



Laatste update: 2 December 2019

Veiligheid en betrouwbaarheid

Vanaf het leggen van de eerste fundamenten van HRorganizer is rekening gehouden met de veiligheid en betrouwbaarheid van het systeem. Veiligheid om ervoor te zorgen dat gegevens alleen door gerechtigde personen gebruikt kunnen worden. Betrouwbaar, zodat gebruikers altijd de beschikking hebben over het systeem. Dit heeft geresulteerd in:

- 99.98% uptime vanaf 2013
- nog nimmer is een poging tot digitale inbraak geslaagd.

Systeemvereisten

Voor het gebruik van onze software-as-a-service adviseren en ondersteunen wij het gebruik van systemen die voldoen aan deze eisen:

Internet

768 kbps DSL (of sneller)

Browser & Besturingssysteem

Een van de volgende browser en besturingssysteem combinaties:

- Internet Explorer 11.0 (en hoger) op Windows 8.1 / Windows 10
- Edge op Windows 10
- Firefox 30.0 (en hoger) op Windows 8 en hoger / MacOS X en hoger
- Chrome 36.0 (en hoger) op Windows 8 en hoger / MacOS X en hoger
- Safari 8.0 (en hoger) op MacOS X 10.10 en hoger
- Android 4.4 (en hoger)
- iOS 8.0 (en hoger)

Aanvullende software

Voor sommige onderdelen is de Adobe Flash Plug-in vereist. We streven ernaar om deze vereiste in 2020 helemaal te laten vervallen.

Maatregelen

Op alle niveaus is rekening gehouden met de veiligheid en betrouwbaarheid.

Gebruikersniveau

- Beveiligde toegang met persoonlijke toegangsgegevens. Deze is versleuteld in ons systeem opgeslagen en dus ook bij ons niet bekend.
- Strikte geautomatiseerde procedure voor het herstellen van de toegang, wanneer het wachtwoord zoek is.
- Op aanvraag uit te breiden met digitale certificaten of eenmalige toegangscode (al dan niet tijdgebonden).

Mobiel en Webapplicatie niveau

- Volledig beveiligde verbinding (https, ssl).
- Alle gegevens worden gepseudonimiseerd opgeslagen. Alleen de applicatie en 3 IT-medewerkers van HRorganizer hebben toegang tot de sleutel.
- Database en back-ups zijn continu versleuteld (met zgn Transparent Data Encryption)
- Ontworpen om gegevens van licentiehouders strikt te scheiden.
- Ontworpen om alle bekende aanvalsmethoden te weerstaan (bijv sql-injection).
- Monitoring van beschikbaarheid en prestatie zowel van binnenuit als van buitenaf.
- 99,8% gegarandeerde beschikbaarheid.

Niveau van de fysieke verbinding

- Dit ligt in vertrouwde handen van ArchiLogiQ (www.archilogiq.nl)
- Datacenters volledig tweevoudig aangesloten op de door ArchiLogiQ beheerde netwerk infrastructuur.
- Deze infrastructuur is voorzien van meerdere redundante internetverbindingen (Gigabit Ethernet backbone).
- De datacenterpartner is gecertificeerd volgens deze richtlijnen: ISO 9001, ISO 27001, ISAE3402

Niveau fysieke locatie centrale computer(s)

- Dit ligt in de vertrouwde handen van Equinix (www.equinix.nl).
- Stroomvoorziening: meervoudig uitgevoerde, schaalbare high capacity, permanent gegarandeerd met Uninterruptible Power Supply (UPS)-systemen en on-site backup dieselgeneratoren.
- Branddetectie en –bestrijding: Very Early Smoke Detection Apparatus (VESDA) in elke ruimte geïnstalleerd, verbonden met het Building Management System (BMS) dat continu in de gaten gehouden wordt vanuit een netwerk operationscenter. Brand wordt

in een zeer vroeg stadium gedetecteerd en via een koppeling met een brandbestrijdingsstelsel gebaseerd op milieuvriendelijk gas of een watermist onmiddellijk geblust met minimale beschadiging van de apparatuur. Verlies van data en bedrijfsonderbreking wordt op deze manier voorkomen.

- Airconditioning: alle datavloeren op een constante temperatuur en een relatieve lage vochtigheid.
- Fysieke beveiliging: fysieke veiligheidsgrenzen, 24x7x365 monitoring door on-site personeel die alle personen die het gebouw binnengaan controleren, een CCTV-videocamerabewaking, en alarmering bij inbraak.
- Toegang: individueel programmeerbare toegangskaarten en visuele identificatie, alleen toegang indien de on-site engineer ons verzoek goedkeurt. Verantwoorde standaardprocedures zorgen ervoor dat we snel toegang krijgen tot de apparatuur, dag en nacht.

Niveau centrale computers (ArchiLogiQ)

- Meerdere computers met virtualisatie hard- and software.
- Automatische 'failover' van virtuele servers naar andere fysieke machines bij het falen van hardware.
- Automatische verdeling van resources van virtuele servers over de fysieke hostservers.
- Gegevens opslag via FC SAN (Fiber Channel Storage Area Network) meervoudig uitgevoerd.
- Veel geraadpleegde gegevens worden automatisch naar snelle SSD storage verplaatst.

Niveau centrale virtuele servers (ArchiLogiQ)

- Voor gepland onderhoud aan hardware kunnen servers verplaatst worden tijdens de operatie (door virtualisatie) naar andere hardware zonder dat dit de beschikbaarheid beïnvloed.
- Op afstand alleen toegankelijk vanaf Spijk 5 in Wageningen, waar gebruik gemaakt wordt van gescheiden netwerken voor medewerkers en gasten.
- Nachtelijke differentiële database back-up, wekelijkse volledige back-up, ieder uur transactie log back-up.
- Eenvoudig op te schalen.