Beveiligingsprotocol & Adviezen

Versie 2018.7

In dit beveiligingsprotocol beschrijven wij hoe wij onze diensten hebben beveiligd, zowel technisch als organisatorisch. Tevens leggen wij uit hoe bepaalde beveiligingen werken, hoe u deze het beste kunt inzetten, en hoe u kunt handelen in geval van diefstal van laptops/computers.

Organisatorische maatregelen

Al onze medewerkers hebben een geheimhoudingsverklaring getekend.

Wachtwoorden die wij beheren voor ons zelf of ten behoeve van onze klanten zijn versleuteld opgeslagen.

Urios, het programma

Controleer certificaat bij installatie en update

Onze programmatuur is ondertekend met een digitaal certificaat door Eitri B.V. of Urios B.V. U dient zelf bij een download te controleren of het certificaat nog aanwezig is. Windows wijst u hierop bij het uitvoeren van een update of installatie. Windows toont u een scherm “Wilt u toestaan dat deze app wijzigingen aan uw apparaat aanbrengt?” met daarbij een “Geverifieerde uitgever”. Hier dient “Eitri B.V.” of “Urios B.V.” te staan. Als dat niet het geval is komt de update niet van ons. Een digitaal certificaat garandeert dat het programma / de update niet is gewijzigd tussen het moment dat wij het maakte en het u bereikte.

Instellen van wachtwoord voor gebruikers

U kunt zelf een wachtwoord instellen en rechtenniveaus bepalen per gebruiker. Dit is onderdeel van onze Module Gegevensafscherming. Hiermee beperkt u de toegang tot Urios tot personen die het/hun wachtwoord weten. En kunt u de toegang tot bepaalde financiële gegevens afschermen voor uw mede-gebruikers.

TeamViewer

voor het meekijken bij u

Onze helpdesk gebruikt het programma TeamViewer om u te kunnen ondersteunen. Met dit programma kunnen wij op uw computer meekijken en kunnen wij de bediening overnemen.

De verbinding van ons naar uw computer tijdens de sessie is versleuteld. Dit betekent dat derden niet mee kunnen kijken.

Wij kunnen alleen verbinding met uw computer maken als het programma TeamViewer is opgestart en u het ID nummer en het wachtwoord heeft doorgegeven aan ons. Geef deze codes alleen telefonisch door aan personen die u vertrouwd.

Standaard bestaat het wachtwoord uit vier cijfers. U kunt dit wijzigen in TeamViewer door te klikken op Extra’s > Opties, vervolgens bij Beveiliging > Willekeurig wachtwoord (voor spontane toegang). Hier kunt u de wachtwoordsterkte in te stellen.

Wij raden u aan TeamViewer af te sluiten nadat wij (of iemand anders) is ingelogd geweest.

De beveiligingsverklaring van TeamViewer kunt u vinden op:
https://www.teamviewer.com/nl/security/

Er zijn meerdere edities van TeamViewer. Wij gebruiken de TeamViewer QuickSupport. Dat is een programma dat u zelf opstart en zelf kunt afsluiten. Sommige systeembeheerders gebruiken TeamViewer Host waarmee zij te allen tijde toegang tot u systeem kunnen krijgen. Wij raden dit ten sterkste af. Omdat daarmee permanent een poortje naar uw computer openstaat.

Tevens biedt TeamViewer een optie om automatisch te starten bij het opstarten van Windows. Gebruik dit alleen als u een erg sterk / zeer veilig wachtwoord heeft ingesteld en u deze functie daadwerkelijk zelf gebruikt om van bijvoorbeeld thuis in te loggen op uw computer op kantoor.

Urios Cloud Drive

de dienst voor het opslaan van uw bestanden in de cloud

De Urios Cloud Drive is een dienst waarmee uw bestanden worden gesynchroniseerd met een cloudopslag. Wij kopen deze dienst in bij RFC IT. De dienst wordt in Nederland geleverd door Cloud2. De feitelijke opslag vind plaats bij Cloud2. Zij gebruiken hiervoor het programma Anchor van eFolder.

De bestanden staan dus lokaal op uw eigen apparaten en opgeslagen bij Cloud2. De sub-verwerker Cloud2 waar de data is opgeslagen voldoet aan de standaard voor informatiebeveiliging ISO 27001

De initieel door onze uitgegeven wachtwoorden zijn sterke wachtwoorden bestaande uit minimaal 12 karakters, hoofdletters, kleine letters en cijfers.

U kunt zelf het wachtwoord wijzigen, wij raden dat dan ook ten zeerste aan. Handleiding hiervoor: https://support.efolder.net/hc/en-us/articles/115010652868-Anchor-Accessing-and-Managing-Account-Settings Denk er aan dat u na het wijzigen van het wachtwoord u het wachtwoord op al uw apparaten opnieuw moet invoeren.

Bij diefstal van een laptop/computer raden wij u aan deze zo snel mogelijk te laten wipen. Zie de handleiding: https://support.efolder.net/hc/en-us/articles/115010486507-Anchor-Remotely-Wipe-Machines-and-Accounts-Remote-Wipes-

Urios Cloud Database

de dienst waarmee u overal met Urios kunt werken

De clouddatabase is een database die is opgeslagen bij onze sub-verwerker CloudVPS. De sub-verwerker CloudVPS waar de data is opgeslagen voldoet aan de standaard voor informatiebeveiliging ISO 27001. De veiligheidscertificaten en auditrapporten voor CloudVPS kunt u inzien op hun website: https://www.cloudvps.nl/over-cloudvps/certificeringen

De back-ups van de clouddatabase staan opgeslagen bij Cloud2. De sub-verwerker Cloud2 waar de back-up is opgeslagen voldoet aan de standaard voor informatiebeveiliging ISO 27001.

De initieel door onze uitgegeven wachtwoorden zijn sterke wachtwoorden bestaande uit minimaal 12 karakters, hoofdletters, kleine letters en cijfers.

Bij diefstal van een laptop/computer raden wij u aan zo snel mogelijk het wachtwoord te laten wijzigen.

Datamigraties

Voor klanten die overstappen van een ander pakket kunnen wij datamigraties uitvoeren. Hierbij beschikken wij tijdelijk over alle data die in het vorige pakket stond. Na het uitvoeren van de migratie versleutelen wij uw oude data. Deze data verwijderen wij drie maanden nadat wij de migratie hebben uitgevoerd. Wij bewaren deze data tijdelijk omdat in de praktijk is gebleken dat na de initiële migratie het soms nodig is extra data te migreren.