WOMsys

Beveiligings- en architectuuroverzicht

Werkorder Management Systeem · t.b.v. ICT-beoordeling · versie 2026 Q2 · publieke versie

Onderdeel	Waarde
Opgesteld door	DC WebApps (Dennis Ceulemans)
Datum	juni 2026 · revisie 2026 Q2
Betreft	WOMsys monteurs-app (Android) en monteurs-webomgeving
Wijzigingen in deze revisie	Media-/signed-URL-beveiliging toegevoegd (sectie 4 en 7); Firebase (Crashlytics/FCM) en bijbehorende gegevensverwerking transparant gemaakt (sectie 9, 15 en 16); access-token ook in de Android Keystore; overgestapt op een kwartaal-versieschema.

1. Inleiding en doel

Dit document beschrijft de opzet en beveiliging van WOMsys, het werkordermanagementplatform dat onderhoudsmonteurs ondersteunt bij hun dagelijkse werk. Het is bedoeld om ICT-/securityafdelingen inzicht te geven in de architectuur, de gegevensverwerking en de beveiligingsmaatregelen, zodat een onderbouwde afweging gemaakt kan worden over het toelaten van de applicatie op (zakelijke) toestellen.

WOMsys bestaat uit drie onderdelen: een beheeromgeving voor kantoor (webapplicatie), een mobiele omgeving voor monteurs (zowel een Android-app als een mobiele webpagina) en een centrale server (backend) met database. Alle onderdelen communiceren uitsluitend via versleutelde verbindingen met dezelfde beveiligde server.

2. Onderdelen van het platform

Onderdeel	Beschrijving
Beheeromgeving	Webapplicatie voor kantoor (app.womsys.nl): aanmaken en plannen van werkorders, klantbeheer, toolboxen, rapportages, gebruikersbeheer en audit-overzicht.
Monteurs-app (Android)	Native app (pakketnaam nl.womsys.monteurs) voor monteurs in het veld: werkorders bekijken, foto's maken, storingen melden, toolboxen ondertekenen.
Monteurs-webpagina	Mobiele webversie (monteurs.womsys.nl) met dezelfde functionaliteit als de app, voor toestellen waarop geen app geïnstalleerd kan worden.
Backend + database	Centrale server die alle gegevens beheert en de logica uitvoert. De app en webpagina bevatten zelf geen bedrijfsgegevens; die worden bij gebruik opgehaald van de server.

3. Technische architectuur

De applicatie volgt een klassieke client-server-opzet. De mobiele app en de webpagina zijn 'clients' die zelf geen gevoelige logica of data bevatten; zij tonen alleen wat de server hen toestuurt na succesvolle authenticatie.

Aspect	Hoe geregeld
Backend	Node.js met Express, draaiend onder procesbeheer (PM2). Verwerkt alle verzoeken en autorisatie.

Aspect	Hoe geregeld
Database	PostgreSQL. Bevat alle bedrijfs-, werkorder- en gebruikersgegevens, strikt gescheiden per bedrijf.
Webserver	nginx als reverse proxy, met afgedwongen HTTPS (TLS) op alle domeinen.
Mobiele app	Gebouwd met Capacitor 7.4, een breed gebruikt, open framework voor hybride apps. Minimum ondersteunde Android-versie: API 23 (Android 6.0).
Hosting	Strato VPS, datacenter in Duitsland (EU).
Besturingssysteem	Ubuntu 24.04 LTS.

4. Transportbeveiliging

Alle communicatie tussen de app/webpagina en de server verloopt uitsluitend via HTTPS (TLS). Er is geen onversleuteld verkeer. De domeinen app.womsys.nl en monteurs.womsys.nl beschikken over geldige SSL-certificaten.

- Versleuteld transport (TLS) voor alle dataverkeer, zowel app als webpagina.
- De mobiele app communiceert uitsluitend met de eigen, vaste server. Er worden geen verbindingen gelegd met onbekende of externe partijen (m.u.v. Google Firebase voor pushmeldingen en crashdiagnose; zie sectie 11 en 15).
- Gevoelige gegevens worden nooit in URL-parameters meegestuurd. De ondertekende media-URL's (zie hieronder) bevatten enkel een tijdelijke, niet-geheime handtekening — geen inloggegevens of persoonsgegevens.
- Geüploade media (foto's, pasjes) zijn niet anoniem opvraagbaar: elk bestand wordt geserveerd via een per-bestand ondertekende, kortlevende URL (HMAC-SHA256, circa 1 uur geldig). Zonder geldige handtekening weigert de server het bestand (HTTP 401). Dit is gehandhaafd op zowel app.womsys.nl als monteurs.womsys.nl.

5. Authenticatie en autorisatie

Toegang tot het systeem vereist altijd een persoonlijke gebruikersnaam en wachtwoord. Na inloggen ontvangt de gebruiker een tijdelijk toegangsbewijs (token) dat na 24 uur automatisch verloopt en daarna opnieuw moet worden verkregen. Optioneel — en op organisatieniveau verplicht te stellen — geldt daarnaast tweestapsverificatie (2FA).

Aspect	Hoe geregeld
Wachtwoorden	Worden versleuteld opgeslagen met bcrypt (een sterke, eenrichtings-hashfunctie). Wachtwoorden worden nooit in leesbare vorm opgeslagen of verstuurd.
Sessie / token	JSON Web Token (JWT) met een geldigheid van 24 uur. Elk token bevat een server-side token-versie waarmee individuele sessies onmiddellijk ingetrokken kunnen worden (zie sectie 6).
Refresh-tokens	Voor langere sessies (max 60 dagen) wordt een server-side refresh-token uitgegeven. Refresh-tokens zijn server-side intrekbaar en worden gehashed (SHA-256) opgeslagen — nooit in leesbare vorm.
Tweestapsverificatie (2FA)	Beschikbaar op app én webomgeving. Optioneel per gebruiker en door een beheerder bedrijfsbreed verplicht te stellen. Gebaseerd op TOTP (RFC 6238) en werkt met standaard authenticator-apps (Google/Microsoft Authenticator, Authy, 1Password). Bij verplichtstelling worden gebruikers zonder 2FA bij de eerstvolgende login gedwongen tot het instellen ervan (QR-enrollment) vóórdat toegang wordt verleend. Eenmalige recovery codes dienen als noodtoegang.

Aspect	Hoe geregeld
Rolgebaseerde toegang	Iedere gebruiker heeft een rol (bijv. monteur, werkvoorbereider, beheerder). Functies en gegevens zijn afgeschermd op basis van expliciete rechten per rol.
Scheiding per bedrijf	Een server-side controle (tenant-isolatie) zorgt dat een gebruiker uitsluitend gegevens van het eigen bedrijf kan benaderen. Gegevens van verschillende bedrijven zijn strikt gescheiden.
Biometrie (optioneel)	De app ondersteunt ontgrendeling via de biometrie van het toestel (vingerafdruk/gezicht). Biometrische gegevens blijven op het toestel en worden nooit naar de server gestuurd.

6. Sessiebeheer bij verlies of diefstal van toestel

Wanneer een monteur zijn of haar toestel verliest of dit gestolen wordt, kan een beheerder de toegang van die gebruiker per direct intrekken via een knop in het gebruikersbeheer. Deze actie maakt zowel lopende sessies als opgeslagen refresh-tokens onmiddellijk ongeldig — er hoeft niet gewacht te worden tot het 24-uurs-token vanzelf verloopt.

Aspect	Hoe geregeld
Intrek-knop	Per gebruiker beschikbaar in het gebruikersbeheer (zichtbaar voor beheerders en bedrijfsadmins).
Effect op refresh-tokens	Alle actieve refresh-tokens van de gebruiker worden in één keer ongeldig verklaard. Er kunnen geen nieuwe sessies meer worden gestart zonder opnieuw in te loggen.
Effect op lopende sessie	De server verhoogt de token-versie van de gebruiker. Bij de eerstvolgende API-aanvraag (typisch binnen één seconde) wordt het bestaande JWT geweigerd met de melding 'Sessie is ingetrokken'. De app of webpagina dwingt direct opnieuw inloggen af.
Logging	Elke intrek-actie wordt vastgelegd in het audit-logboek met wie/wanneer/IP en welke gebruiker is ingetrokken (zie sectie 14).

Praktisch betekent dit dat een beheerder bij verlies of diefstal van een toestel de toegang van de betreffende monteur binnen enkele seconden volledig kan blokkeren. Dit is een gerichte maatregel die uitsluitend de geselecteerde gebruiker raakt; andere gebruikers blijven onverstoord ingelogd.

7. Gegevensopslag en -locatie

Alle bedrijfsgegevens worden centraal opgeslagen in de database op de server in het EU-datacenter (Duitsland). De mobiele app slaat zelf geen bedrijfsgegevens permanent op het toestel op.

Aspect	Hoe geregeld
Serverlocatie	Datacenter in Duitsland (EU). Onder de Europese privacywetgeving (AVG/GDPR).
Opslag op het toestel	Op de Android-app worden uitsluitend het toegangstoken en het refresh-token lokaal bewaard, en wel in de Android Keystore: een door het besturingssysteem beheerde, hardware-ondersteunde versleutelde opslag die door andere apps niet uitleesbaar is. In de browserversie staan deze tokens in de standaard, sandboxed browseropslag (browsers bieden geen hardware-keystore). Er staat geen klant- of werkorderdata op het toestel.
Foto's en meldingen	Worden bij het maken direct naar de beveiligde server geüpload en niet als losse bestanden buiten de app bewaard. Op de server zijn ze uitsluitend via een ondertekende, kortlevende URL opvraagbaar (zie sectie 4).

Aspect	Hoe geregeld
Uitloggen	Bij uitloggen worden zowel het toegangstoken als het refresh-token uit de Keystore (resp. browseropslag) verwijderd.

8. Back-up en noodherstel

De gegevens worden centraal opgeslagen op de server; de continuïteit daarvan wordt geborgd met geautomatiseerde, geteste back-ups en een versleutelde kopie buiten de productieserver.

Aspect	Hoe geregeld
Dagelijkse back-up	De volledige database (inclusief de gebruikersrollen) wordt elke nacht automatisch geback-upt via een geplande taak. Elke back-up wordt direct na het maken op integriteit gecontroleerd; faalt die controle, dan slaat het proces alarm.
Versleutelde off-site kopie	Iedere back-up wordt client-side versleuteld en gerepliceerd naar een onafhankelijke opslaglocatie in een tweede EU-datacenter (Hetzner, Duitsland). Deze kopie staat volledig los van de productieserver, zodat verlies, uitval of compromittering van de server niet leidt tot verlies van de back-ups.
Bewaarbeleid (retentie)	Er worden 7 dagelijkse, 4 wekelijkse en 6 maandelijkse versies bewaard; oudere versies worden automatisch opgeschoond. Deduplicatie houdt de benodigde opslag minimaal.
Afscherming	Lokale back-ups zijn uitsluitend leesbaar voor het systeemaccount (bestandsrechten 600). De off-site kopie is versleuteld met een sleutel die niet in leesbare vorm op de productieserver staat.
Getest herstel	De herstelprocedure is daadwerkelijk getest: back-ups zijn aantoonbaar terug te zetten en op integriteit geverifieerd — zowel lokaal als vanaf de off-site kopie. Een apart herstel-draaiboek beschrijft de stappen voor een volledige herbouw.
Hersteltijd (indicatie)	Door de beperkte omvang van de dataset is een volledige database-restore een kwestie van minuten. Herbouw van een complete server inclusief restore is doorgaans binnen enkele uren gereed.

9. De Android-app in detail

De app is gebouwd met Capacitor 7.4. Hieronder staan de toestelrechten (permissions) die de app gebruikt, met telkens de reden. De app vraagt uitsluitend rechten die nodig zijn voor de werkfunctionaliteit.

Toestelrecht	Waarvoor gebruikt
Camera	Foto's maken bij werkorders en storingen.
Locatie	Navigatie naar werklocaties en het vastleggen van een check-in bij een werkorder.
Notificaties	Pushmeldingen voor nieuwe werkorders, planning en toolboxen.
Camera (QR)	Scannen van QR-codes op locatie om snel de juiste klant/werkorder te openen.
Biometrie	Optionele, snelle en veilige ontgrendeling van de app.

Wat de app nadrukkelijk NIET doet

Voor de beoordeling is het volgende relevant. De app:

- heeft geen toegang tot contacten, sms-berichten, oproepgeschiedenis of e-mail op het toestel;
- heeft geen toegang tot bestanden buiten de eigen, afgeschermde app-omgeving;
- vereist geen root- of jailbreak-toegang en wijzigt geen systeeminstellingen;
- bevat geen advertenties en geen commerciële tracking- of reclamemodules; voor crashdiagnose en pushmeldingen gebruikt de app Firebase (Crashlytics + Cloud Messaging, Google), wat standaard Google-componenten en een advertentie-ID-permissie meebrengt — die WOMsys niet voor advertenties of profilering inzet;
- voert geen achtergrond-locatietracking uit buiten actief gebruik van de werkfuncties;
- bewaart geen bedrijfsgegevens permanent op het toestel — alles wordt bij gebruik opgehaald van de beveiligde server.

Distributie en beheer

- Via de officiële Google Play Store (uitrol via een besloten testkanaal is in voorbereiding);
- Via een Mobile Device Management (MDM)-oplossing of Managed Google Play, zodat ICT de installatie en updates centraal kan beheren;
- Via een directe, met een vaste release-sleutel (CN=WOMsys Monteurs) ondertekende installatie (APK) vanaf de eigen beveiligde omgeving, zodat updates verifieerbaar van dezelfde uitgever afkomstig zijn.

Wij werken graag mee aan de distributievorm die past binnen het beveiligingsbeleid van de organisatie, inclusief plaatsing in een MDM-catalogus.

10. De monteurs-webpagina

- Dezelfde authenticatie (inloggen, token van 24 uur, en tweestapsverificatie indien verplicht) en dezelfde rolrechten als de app.
- Volledig over HTTPS; er wordt niets buiten de browser-sandbox op het toestel geschreven.
- Geschikt voor toestellen met een strikt app-beleid: alleen een browser en internettoegang naar monteurs.womsys.nl zijn nodig.

11. Pushmeldingen

Pushmeldingen verlopen via Firebase Cloud Messaging (FCM) van Google, de standaardvoorziening voor meldingen op Android. De inhoud van een melding bevat uitsluitend een korte titel en omschrijving (bijvoorbeeld 'Nieuwe toolbox'); er wordt geen gevoelige bedrijfsinformatie in de melding zelf meegestuurd.

12. Netwerk: te whitelisten adressen en poorten

Om de app of webpagina te laten functioneren binnen een beheerd netwerk hoeven uitsluitend onderstaande adressen bereikbaar te zijn (uitgaand verkeer). Wij adviseren whitelisting op domeinnaam in plaats van op IP-adres, omdat IP-adressen bij de hostingpartij kunnen wijzigen.

Adres	Poort en doel
app.womsys.nl	TCP 443 (HTTPS) — API-verkeer en het ophalen van documenten/PDF's. Gebruikt door zowel de app als de beheeromgeving.
monteurs.womsys.nl	TCP 443 (HTTPS) — de mobiele webversie.
fcm.googleapis.com	TCP 443 — Firebase Cloud Messaging (pushmeldingen, Google).
firebaseinstallations.googleapis.com	TCP 443 — registratie van het toestel voor pushmeldingen.

Adres	Poort en doel
firebasecrashlytics.googleapis.com	TCP 443 — aanlevering van crashrapporten (Crashlytics, Google).
Google FCM-verbinding	TCP 5228 (en 5229/5230 als reserve) — de vaste verbinding die Android gebruikt voor pushmeldingen. Dit is standaard Android-/Google-verkeer.

Het serverplatform draait bij Strato (VPS, datacenter Duitsland). Voor whitelisting heeft de domeinnaam de voorkeur boven het IP-adres. Inkomend hoeft op de toestellen niets te worden opengezet — al het verkeer wordt door de app/webpagina zelf geïnitieerd (uitgaand).

13. Beheer, updates en kwetsbaarhedenbeleid

Onderdeel	Beleid
Besturingssysteem	De server draait Ubuntu 24.04 LTS en ontvangt reguliere security-updates.
Afhankelijkheden	De gebruikte softwarebibliotheken (o.a. Node.js, Capacitor) worden periodiek bijgewerkt. Bekende kritieke kwetsbaarheden (CVE's) worden met voorrang verholpen.
TLS-certificaten	Worden automatisch vernieuwd, zodat verbindingen altijd geldig versleuteld blijven.
App-updates	Nieuwe versies worden uitgebracht via het gekozen distributiekanaal (Play Store / MDM) en zijn ondertekend met een vaste release-sleutel. Bij beheer via MDM kan de organisatie updates centraal uitrollen.
Server-hardening	De server is afgeschermd met een firewall die uitsluitend de noodzakelijke poorten toelaat (HTTPS en beheertoegang). SSH-toegang verloopt uitsluitend via sleutels (geen wachtwoord-login), verdachte inlogpogingen worden automatisch geblokkeerd, en interne diensten (database en applicatieserver) zijn alleen lokaal benaderbaar — niet vanaf het internet.
Incidenten / datalekken	Bij een (vermoed) datalek wordt de betrokken organisatie geïnformeerd, conform de AVG-meldplicht (binnen 72 uur). Een verwerkersovereenkomst kan dit nader vastleggen.

14. Logging, audit-trail en toezicht

Het systeem houdt een centraal audit-logboek bij in de database. Hiermee is achteraf herleidbaar wie wanneer toegang had en welke gevoelige handelingen zijn uitgevoerd. Per gebeurtenis worden gebruiker, rol, tijdstip, IP-adres en de gebruikte app/browser vastgelegd, plus of de handeling slaagde.

In de beheeromgeving (Instellingen → Audit log) is een overzicht beschikbaar waarmee beheerders het audit-logboek kunnen doorzoeken, filterbaar op categorie, periode en gebruiker. Per gebeurtenis worden gebruiker, actie, doelobject, IP-adres en samenvattende details in kleurgecodeerde labels getoond; de volledige inhoud van elk event kan worden uitgeklapt.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

Wat wordt vastgelegd

Categorie	Vastgelegde gebeurtenissen
Aanmeldingen	Geslaagde en mislukte inlogpogingen — ook die via de mobiele app — met gebruiker, rol, tijdstip en IP-adres. Bij mislukte pogingen wordt ook de reden vastgelegd. Bij herhaalde mislukte pogingen treedt een automatische tijdelijke blokkade in werking (brute-force-bescherming), die als apart event wordt gelogd.

Categorie	Vastgelegde gebeurtenissen
Tweestapsverificatie (2FA)	Het instellen (enrollment), in- en uitschakelen van 2FA, geslaagde en mislukte 2FA-verificaties bij login, en het bedrijfsbreed verplicht stellen of opheffen van 2FA door een beheerder.
Wachtwoord-resets	Aanvragen tot wachtwoord-reset en de uitvoering ervan worden afzonderlijk gelogd.
Gebruikersbeheer	Het aanmaken, wijzigen, activeren, deactiveren en verwijderen van gebruikersaccounts.
Sessie-intrekking	Elke uitvoering van de 'Intrek alle sessies'-knop (zie sectie 6), inclusief welke gebruiker werd ingetrokken en hoeveel actieve sessies werden beëindigd.
Werkorders	Aanmaak, wijziging, verwijdering, doorsturen tussen afdelingen en het toewijzen of wisselen van monteurs.
Storingen en klantlogs	Aanmaak van storingen en klant-logregels door monteurs in het veld.
Toolboxen	Aanmaak en digitale ondertekening van toolboxen, inclusief de afdeling waarvoor de toolbox geldt.
Digitaal ondertekenen	De volledige ondertekenstroom van formulieren: link geopend, document bekeken, ondertekend, inclusief verificatie via een eenmalige SMS-code.

Audit-logregels worden één jaar bewaard en daarna automatisch opgeschoond via een nachtelijke achtergrondtaak — conform het AVG-principe van dataminimalisatie; de termijn kan op verzoek worden aangepast. Daarnaast is per gebruiker zichtbaar welk toestel is gekoppeld, het platform en het tijdstip van de laatste activiteit, zodat een beheerder een toestel zo nodig kan loskoppelen.

15. Externe diensten (sub-verwerkers)

Dienst	Rol
Strato AG	Hosting van server en database. Datacenter in Duitsland (EU).
Hetzner Online GmbH	Versleutelde off-site opslag van database-back-ups (Storage Box). Datacenter in Duitsland (EU).
Google Firebase	Pushmeldingen (Cloud Messaging) en crashdiagnose (Crashlytics). Verwerkt beperkte technische gegevens (toestel-/installatie-ID, diagnostische crashdata); deze kunnen buiten de EU worden verwerkt onder de EU-modelcontractbepalingen (SCC's).
TOPdesk	Optionele koppeling voor ticket-/meldingenuitwisseling, indien de organisatie dit gebruikt.
Strato (e-mail)	Verzending van systeem-e-mails (zoals meldingen) via beveiligde SMTP.

16. Privacy en AVG/GDPR

WOMsys verwerkt persoonsgegevens van gebruikers (zoals naam en inloggegevens) en werkgerelateerde gegevens. De verwerking is ingericht volgens de AVG.

- Er is een privacyverklaring beschikbaar op de canonieke URL womsys.nl/privacy.html (geldt voor zowel het webplatform als de monteurs-app).
- Bedrijfs- en persoonsgegevens van het platform worden uitsluitend binnen de EU opgeslagen (Strato en Hetzner, Duitsland). Voor pushmeldingen en crashdiagnose verwerkt Google (Firebase) beperkte technische gegevens, die mogelijk buiten de EU worden verwerkt onder de EU-modelcontractbepalingen (SCC's); zie sectie 15.

- Er kan een verwerkersovereenkomst worden afgesloten met de organisatie.
- Gebruikers hebben recht op inzage en verwijdering van hun gegevens; verzoeken worden via de beheerder verwerkt.

17. Samenvatting voor ICT

Kort samengevat is WOMsys ontworpen met databeperking en afscherming als uitgangspunt:

Punt	Toelichting
Versleuteld verkeer	Uitsluitend HTTPS/TLS; geen onversleutelde verbindingen.
Sterke authenticatie	Persoonlijke login, gehashte wachtwoorden (bcrypt), token van 24 uur, server-side intrekbare refresh-tokens, rolrechten, scheiding per bedrijf en optionele/bedrijfsbreed verplichte tweestapsverificatie (2FA).
Tweestapsverificatie (2FA)	Optioneel per gebruiker en bedrijfsbreed verplicht te stellen; TOTP via authenticator-app met eenmalige recovery codes. Beschikbaar op zowel de app als de webomgeving.
Sessie direct intrekbaar	Beheerder kan bij verlies of diefstal de sessie van de betrokken gebruiker binnen één seconde ongeldig maken — zonder te wachten op de 24-uurs-tokenexpiry.
Versleutelde tokenopslag	Toegangs- en refresh-tokens worden op het Android-toestel opgeslagen in de Android Keystore (hardware-ondersteund); in de browserversie in de standaard, sandboxed browseropslag.
Afgeschermde media	Geüploade foto's en pasjes zijn niet anoniem opvraagbaar; uitsluitend via per-bestand ondertekende, kortlevende URL's, gehandhaafd op beide domeinen.
Databeperking op toestel	Geen bedrijfsgegevens permanent op het toestel; alleen tokens in beveiligde opslag.
Minimale rechten	Alleen camera, locatie, notificaties en (optioneel) biometrie — elk met duidelijke werkreden.
EU-hosting	Server en database in een EU-datacenter (Duitsland), AVG-conform. Firebase (push/crash) verwerkt beperkte technische data onder SCC's (zie sectie 15/16).
Server-hardening	Firewall met uitsluitend noodzakelijke poorten, SSH alleen met sleutels, automatische blokkade van brute-force-pogingen, en interne diensten enkel lokaal bereikbaar.
Back-up & noodherstel	Dagelijkse, op integriteit gecontroleerde back-ups; versleutelde off-site kopie in een tweede EU-datacenter met retentie (7 dagelijks / 4 wekelijks / 6 maandelijks); herstel is getest en gedocumenteerd in een draaiboek.
Centraal audit-logboek	Logins (ook via de app), mislukte pogingen, 2FA-gebeurtenissen, gebruikersbeheer, sessie-intrekking, werkorder- en formulier-acties worden vastgelegd met wie/wanneer/IP. Filterbaar overzicht; één jaar bewaartermijn met automatische opschoning.
Beheerbaar	Uitrolbaar via Play Store, MDM/Managed Google Play of beveiligde directe installatie (ondertekend met vaste release-sleutel).
Webalternatief	Volledige functionaliteit ook via de browser, zonder installatie, voor strikt beheerde toestellen.

18. Contact

Voor aanvullende vragen, een verwerkersovereenkomst of een technische toelichting aan uw ICT-/securityteam zijn wij graag beschikbaar.

DC WebApps · Dennis Ceulemans
Van IJsendijkstraat 87, 1442 CJ Purmerend · KvK 99326922 · info@dcwebapps.nl · info@womsys.nl