

Beveiligingsprotocol & Adviezen

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

1. Al onze medewerkers zijn contractueel gebonden geheimhouding. Tevens zijn er richtlijnen opgesteld over de omgang met klantgegevens. Deze zijn o.a. omschreven in het Urios Personeelshandboek.
2. Wachtwoorden die wij beheren voor ons zelf of ten behoeve van onze klanten zijn versleuteld opgeslagen. Deze versleuteling kan alleen met een wachtwoord ongedaan worden gemaakt.
3. Ordners waarin fysieke klantgegevens te vinden zijn, zoals Urios Bestelformulieren, worden in een afgesloten kast bewaard.

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 voor Urios instellen en rechte-niveaus bepalen per gebruiker. Dit is onderdeel van onze Module Gegevensafscherming. Hiermee beperkt u de toegang tot Urios tot personen die het/hun wachtwoord weten. Daarnaast kunt u de toegang tot bepaalde financiële gegevens afschermen voor uw medegebruikers.

RealVNC | voor het meekijken bij u

Onze helpdesk gebruikt het programma RealVNC om u te kunnen ondersteunen bij uw vragen. 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 RealVNC is

opgestart en u de 9-cijferige code, die wij aan u verstrekken, heeft ingevuld op uw computer. Wij raden u aan zelf RealVNC af te sluiten nadat wij (of iemand anders) ingelogd is geweest.

De beveiligingsverklaring van RealVNC kunt u vinden op: <https://www.realvnc.com/en/legal/#privacy>

Urios Cloud Drive | de dienst voor het opslaan van uw bestanden in de cloud

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

De bestanden staan dus lokaal op uw eigen apparaten en in de cloud opgeslagen bij Ek.co. De subverwerker Ek.co, waar de data is opgeslagen, voldoet aan de standaard voor informatiebeveiliging ISO 27001.

De initieel door ons uitgegeven wachtwoorden voor uw Urios Cloud Drive zijn sterke wachtwoorden: ze bestaan uit minimaal 12 karakters bestaande uit hoofdletters, kleine letters en cijfers.

U kunt zelf het wachtwoord van uw Cloud Drive wijzigen. Wij raden dit dan ook ten zeerste aan. Zie handleiding:

<https://support.efolder.net/hc/en-us/articles/115010652868-Anchor-Accessing-and-Managing-Account-Settings>

Denk er aan dat u na het wijzigen van uw wachtwoord, het wachtwoord op al uw apparaten opnieuw moet invoeren om weer verbinding te kunnen maken met de Cloud Drive.

Bij diefstal van een laptop of computer raden wij u aan om het hoofdwachtwoord te wijzigen en deze laptop/computer zo snel mogelijk te swipen (bestanden te wissen). Zie 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 cloud database is een database die is opgeslagen bij onze subverwerker CloudVPS. De subverwerker 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 Ek.co. De subverwerker Ek.co, waar de back-up is opgeslagen, voldoet aan de standaard voor informatiebeveiliging ISO 27001.

De initieel door onze uitgegeven wachtwoorden voor de Cloud Database zijn sterke wachtwoorden bestaande uit minimaal 12 karakters bestaande uit hoofdletters, kleine letters en cijfers. Jaarlijks wordt de gebruiker gevraagd om dit wachtwoord te wijzigen.

Bij diefstal van een laptop of computer raden wij u aan zo snel mogelijk het wachtwoord te wijzigen, zodat er vanaf de verdwenen pc geen verbinding meer met de Urios Database gemaakt kan worden.

Datamigraties

Voor klanten die overstappen van een ander pakket kunnen wij een datamigratie uitvoeren. Hierbij beschikken we tijdelijk over alle data die in het vorige pakket stond. Na het uitvoeren van de migratie versleutelen wij uw oude data. Deze versleuteling kan alleen met een wachtwoord ongedaan worden gemaakt.

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. Voor meer informatie zie ons *Privacy protocol nieuwe Urios-gebruikers – Datamigratie*.

Versie 2021.6