehanteerd:

- Zonder de benodigde autorisaties wordt geen toegang verleend tot de gevraagde functie of gegevens.
- Alle pogingen om functies uit te voeren die niet geautoriseerd zijn, worden vastgelegd in de logging en actief gemaild naar de beheerders van het ouderportaal.

1.3. Beveiliging van de verbinding

De verbinding tussen de browser en de server is beveiligd. Er worden alleen verbindingen geaccepteerd die via een beveiligde verbinding plaatsvinden (https). Verbindingen die opgebouwd wordt via onbeveiligde verbinding (http), wordt in direct gerouteerd naar de beveiligde verbinding, zodat door middel van SSL (TLS 1.2) de verbinding tussen de client (browser) en de Konnect infrastructuur beveiligd is.

1.4. Gegevensbeveiliging

Dit betreft zowel de toegang tot gegevens door gebruikers als het beveiligen van de opslag van deze gegevens.

Een gebruiker heeft alleen recht om de gegevens met betrekking tot de locaties en groepen waar de gebruiker aan gekoppeld is. Voor een ouder betreft dit alleen de gegevens van de eigen kinderen en de informatie (zoals foto's) van de groepen waar van de eigen kinderen. Per locatie is instelbaar of een ouder alleen geautoriseerd is voor foto's van het eigen kind of van de groep waar het kind op zit. Een bredere autorisatie dan de groep(en) waar het eigen kind geplaatst is, is niet mogelijk.

Voor medewerkers is het alleen mogelijk informatie te zien en toe te passen van de locaties en groepen waaraan de betreffende medewerker gekoppeld is. Het is mogelijk bepaalde (super) gebruikers (alleen mogelijk voor medewerkers) toegang te geven tot alle locaties en groepen binnen de organisatie, zonder expliciet aan te geven welke dit zijn.

Voor de gegevensopslag zijn verschillende beveiligingsmaatregelen ingeregeld, waaronder:

- Alle foto's, nieuwsbrieven en andere bestanden zijn versleuteld (onleesbaar) opgeslagen op het bestandssysteem. Deze zijn niet leesbaar en alleen leesbaar te maken door het Konnect systeem.
- De toegang tot de database is beveiligd met een wachtwoord.
- Daarnaast is de database en het bestandssysteem alleen toegankelijk vanuit de ouderportaal applicatie en voor de beheerders van Konnect. Hiervoor is een VPN verbinding noodzakelijk, beveiligd met PKI certificaten en gebruikersnaam/wachtwoord.
- Backups van de gegevens zijn op twee fysiek gescheiden locaties beschikbaar.

Aanvullende opmerkingen voor persoonsgebonden gegevens in Konnect:

- De volgende kindgegevens worden opgeslagen: Naam, geboortedatum, geslacht.
- De volgende oudergegevens worden opgeslagen: Naam, geboortedatum, emailadres, telefoonnummers.
- Konnect bevat geen BSN nummers
- De adresgegevens van de ouder worden apart opgeslagen. De verwijziging naar de adresgegevens is versleuteld opgeslagen bij de ouder, zodat de adresgegevens niet gerelateerd kunnen worden aan de persoon.

Indien de persoonsgebonden gegevens van het Kocon back-office systeem te beheren zijn:

- De administratieve gegevens van de ouder (waaronder mogelijk BSN nummer en adresgegevens) zijn alleen per individuele ouder opvraagbaar.
- Bij het opvragen van deze persoonsgebonden gegevens wordt altijd de gebruiker en het wachtwoord (versleuteld) meegestuurd, zodat alleen de ouder zelf in staat is deze gegevens in te zien en te wijzigen.
- Deze persoonsgebonden gegevens worden niet gecached of bewaard, maar worden voor elk individueel verzoek opnieuw opgehaald uit het administratieve systeem.

1.5. Traceerbaarheid van gebruik

Konnect voorziet in de mogelijkheid om bepaalde acties die optreden in het ouderportaal te traceren. Indien acties leiden tot fouten, wordt dit tevens vastgelegd. De gegevens ten behoeve van de traceerbaarheid worden vastgelegd in de auditlog en technische logging.

De volgende acties worden standaard vastgelegd in Konnect ten behoeve van de traceerbaarheid:

- alle inlogpogingen (zowel succesvolle als niet-succesvolle);
- het blokkeren van een gebruiker;
- het uitloggen van een gebruiker of het verlopen van een sessie;
- indicatie dat een bericht verstuurd wordt naar een bepaalde gebruiker met een aanduiding welk type bericht verstuurd wordt

Fouten die zich voordoen in het ouderportaal wordt gelogd in de technische logging. Waar de auditlog zich meer richt op bepaalde functionele acties, richt de technische logging zich op het loggen van technische fouten. Indien zich technische fouten hebben voorgedaan, worden de beheerders van Konnect hier via email direct van op de hoogte gebracht. Op basis van deze actieve signalering, kan het ontwikkelteam van het ouderportaal proactief verbeteringen doorvoeren ter voorkoming van fouten.

1.6. Centrale Konnect omgeving (server)

Konnect wordt standaard gehost in een hostingcentrum in Nederland (Dronen). Het hosting centrum beschikt over de noodzakelijke fysieke beveiliging om:

- ongeoorloofde toegang tot de fysieke infrastructuur te voorkomen
- DDoS aanvallen te signaleren en te blokkeren.