

Bij Fellow Digital's staat **veiligheid centraal**



Inhoudsopgave

Veiligheid in goede handen bij Fellow Digitals	3
Veiligheid, compliance en certificering	4
Algemene verordening gegevensbescherming	
Fellow Digitals certificaten	
ISO 27001	
ISO 27701	
NEN 7510	
Beveiliging van hosting en datacenters	6
Uitwijklocatie	
Fysieke serverbeveiliging	
Critical Environment Management	
Stroomvoorziening	
Patchmanagement	
Digitale bescherming	
Gebouw- en brandbeveiliging	
Serverlocatie in datacenter	
Secure by design software development	8
Branche protection	
Automated testing	
Code reviews	
Applicatie specifieke voorzorgsmaatregelen	9
Single Sign-On	
Twee-factor authenticatie	
Gebruikersrechten en rollen	
Streng wachtwoord-beleid	
Automatisch accounts blokkeren	
User provisioning API	
Audit trail logging	
Multi-tenant architectuur	
Externe audits	11
Code reviews en penetratietests	
ISO & NEN	
Overige zekerheden	12
SLA met 99,9% uptime	
REST-API	

Veiligheid in goede handen

bij Fellow Digital

In het tijdperk van AVG is de beveiliging van gegevens essentieel. Onze klanten vertrouwen erop dat de veiligheid van hun gegevens en informatie altijd topprioriteit zijn. In deze brochure lees je hoe Fellow Digital voldoet aan de hoogste mogelijke beveiligingsstandaarden, zodat iedereen met een gerust gevoel aan de slag kan gaan, ook thuis.

Wat betreft beveiliging doen wij geen concessies. Al sinds 1997 vertrouwen onze klanten erop dat zij in een veilige en betrouwbare omgeving kunnen werken. Ook bij het koppelen of integreren van andere platformen of bij het uitnodigen van externe gebruikers. Onze servers worden 24 uur per dag bewaakt door de Nederlandse hostingprovider, in de wetenschap dat ieders veiligheid onaangetast blijft.

ISO 27001 is een internationaal erkende beveiligingsstandaard die eisen specificeert voor het opzetten, implementeren, onderhouden en continu verbeteren van informatiebeveiligingsbeheersystemen. Belangrijk te weten dat Fellow Digital beschikt over het NEN 7510-certificaat, dat zich richt op informatiebeveiliging in de zorgsector.

Ook beschikt Fellow Digital sinds 2022 over het ISO 27701 certificaat. De internationale norm ISO 27701 biedt richtlijnen voor de bescherming van privacy, hoe organisaties persoonlijke informatie moeten beheren en ondersteunt de norm bij de naleving van privacyregels wereldwijd.



Veiligheid, **compliance** **en certificering**

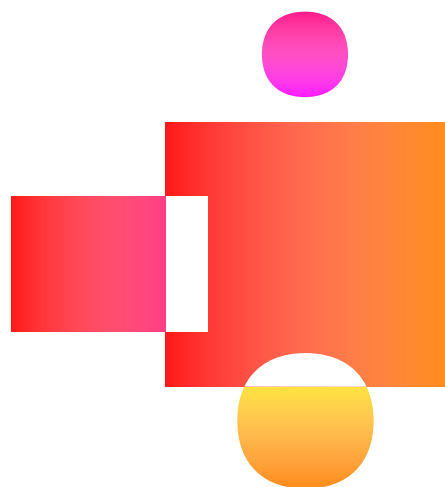
De veiligheid van jullie bedrijfsgegevens staat altijd centraal bij Fellow Digital's. Om die veiligheid te waarborgen worden onze servers onder 24 uren bewaking in Nederland gehost. Hiermee voldoen we aan de Algemene Verordening Persoonsgegevens van de EU (AVG/GDPR). Daarnaast zijn we ISO/IEC 27001, ISO/IEC 27701 en NEN 7510 gecertificeerd.

Algemene verordening gegevensbescherming

De producten van Fellow Digital's worden gehost in Nederland. Onze beveiligingsstandaarden voldoen aan de eisen van de Europese Algemene Verordening Gegevensbescherming (AVG) en zijn van toepassing op gegevens van medewerkers, stakeholders en klanten.

Op het gebied van veiligheid blijft Fellow Digital's zich ontwikkelen. Dit blijkt onder andere uit het in 2022 behaalde ISO 27701 certificaat. ISO 27701 bevat maatregelen specifiek gericht op de bescherming van privacygevoelige informatie.

Medewerkers van Fellow Digital's zijn op de hoogte van de huidige privacy-regelgeving. Hiermee beschikken zij over de meest actuele kennis om de veiligheid van jullie gegevens te garanderen.



Fellow Digital's certificaten

ISO 27001

Fellow Digital's is ISO 27001 gecertificeerd. Dit betekent dat wij voldoen aan de hoogste eisen rondom gegevens- en informatiebeveiliging. Gebruikers kunnen gebruik maken van de producten van Fellow Digital's, zonder zich zorgen te maken over de veiligheid. Met het ISO 27001 certificaat laat Fellow Digital's het volgende zien:

- ✓ Een zorgvuldige omgang met data op alle niveaus
- ✓ Naleving van de wet- en regelgeving
- ✓ Een geloofwaardig en professioneel bedrijf te zijn
- ✓ Het inperken van de kans op risico's en incidenten



ISO 27701

De ISO 27701 norm is een uitbreiding op de ISO 27001 norm voor informatiebeveiliging, en geeft specifieke beheersmaatregelen voor privacygevoelige gegevens.

Deze norm biedt de zekerheid dat Fellow Digital's voldoet aan de internationale eisen ten aanzien van de bescherming van persoonsgegevens in de breedste zin van het woord.

NEN 7510

Waar de ISO 27001 norm zich richt op 'algemene' gegevens- en informatiebeveiliging, richt de NEN 7510 norm zich specifiek op de bescherming van medische persoonsgegevens. Het NEN 7510 keurmerk is een zeer relevant certificaat voor diverse klanten van Fellow Digital's in de gezondheidszorg.



Beveiliging van **hosting** **en datacenters**

Persoonsgegevens, documenten en bedrijfsinformatie. Dit zijn zomaar wat voorbeelden van data die geplaatst kunnen worden in de platformen van Fellow Digital's. Deze gegevens worden op een fysieke locatie opgeslagen die voldoet aan de hoogst mogelijke veiligheidseisen. Hiermee wordt de kans op calamiteiten of diefstal tot het minimum beperkt.

De servers van Fellow Digital's worden door Exonet gehost en beheerd. Exonet is ISO 27001, ISO 9001 en NEN 7510 gecertificeerd en voldoet daarmee aan de hoogste beveiligingsnormen. De server bevindt zich in het datacenter van BIT in Ede. Back-ups worden beveiligd opgeslagen in een tweede (fallback) datacenter: Smartdc in Rotterdam (Nederland).

Onze servers zijn standaard uitgerust met de meest actuele beveiligingspatches. De servers staan achter een firewall, waardoor ze niet toegankelijk zijn voor hackers en andere aanvallers.

Kenmerken van Exonet (Managed Hosting)

- ✓ ISO 27001, ISO 9001 en NEN 7510 gecertificeerde managed hosting
- ✓ Klantgerichtheid, klanttevredenheid, klachtenmanagement
- ✓ Dienstverleningsprocessen, productontwikkeling
- ✓ Kwaliteitsaudits
- ✓ Integratie van producten en open standaarden
- ✓ Service Level Agreement (SLA)
- ✓ Uptime van minimaal 99,9%
- ✓ Hosting en onderhoud van de systemen
- ✓ Testsystemen, testprocedures en incidenten

Kenmerken van BIT en Smartdc (datacenter)

- ✓ ISO 27001
- ✓ NEN 7510
- ✓ Uitwijklocatie



Uitwijklocatie

We gaan er niet van uit, maar wat als één of meerdere servers uitvallen door een calamiteit? Bij Fellow Digitals nemen wij geen enkel risico. Daarom beschikken wij sinds 2021 over een uitwijklocatie. Hier staat een serveromgeving die identiek is aan de omgeving in ons primaire datacenter en wordt ook beheerd door onze hostingprovider Exonet. Zo heb je razendsnel weer toegang tot je gegevens.

Fysieke serverbeveiliging

- ✓ 24/7 bezetting van het Operation Center
- ✓ 24/7 veiligheidspatrouilles
- ✓ Permanente CCTV-bewaking
- ✓ Beveiliging tegen ongeoorloofde toegang en alarmbeveiliging op het terrein en in het gebouw
- ✓ Toegang tot het gebouw en het terrein alleen via sluizen en veiligheidsbarrières
- ✓ VEB-gecertificeerd beveiligingsklasse 4
- ✓ Aparte uitwijklocatie bij calamiteiten

Critical Environment Management

- ✓ Ervaren managementteam
- ✓ (Thermische) klimaatbeheersing
- ✓ Permanente monitoring van de gebouwbeheersystemen (BMS)
- ✓ Internationaal erkend Critical Environment Programme

Stroomvoorziening

- ✓ Stroomvoorziening: 50 kV
- ✓ Ononderbroken stroomvoorziening – tot 48 uur bij volle capaciteit
- ✓ 1.500 W/m2 (hoger mogelijk)

Patchmanagement

Dagelijks worden er beveiligingsupdates en besturingssysteempatches geïnstalleerd. Dringende hotfixes worden op verzoek uitgevoerd (noodonderhoud). Bij elke versie van Fellow Intranet of Fellow LMS worden de codeafhankelijkheden bijgewerkt. Om het patchmanagementproces te controleren voert een derde partij (bijv. Securify) regelmatig controles uit. Hier lees je meer over in het hoofdstuk “Externe audits”.

Digitale bescherming

- ✓ SSL/HTTPS-versleuteling
- ✓ Firewalls
- ✓ Regelmatige beveiligingspatches
- ✓ Penetratietests
- ✓ Servermonitoring 24 uur per dag, 365 dagen per jaar
- ✓ Beheer via gescheiden VPN-netwerk
- ✓ Server virtualization
- ✓ Central logging
- ✓ Off site backup
- ✓ Encrypted Data Storage

Gebouw- en brandbeveiliging

- ✓ Rook- en brandmelders door het hele gebouw
- ✓ Inergen-gas (blusmiddel) op technische afdelingen
- ✓ Betonnen muren en dak

Serverlocatie in het datacenter

- ✓ Hardware in speciale racks in datacenters
- ✓ Virtuele hardware voor een hogere beschikbaarheid en schaalbaarheid
- ✓ Hardware dubbel uitgevoerd

Secure by design

software development

Fellow Digitalis ontwikkelt haar software volgens het secure by design principe. De veiligheid en bescherming van (persoons-) gegevens vormen het uitgangspunt bij het ontwerp van nieuwe functionaliteiten en verbeteringen. Hierbij volgen wij onder meer de volgende richtlijnen:

- ✓ OWASP Top 10
- ✓ ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum

Branch protection

Fellow Digitalis maakt gebruik van branche protection, waardoor aanpassingen in de programmacode altijd volgens het vier-ogenprincipe wordt gecontroleerd voordat het in productie gaat.

Automated testing

Fellow Digitalis maakt gebruik van Selenium automated testing. Door continu regressietests uit te voeren worden mogelijke fouten vroegtijdig opgespoord en verholpen.

Code reviews

Het externe bureau Securify voert op gezette tijden penetratietests en white box code reviews uit. Met behulp van Securify sporen wij proactief problemen in onze software op. En blijven wij up-to-date met de laatste ontwikkelingen wat betreft informatiebeveiliging.

Naast de regelmatige interne beveiligingsaudits en penetratietests, helpt Fellow Digitalis klanten ook graag met hun eigen tests en penetratietests.



DDoS-protectie en anti-virus

Denial of service attacks (DDoS) zijn helaas een bekend fenomeen op het internet. Gelukkig beschikt Fellow Digitalis over een inbraakdetectiesysteem waarmee dit soort aanvallen snel kunnen worden geconstateerd en ingedamd. Bij een DDoS-aanval wordt het verkeer via de Nationale Wasstraat (NaWas) omgeleid en "schoon" afgeleverd.

Fellow Digitalis gebruikt dagelijks bijgewerkte virusscanners om gevaar van buiten af tot het minimum te beperken.



Applicatie specifieke voorzorgsmaatregelen

Onze producten Fellow Intranet en Fellow LMS voldoen aan de hoogste veiligheidseisen. Beide producten beschikken over de moderne technologieën om veilig gebruik van de software te garanderen.

Single Sign-On

De producten van Fellow Digital's bieden de mogelijkheid om in te loggen met Single Sign-On (SSO). Gebruikers hoeven slechts één keer in te loggen waarna zij veilig en eenvoudig kunnen schakelen tussen de gekoppelde systemen. Fellow Digital's ondersteunt SAML of OpenID Connect om bijvoorbeeld Active Directory te integreren.

Twee-factor authenticatie

Fellow Intranet en Fellow LMS ondersteunen twee-factor authenticatie (2FA). Hierbij wordt een extra stap toegevoegd aan het inlogproces. Wanneer 2FA is geactiveerd zijn deelnemers verplicht om naast gebruikersnaam en wachtwoord, ook een tijdelijke pincode in te voeren, met behulp van de Google Authenticator app.

Gebruikersrechten en rollen

Binnen Fellow Intranet en Fellow LMS heb je de mogelijkheid om in te stellen welke gebruikers welke bevoegdheden hebben. Onze software heeft een fijnmazig authenticatiemodel. Waarin verschillende rechten en rollen onderscheiden worden.

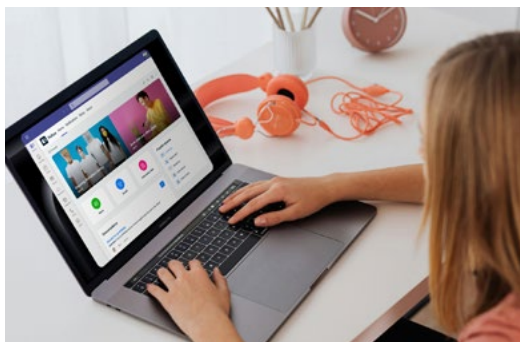


Single Sign-On in de praktijk

Een eindgebruiker maakt gemiddeld gebruik van wel 9 verschillende inlogcodes voor allerlei applicaties. Dit leidt tot situaties waarbij werknemers dezelfde wachtwoorden gebruiken en deze opslaan op slecht beveiligde locaties. Niet ideaal dus.

Single Sign-On biedt hierin uitkomst. Dankzij open standaarden kan een veilige verbinding tussen Fellow Intranet of Fellow LMS met Active Directory tot stand worden gebracht, waardoor je slechts één keer in hoeft loggen met dezelfde gegevens. Dit is niet alleen veiliger, maar ook gebruiksvriendelijker.

Hierdoor is het mogelijk om snel te schakelen tussen Fellow Intranet, Fellow LMS en andere gekoppelde applicaties zoals bijvoorbeeld Office 365.



Gebruikersrechten in de praktijk

Fellow Intranet en Fellow LMS hanteren de volgende rechtenniveaus.

Fellow Intranet

Lezen - Documenten lezen

Reageren - Lezen en reageren op documenten

Toevoegen - Voeg documenten toe aan het platform

Bewerken - Bewerk de inhoud van documenten

Beheren - Alle beheersfuncties van het platform

Fellow LMS/ LMS+

Deelnemer - Deelnemen als cursist

Assistent - Gebruikers- en inschrijfmanagement

Auteur - Contentcreatie en managementfuncties

Auditor - Beoordelen van content en resultaten

Trainer - Beoordelen en geven van feedback

Manager - Alle bovenstaande rechten plus het beheer van de academie

Streng wachtwoord-beleid

Wanneer een deelnemer een account bij Fellow Intranet of Fellow LMS creëert, moet deze voldoen aan een aantal eisen. Zoals de lengte en het gebruik van speciale karakters. Dit maakt het account minder hack-gevoelig.

Automatisch accounts blokkeren

Ons systeem zal een gebruikersaccount automatisch blokkeren wanneer het maximaal aantal foutieve login-pogingen is bereikt.

User provisioning API

Via een API-connectie is het mogelijk om user provisioning te realiseren. Dit houdt in dat er op een eenvoudige, maar veilige wijze deelnemers aan het platform kunnen worden toegevoegd en verwijderd.

Audit trail logging

De log-bestanden van activiteiten worden op een centrale server bewaard en zo veilig zijn gesteld voor audits en mogelijk forensisch onderzoek.

Multi-tenant architectuur

In een multi-tenant architectuur werken meerdere instanties van een applicatie in een gedeelde omgeving. Deze techniek zorgt er voor dat klanten op een veilige manier tegelijkertijd gebruik kunnen maken van het platform.

Externe **audits**

Om er zeker van te zijn dat de genomen veiligheidsmaatregelen het gewenste effect hebben, wordt Fellow Digitalts met regelmaat gecontroleerd door externe partijen.

Code reviews en penetratietests

Het Nederlandse bedrijf Securify voert meerdere keren per jaar diverse soorten tests uit. De veiligheid en betrouwbaarheid van het platform wordt geverifieerd. Fouten worden gerapporteerd, zodat deze tijdig worden verholpen.



- ✓ Penetratietest (ieder kwartaal)
- ✓ White box code review (jaarlijks)



ISO en NEN

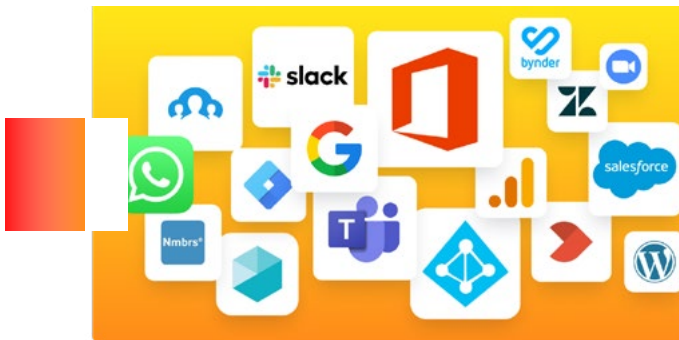
Kiwa is een Nederlandse organisatie voor het testen, inspecteren en certificeren van producten, systemen en processen. Deze instantie is verantwoordelijk voor de jaarlijkse audits en certificering van Fellow Digitalts.

- ✓ ISO 27001
- ✓ ISO 27701
- ✓ NEN 7510

Overige **zekerheden**

SLA met 99,9% uptime

Fellow Digitals levert haar diensten met een service level agreement (SLA). Hierin worden afspraken gemaakt over de kwaliteit van onze dienstverlening. Wij garanderen een uptime van 99,9%, waarmee jullie platform nagenoeg altijd online bereikbaar is.



REST-API

Met de industriestandaard REST-API van Fellow Intranet en Fellow LMS kunnen andere applicaties eenvoudig worden geïntegreerd. Zo wordt jullie platform het hart van de digitale werkplek voor alle bedrijfs- of leermanagementprocessen.

Heb je nog **vragen?**

Wij helpen je **graag**

Neem contact met ons op via info@fellowdigitals.com
of bel naar +31 (0)20 305 76 60

Fellow Digitals bv

Amsterdam Office

Weesperplein 4A
1018 XA Amsterdam
Nederland

T: +31 (0)20 305 76 60
www.fellowdigitals.com
info@fellowdigitals.com

Fellow Digitals GmbH

Keulen Office

Brüsseler Str. 25
50674 Keulen
Duitsland

T: +49 (0)221 828 293 64
www.fellowdigitals.de
info@fellowdigitals.de

Bayern Office

Hauptstrasse 48
83684 Tegernsee
Duitsland

+49 (0)221 828 293 64
www.fellowdigitals.de
info@fellowdigitals.de

Fellow Digitals Pte. Ltd.

Singapore Office

1 Paya Lebar Link #04-01,
Paya Lebar Quarter
408533 Singapore

T: +65 9155 4446
www.fellowdigitals.com
info@fellowdigitals.com

Succeeding together

