V1.1/2023

Beveiliging OnView Platform

Veiligheidsverklaring

- OnView BV, hierna te noemen ''OnView'' neemt de beveiliging van persoonlijke gegevens zeer serieus en gebruikt dan ook een aantal technische oplossingen om het gebruik van de webapplicatie veilig te maken.
- Deze veiligheidsverklaring geldt voor alle diensten en websites die worden aangeboden door OnView.

Op gebruikersniveau

- Elke gebruiker heeft een unieke gebruikersnaam en een bijbehorend wachtwoord. Het wachtwoord is alleen bij de gebruiker bekend en is hashed opgeslagen.
- De 'back' knop in de browser is uitgeschakeld, zodat gevoelige gegevens niet uit de historie gehaald kunnen worden.
- Er worden geen gevoelige gegevens lokaal opgeslagen. De computer kan dus gebruikt worden door anderen. Of als de computer bij zijn levenseinde komt, dan kan deze dus veilig bij het vuil gezet worden.
- OnView klanten hebben de mogelijkheid om op een veilige manier in te loggen middels twee factor authenticatie.

Op verbindingsniveau

- Communicatie met OnView gaat over een SSL(Secure Sockets Layer)/HTTPS verbinding. Op deze manier kunnen er geen gevoelige gegevens worden ‘afgeluisterd’. Hiervoor maken wij gebruik van het SSL Certificaat van Quo Vadis.
- SSL zorgt ervoor dat gevoelige informatie gecodeerd wordt. Hierdoor kan deze informatie niet door anderen gelezen worden als deze onderschept zou worden.

Op serverniveau

- Hosting op Windows 2012 R2, Windows 2016 en Windows Server 2019 servers.
- SQL Servers. Deze servers zijn niet rechtstreeks benaderbaar via het Internet.
- We hebben een DDoS beveiliging. Hiermee kunnen we aanvallen van buitenaf tegenhouden.

Datacenter Linfosys

- Met een ‘Managed Firewall’ beveiligen wij ons datacenter. Linfosys verzorgt het beheer en updates van de Firewalls.
- OnView draait op meerdere clusters met meerdere virtuele servers.
- Actieve 24/7 monitoring van hard-, software en netwerk bandbreedte.

Back-up OnView

- We maken volledige back-ups van uw data en deze worden minimaal 7 dagen bewaard in een van de datacenters van Linfosys.
  Voor de recovery van data maken we gebruik van de procedure zoals die is vastgelegd in de ISO-27001 certificering van Linfosys.
- Linfosys maakt gebruik van twee datacenters, waarbij beide datacenters elkaars taken kunnen overnemen in geval van een calamiteit/ramp.

Database

- Database van bestaande OnView klanten worden minimaal 7 jaar bewaard. Tenzij de klant opzegt, dan wordt er handmatig een volwaardige export gemaakt en aan de klant overhandigd. Vervolgens vernietigd OnView alle gegevens van de opdrachtgever na verloop van één maand na het einde van het Abonnement. Hierbij is OnView op geen enkele wijze een schadevergoeding verschuldigd aan welke partij dan ook.

Organisatorisch

- Bewustwording bij medewerkers wordt gestimuleerd door training(en), contractuele verplichtingen en herinneringen.
- Binnen OnView is het elektronische apparatuur volledig versleuteld.
- OnView voert periodieke controles uit op het beveiligingskader. Dit wordt middels interne audits, pentesten en managementbeoordelingen uitgevoerd.

Uw verantwoordelijkheid

- Samen zorgen we ervoor dat uw gegevens veilig zijn. Dit betekent dat u er ook voor moet zorgen dat uw eigen systemen beveiligd zijn. We adviseren u om uw wachtwoord(en) complex te maken en deze ook veilig op te slaan.

Rechten

- De hierboven beschreven verklaring geldt voor de webapplicatie OnView. OnView behoudt zich echter het recht om deze verklaring van tijd tot tijd aan te passen. Deze veiligheidsverklaring is dan ook niet bedoeld als een overeenkomst en er kunnen geen rechten aan ontleend worden.