

ICT-omgeving CVO Zuid-West Fryslân & technische specificaties



Leerlingenadministratiesysteem

Beschrijving ICT omgeving CVO Zuid West Fryslân

Inleiding

CVO beschikt over een centrale netwerkomgeving met een interne beheersorganisatie. De ICT afdeling streeft naar standaardisatie, uniformiteit, centralisatie en beheersbaarheid.

Het automatiseringsconcept op hoofdlijnen

CVO heeft de centrale ICT omgeving op de locatie De Diken. Er wordt gebruikt gemaakt van een hybride Active Directory/Azure omgeving. De meeste gebruikers maken gebruik van Windows 10.

Netwerk

De Diken is met eigen glasvezel verbonden met de locaties Hemdijk 2, Hemdijk 47 en Fultura. De locatie Balk, Koudum en Bolsward zijn met gehuurde glasvezel verbonden. Het netwerk heeft per gebouw minimaal 3 subnetten. Openbaar internet, Active Directory en beheer subnet. Het netwerk bestaat uit Aruba/HPE apparatuur, met Sophos firewalls. De toegang naar internet is in verband met de benodigde bandbreedte lokaal per locatie. Bij storing is deze om te leiden via de glasvezelverbindingen naar een andere locatie.

Gebruikersbeheer

Gebruikers zijn ouders, leerlingen, medewerkers en speciale accounts. Alle gebruikers, behalve de speciale accounts worden met geautomatiseerde processen aangemaakt en beheerd.

Gebruikers hebben allemaal een Active Directory account. Active Directory wordt gesynchroniseerd naar Azure. Azure/Office365 wordt onder andere gebruikt voor alle email, OneDrive, Teams en SharePoint en multifactor authenticatie.

De primaire authenticatie voor externe toepassingen zoals bijvoorbeeld

Zermelo, It's Learning, Magister en Profit is de interne ADFS, waarbij eventueel via Azure een MFA verzoek wordt gedaan.

Printen

Er wordt gebruik gemaakt van Konica Minolta printers die met SafeQ worden aangestuurd. Hiermee kan de gebruiker de printopdracht bij elke printer uitprinten. Er wordt gebruik gemaakt van één universele printerdriver.

Werkplek

Elke docent beschikt over een laptop. Leerlingen beschikken over een laptop of tablet.

Ondersteunend personeel maakt gebruik van een PC of laptop. Daarnaast zijn er een aantal computerlokalen en werkruimtes met computers voor leerlingen beschikbaar.

De werkplekken van medewerkers, en in de lokalen zijn voorzien van Windows 10. Wij streven erna altijd de meest recente Windows 10 versie te gebruiken. Er wordt voor opslag gebruik gemaakt van OneDrive, Teams, SharePoint en gedeelde servermappen. De werkplekken zijn voorzien van Office 2019.

Servers

CVO maakt gebruik van Hyper-V 2019 als virtualisatie platform. De servers zijn voornamelijk Windows 2019 en 2016. Active Directory en ADFS hebben versie 2016.

Koppelingen

Er worden vanuit verschillende systemen en met verschillende doelen koppelingen gelegd met het Leerlingenadministratiesysteem. Deze koppelingen staan hieronder globaal genoemd.

Koppelingen, im- en exports:

Naar	Soort koppeling	Richting
Rooster (Zermelo)	Dynamisch	↔
DUO	M2M	↔
RIO	M2M	↔
Facet	Export/Import	↔
CITO/VAS	Export/Import	↔
DIA toetsen	Export/Import	↔
Woots	Export/Import	↔
WOLF	Export/Import	↔
Educatieve uitgevers (digitaal lesmateriaal)	Entree federatie	→
OSO	Export/Import	↔
Mediatheek (Aura)	Export	→
Voorziening vroegtijdig aanmelden MBO VVA	M2M	↔
VSV Vroegtijdig School Verlaten	M2M	↔
Kwaliteitscholen	Ophalen gegevens	→
Wis Collect	Ophalen gegevens	→
Mastage (Maatschappelijke stage)	Ophalen gegevens	→
Tools4ever (UMRA)	Ophalen/schrijven gegevens	↔
HoyApp	Ophalen gegevens	→
JIJ-toetsen	Ophalen gegevens	→
Entree federatie Eck-id	M2M	↔
Leerlingbespreking.nl	Ophalen gegevens	→
TIG Qlik-view	Ophalen gegevens	→
Profit (AFAS)		↔
Office 365 INCL. Teams, Azure, sharepoint, enz.		↔
CJP	Export	→
Quayn		↔
Profijt	Import/Export	↔
Masterplan	Import/Export	↔

Uitleg systemen:

- Active Directory: Windows gebruikeraccounts en groepen van personeel en leerlingen.
- UMRA: Koppeling van Tools4ever om het gebruikeraccountbeheer te automatiseren.
- Afas Profit: CRM systeem voor HRM, personeel en financiële administratie
- Schoolmaster Magister: Leerlingen informatiesysteem
- MMP: Magister Management Portaal
- It's Learning: Electronische leeromgeving
- Office 365: Office applicaties van Microsoft in de cloud
- Kwaliteitscholen: Enquete tool
- RAP VO: HRM kennissysteem
- Portaal: School app voor communicatie met ouders, leerlingen en personeel
- Profit: Een alles in één ERP oplossing voor o.a. CRM, HRM & Payroll, Ordermanagement, Project- en urenadministratie en financiële administratie.
- DUO / BRON: Basisregister Onderwijs
- DUO personeels en lerarenregister: Aanleveren personeelsgegevens aan DUO
- ABP: Pensioenfonds voor overheid en onderwijs
- UWV: Uitvoeringsinstituut Werknemersverzekeringen
- OSO: Overstap Service Onderwijs
- Zermelo: Roosterpakket
- WIS Collect: innnen ouderbijdragen en overige schoolkosten.
- Noordhof: klassen synchroniseren i.v.m. lesmateriaal
- Abobe: Gebruikerssynchronisatie en login
- Entree federatie kennisnet: koppelvlak educatieve software
- Vensters: informatievoorziening richting ouders
- Leerlingbespreking: tool gebruikt door het Marne college om leerlingen op een andere wijze te bespreken.
- Teams: Online leer en werkomgeving (onderdeel Microsoft Office 365)

Technische specificaties Applicatie

- a. De Applicatie die Opdrachtnemer levert aan Opdrachtgever is een SaaS-Applicatie.
- b. Hosting geschiedt door de Opdrachtnemer.
- c. De Applicatie voldoet aan alle eisen die ingevolge wet- en regelgeving aan Applicaties van deze aard worden gesteld, nu en in de toekomst. Onder andere, maar niet uitsluitend, ten aanzien van privacy zoals de Wet Bescherming Persoonsgegevens, de Uitvoeringswet Algemene Verordening Gegevensbescherming
- d. Opdrachtnemer beschikt over een portaal waartoe alleen toegang kan worden verkregen door middel van gebruikersnaam en wachtwoord. Voor medewerkers van opdrachtgever geldt tevens een authenticatiecode.
- e. Als gevolg van SaaS worden bedrijfsprocessen uitbesteed aan de Opdrachtnemer. In dat kader beschikt Opdrachtnemer over TPM in de vorm van een ISAE 3402 verklaring type I en type II¹, afgegeven door een externe accountant. Van deze periodieke audit brengt de Opdrachtnemer verslag uit aan Opdrachtgever.
- f. Om de continuïteit van de Applicatie te kunnen garanderen heeft de Opdrachtnemer de broncode van de Applicatie, op basis van een actieve Escrow-Overeenkomst², in bewaring gegeven bij een onafhankelijke Escrow-agent. De Escrow-Overeenkomst wordt getekend door de Opdrachtnemer van de Applicatie, de Escrow-agent en Opdrachtgever. De Opdrachtnemer geeft bij de opdrachtgever aan in welke programmeertaal en versie van de programmeertaal de broncode is ontwikkeld is.
- g. De gegevenssynchronisatie met programma's³ die gekoppeld moeten kunnen worden aan de Applicatie vindt automatisch plaats.
- h. De Applicatie is tijd- en werkplekonafhankelijk te gebruiken vanaf elke gangbare device. De verschillende gebruikers hebben de mogelijkheid om vanuit elke werkplek (school- dan wel thuiswerkplek) en vanaf elke gangbare device de Applicatie te gebruiken.
- i. Aangezien scholen van Opdrachtgever met verschillende Operating Systemen en verschillende browsers werken, dient het gebruik van de Applicatie op gangbare browsers en besturingssystemen plaats te kunnen vinden.
- j. De Applicatie is gebruiksvriendelijk. Hieronder wordt onder andere verstaan:
 - de zichtbaarheid van de handelingen (bewerkingssignaal);
 - ondersteunende workflows;
 - foutmeldingen dienen eenduidig en helder gemeld te worden;
 - symboolweergave van activiteiten;
 - adequate Nederlandstalige helpfunctie bij elke menukeuze, uit te breiden door de gebruiker;

¹ De ISAE 3402 is een "internationale" standaard die toe ziet op zogenaamde Third Party Assurance rapportages. Met zo'n derdenverklaring wordt aangegeven dat een serviceorganisatie, waar een gebruikersorganisatie activiteiten aan heeft uitbesteed, 'in control' is.

² Escrow is een overeenkomst waarbij een software leverancier of distributeur en gebruiker overeenkomen dat de leverancier de broncode van een software product ten behoeve van de gebruiker deponeert bij een gespecialiseerd Escrow- agent.

³ In hoofdstuk 2 wordt een niet limitatieve opsomming van programma's genoemd.

- k. De Applicatie voert controles uit direct nadat mutaties zijn verricht en voordat deze verwerkt worden in de Applicatie dan wel worden uitgewisseld met andere, externe, Applicaties.

Beschikbaarheid, capaciteit en testomgeving

Ten aanzien van de beschikbaarheid van de Applicatie zorgt Opdrachtnemer voor het volgende.

- a. Het leerlingensysteem is 24 uur per dag, 7 dagen per week beschikbaar voor gebruik door Opdrachtgever. De Applicatie is tijd- en werkplekonafhankelijk te gebruiken. Gebruikers moeten zo de mogelijkheid hebben om niet alleen op hun werkplek maar ook vanuit hun werkplek thuis of waar dan ook de Applicatie te kunnen gebruiken. Regulier onderhoud (vervangen van hardware, plaatsen van nieuwe versies van de software) zal plaatsvinden in een service-window dat minimaal 24 uur voordien aangekondigd wordt. Dit service-window wordt gepland in de tijdsperiode 22.00 – 07.00 uur.
- b. De Applicatie kent een beschikbaarheidspercentage van minimaal 99,8%, waarbij de niet beschikbaarheid van maximaal 0,2% maximaal 4 uur bedraagt. Uitzondering hierop is het beschikbaarheidspercentage voor de rapportagedatabase en de portal voor de ouder en leerling: deze is 99,5%, waarbij de niet-beschikbaarheid van 0,5% maximaal 4 uur aaneengesloten is.
- c. 60% van alle gebruikers van Opdrachtgever met een actief account kunnen tegelijkertijd mutaties verrichten zonder negatieve gevolgen voor de performance van de Applicatie. Dit geldt natuurlijk ook voor de piekbelasting van het leerlingensysteem in de examenperiode (kritieke periode).
- d. Inschrijver stelt een separate testomgeving beschikbaar, die onafhankelijk van de productieomgeving draait en die minimaal maandelijks wordt ververst. Deze testomgeving is functioneel en operationeel dezelfde versie als de actuele omgeving waarbij de mogelijkheid bestaat, binnen 24 uur na het verzoek hiertoe, een kopie van de actuele productieomgeving in de testomgeving beschikbaar te hebben.

Performance

Ten aanzien van de performance van de Applicatie zorgt Opdrachtnemer voor het volgende.

- a. De responstijd van de applicatie bedraagt in 95% van de gevallen maximaal 2 seconden en voor de overige 5%, maximaal 5 seconden.
- b. Opdrachtnemer bewaakt de responstijden en rapporteert 1 x per kalenderjaar daarover aan Opdrachtgever zoals aangeboden in de offerte van Opdrachtnemer.

Toegankelijkheid en beveiliging

Ten aanzien van de toegankelijkheid en beveiliging van de Applicatie zorgt Opdrachtnemer voor het volgende.

- a. Het leerlingensysteem is via elke moderne browser toegankelijk en daardoor dienovereenkomstig beveiligd.
- b. De scherm-lay-out is binnen alle browsers gelijk.
- c. De gebruiker heeft toegang tot de Applicatie via het internet en hoeft op geen enkele wijze specifieke software te installeren.
- d. Toegang tot de Applicatie is in ieder geval mogelijk via het authenticatieportaal (ADFS) van Opdrachtnemer waarbij de gebruiker zich éénmaal identificeert door middel van een eigen gebruikersnaam, wachtwoord en extra authenticatie (one time password via sms of soft-/hardware token), waarna de gebruiker zonder afzonderlijke inlogprocedure toegang krijgt tot de Applicatie.
- e. Ingeval van een klacht of indien de authenticatieportaal van Opdrachtnemer niet toegankelijk is, waardoor geen toegang tot de Applicatie mogelijk is, biedt Opdrachtnemer de gebruikers van Opdrachtgever een noodplan.
- f. Bij de werking van het noodplan is het aantal keren dat foutief ingelogd kan worden beperkt tot maximaal 3 keer. Bij overschrijding hiervan wordt het betreffende account geblokkeerd. Een hiertoe bevoegde functionaris dient daarbij direct te worden geïnformeerd en kan het account weer open zetten volgens een vastgelegde procedure.
- g. Elke poging (geslaagd of niet geslaagd) tot inloggen dient gelogd te worden. Dit logbestand heeft een voldoende lange bewaartermijn (6 maanden tot een jaar) om te kunnen analyseren.
- h. De gegevens zijn via een browser toegankelijk en dienen daarom ook dienovereenkomstig beveiligd te zijn (inter- en intranet). Versleuteling van data zal plaatsvinden op basis van minimaal TLS 1.2 encryptie.
- i. Voor toegang tot bepaalde functionaliteiten via een App wordt authenticatie op een gepaste en veilige manier conform wet- en regelgeving gerealiseerd.
- j. De online toegang tot de servers is afgeschermd voor een digitale aanval (bijvoorbeeld DDOS) van kwaadwillenden.
- k. Gebruikers worden geautoriseerd op persoonsniveau door daartoe bevoegde functionarissen van Opdrachtgever. Gebruikers worden aangemaakt met bijbehorende autorisatie voor schermen, rapporten enzovoort met een onderscheid tussen lezen, aanmaken/wijzigen en verwijderen. Daarnaast moet deze autorisatie onderscheid kunnen maken op persoonsniveau (dus bijvoorbeeld alleen de leerlingen waar iemand docent van is).
- l. De Applicatie voert routinecontroles uit op autorisaties en fraudegevoelige aspecten, zoals bijvoorbeeld, maar niet uitsluitend, het invoeren van bankrekeningnummers.
- m. Autorisatie van gebruikers en gebruikersgroepen in de Applicatie is mogelijk op veldniveau. Daarbij heeft Opdrachtgever op stichtingsniveau, schoolniveau en op afdelingsniveau de mogelijkheid voor elke gebruikersrol separate autorisaties toe te kennen, waarbij een gebruiker meerdere gebruikersrollen kan hebben.
- n. Wijzigingen in autorisaties worden gelogd. Hierbij is zichtbaar wie wanneer welke mutatie heeft uitgevoerd.
- o. Er is op eenvoudige wijze een rapportage per gebruiker samen te stellen waaruit blijkt welke autorisaties aan de betreffende gebruiker zijn verstrekt. Middels deze rapportage is eenvoudig te achterhalen welke rechten zijn verstrekt en op welke basis (individueel of groepsrecht en via welk groepsrecht).

Gegevensopslag en -verwerking

- a. Opdrachtgever is en blijft te allen tijde eigenaar van de data in de Applicatie.
- b. Bij calamiteiten garandeert Opdrachtnemer ongestoorde voortgang van het gebruik van de Applicatie.
- c. De Applicatie werkt met behulp van een logische database met een eenduidige structuur waarbij gegevens niet dubbel mogen worden opgeslagen (normaliseren).
- d. Alle functionaliteiten/modules maken gebruik van dezelfde gegevensbron. Ook alle scholen maken daarbij gebruik van dezelfde gegevensbron. Dit impliceert niet noodzakelijk dat deze gegevens ook fysiek op één Locatie staan, maar het geheel aan gegevens dient integraal te kunnen worden benaderd en beheerd.
- e. De database(s) is (zijn) centraal, per school en op afstand te beheren. Uitgangspunt voor de Applicatie is de individuele leerling, waarbij het binnen de Applicatie mogelijk is leerlingen te onderscheiden naar klas, lesgroep, afdeling, locatie en school.
- f. Naast de standaard databasestructuur en -vulling kan Opdrachtgever een database naar wens laten uitbreiden. Deze uitbreidingen kunnen een plaats krijgen in eigen schermen, rapporten en procedures en functioneren integraal met de standaard gegevensverzameling.
- g. Gebruikers en gebruikersgroepen kunnen naar wens worden aangemaakt met bijbehorende autorisaties voor schermen, rapporten, gegevens raadplegen, wijzigen en verwijderen/toevoegen.
- h. De database kan worden geschoond door de Opdrachtgever om daarmee te voldoen aan AVG.
- p. Bij mutaties in de Applicatie worden oude gegevens op basis van mutatielogging bewaard. Nieuwe gegevens worden toegevoegd door een nieuw record met de nieuwe gegevens en daarbij het tijdstip van wijziging en de identiteit van de gebruiker die de wijziging heeft doorgevoerd.
- q. Bij persoonsgegevens, cijfers/examen is een raadpleegbare volledige mutatielogger.
- r. Indien cijfers/examens in de Applicatie worden gemuteerd krijgt de betreffende docent daar een melding van via beveiligde e-mail.
- s. Opdrachtgever bepaalt op stichtingsniveau welke invoervelden verplichte velden zijn. Het datamodel heeft de individuele leerling als uitgangspunt, maar gegevens zijn wel via diverse manieren op te vragen en in te voeren, individueel, per klas, per profiel, per studie, per afdeling, per school.
- t. De database(s) en server dienen van die kwaliteit en capaciteit te zijn, dat gebruikers, rapportages en portalen hier makkelijk gezamenlijk in kunnen werken.
- u. Na gunning wordt er tussen opdrachtgever en opdrachtnemer een verwerkersovereenkomst gesloten. Inschrijver voegt aan zijn inschrijving een concept verwerkersovereenkomst toe. Deze concept versie wordt na gunning tussen opdrachtgever en opdrachtnemer besproken en waar nodig aangepast om tot de definitieve versie te komen.

Back up en restore

- a. De backup-voorziening(en) staan in een brandwerende backuplocatie, welke zich geografisch gespreid bevindt ten opzichte van de serverlocatie.
- b. Dagelijks wordt tussen 00.00 en 06.00 uur een full-backup van de data gemaakt. Deze full-backup wordt weggeschreven naar de backuplocatie.
- c. Opdrachtnemer treft maatregelen om bij uitval zo snel mogelijk adequate vervangende apparatuur te hebben.
- d. Elke twee uur wordt een incremental backup gemaakt, welke wordt weggeschreven naar de backuplocatie.
- e. Dagelijkse backup-bestanden worden 2 maanden bewaard. Ultimo maand backup-bestanden worden gedurende 1 jaar bewaard. Ultimo jaar backup-bestanden worden gedurende 3 jaar bewaard.
- f. Opdrachtnemer beschrijft, in overleg met de opdrachtgever, een duidelijke restore-procedure. Deze procedure wordt bekend gemaakt bij de verantwoordelijke personen bij de opdrachtgever.

Fysieke beveiliging serverruimte

Ten aanzien van de fysieke beveiliging van de serverruimte van de Applicatie voldoet Opdrachtnemer aan ISO27001 en ISO27002.

Klachten

- a. Bij een klacht in de Applicatie spant de Opdrachtnemer zich maximaal in deze klacht zo spoedig mogelijk op te lossen op de op dat moment meest geëigende wijze.
- b. Opdrachtnemer heeft een centraal meldpunt bij Opdrachtnemer voor klachten. Dit meldpunt is voor Opdrachtgever zowel via een website als ook telefonisch bereikbaar.
- c. Opdrachtnemer heeft een meldpunt voor klachten dat via telefoon en via website bereikbaar is. De medewerkers die daartoe geautoriseerd zijn door Opdrachtgever kunnen 24 uur per dag, 7 dagen per week klachten melden bij dit meldpunt.
- d. Klachten worden binnen 1 uur na melding via de website bevestigd door Opdrachtnemer. Hierbij wordt door Opdrachtnemer een indicatie vermeld, wanneer de klacht opgelost zal zijn. Opdrachtnemer meldt richting Opdrachtgever wanneer de klacht door Opdrachtnemer is opgelost. Indien de vermelde indicatietijd niet gerealiseerd wordt door Opdrachtnemer, wordt Opdrachtgever door Opdrachtnemer geïnformeerd over het nieuwe tijdstip. Elke klachtmelding wordt door Opdrachtnemer pas afgesloten nadat Opdrachtgever bevestigd heeft dat de betreffende klacht naar tevredenheid opgelost is.
- e. Opdrachtnemer zorgt er voor dat alle klachtmeldingen van de scholen van Opdrachtgever via de website voor de medewerkers van alle scholen van Opdrachtgever inzichtelijk zijn onder vermelding van

- de status van de betreffende klacht
 - tijdstip van klachtmelding
 - naam van de medewerker die de klacht heeft gemeld
 - aard van de klacht
 - het verwachte moment dat klacht is opgelost door Opdrachtnemer
 - welke persoon bij Opdrachtnemer de klacht in behandeling heeft met contactgegevens
- f. Klachten zijn in de volgende 2 niveaus ingedeeld:
1. Kritiek: ten gevolge van de klacht kan de Applicatie (of een deel daarvan) niet meer worden gebruikt.
 2. Urgent: ten gevolge van de klacht treedt een hinderlijke situatie op in het gebruik van de Applicatie.
- g. Klachten die door Opdrachtgever als kritiek worden aangemerkt, worden door Opdrachtnemer binnen 4 uur na de betreffende klachtmelding en tijdens kritieke perioden binnen 2 uur na de betreffende melding, zodanig opgelost dat Opdrachtgever Applicatie in voldoende mate kan gebruiken. Binnen 24 uur is klacht definitief opgelost door Opdrachtnemer.
- h. Klachten die door Opdrachtgever als urgent worden aangemerkt, worden tijdens werkdagen van 08.00 – 19.00 uur, binnen 6 uur na de betreffende melding en tijdens kritieke perioden op werkdagen en in het weekend van 08.00 – 17.00 uur, binnen 4 uur na de betreffende melding, zodanig opgelost door Opdrachtnemer dat Opdrachtgever Applicatie in voldoende mate kan gebruiken. Binnen 48 uur is de klacht definitief opgelost door Opdrachtnemer.
- i. Zodra Opdrachtnemer constateert dat de herstelmomenten onder de punten g en h niet gerealiseerd kunnen worden dient een escalatieprocedure in werking te treden. Deze escalatieprocedure wordt als bijlage toegevoegd aan de SLA.

Helpdesk

- a. Naast het meldpunt voor klachten heeft Opdrachtnemer ook een helpdesk voor het stellen van vragen over het gebruik van de Applicatie door de Applicatiebeheerder (gemiddeld 1 Applicatiebeheerder per school) van de school van Opdrachtgever.
- b. De medewerkers van de helpdesk van Opdrachtnemer zijn telefonisch bereikbaar op maandag tot en met vrijdag van 08.00 uur tot 17.00 uur.
- c. Wachtijden aan de telefoon van de helpdesk bedragen maximaal 1 minuut. Voor de telefoonkosten worden alleen standaardkosten gerekend en geen extra kosten voor betaallijnen.
- d. Van alle vragen die door Opdrachtgever worden gesteld aan de helpdesk van Opdrachtnemer wordt 80% direct door de helpdesk adequaat beantwoord.
- e. Ten aanzien van alle vragen en wijzigingsverzoeken van Opdrachtgever vindt binnen 24 uur een terugkoppeling plaats door de helpdesk naar de vragensteller van Opdrachtgever. Indien de vraag / wijzigingsverzoek niet binnen deze periode is opgelost dan wordt aangegeven wanneer de oplossing wordt opgeleverd.
- f. Opdrachtnemer biedt realtime informatie aan Opdrachtgever betreffende bugs en andere knelpunten in de Applicatie.