Veiligheid van data en privacy bij het werken met Yuki-software

Toegangsbeveiliging

Yuki gebruikers identificeren zich met een gebruikersnaam (hun eigen email adres) en een wachtwoord. Deze toegangsbeveiliging wordt gerealiseerd door middel van Microsoft.NET Forms Based Security. Dit betekent dat voor heel Yuki 'by design and by default' de toegangsbeveiliging automatisch wordt afgedwongen.

Transportbeveiliging

Alle dataverkeer tussen jouw PC en de servers van Yuki wordt versleuteld middels de SSL encryptietechniek (1024 bits RSA versleuteling). Dit houdt in dat alle gegevens die over het internet gaan (zoals wachtwoorden en financiele cijfers) beveiligd zijn tegen 'afluisteren van het dataverkeer op het internet'.

Digitale serverbeveiliging

De servers van Yuki bevinden zich achter een geavanceerde Basewall firewall om ongeautoriseerde toegang via het internet te voorkomen. Doordat de servers uitsluitend gebruikt worden voor het hosten van de Yuki omgeving is de firewall zodanig strikt geconfigureerd dat vrijwel alle dataverkeer vanaf het internet geblokkeerd wordt.

Fysieke beveiliging

Yuki maakt gebruik van de public Web Services Cloud van Amazon. Amazon is de marktleider in cloud-infrastructuur. De servers van Yuki bevinden zich in de datacenters van Amazon Europe. De data staat opgeslagen bij Amazon in Dublin, Ierland en daarom binnen de EU en haar wet- en regelgeving.

Backup

Van iedere individuele Yuki administratie wordt iedere nacht een back-up gemaakt. Tevens wordt van deze back-up een extra kopie gemaakt die wordt opgeslagen in een ander, op enige afstand gevestigd, datacenter. Dit betekent dat bij alle mogelijke calamiteiten de continuïteit van de opgeslagen data optimaal gegarandeerd is. Database back-ups zijn nu tot op een willekeurig tijdstip binnen de laatste 7 dagen terug te halen.