Inpasbaarheid informatiesystemen - techniek Gemeente Vlissingen, gemeente Middelburg en Orionis Walcheren.

Versie V07, mei 2026

Inhoud

Algemeen. 2

Dwingend werkplekconcept. 2

Clients. 3

Office. 3

Kenmerken infrastructuur. 3

Servers. 3

Server applicaties. 4

Databases. 4

Backup. 4

Netwerk en beveiliging. 4

Internet en koppelingen. 5

Openbare Websites. 5

Remote support. 5

Overig. 5

Algemeen.

De ICT-ondersteuning van de gemeenten Middelburg en Vlissingen en van Orionis Walcheren wordt verzorgd door de I&A Samenwerking Middelburg-Vlissingen. Dit heeft o.a. geleid tot een uniform werkplekconcept en een gemeenschappelijke ICT-infrastructuur.

Bij het aanschaffen of vervangen van een informatiesysteem/applicatie zijn vanuit de techniek twee zaken van belang:

- Inpasbaarheid in ons werkplekconcept;
- Aansluiting (waar nodig) op onze ICT-infrastructuur;

Om eventuele knelpunten in een zo vroeg mogelijk stadium te onderkennen geeft dit document een aantal karakteristieken weer. Aan de hand hiervan kan een leverancier van software en hardware een eerste inschatting maken van de inpasbaarheid van zijn software of diensten. Daarbij is het belangrijk om te realiseren dat bij incompatibiliteit het werkplekconcept of de infrastructuur niet zal worden aangepast aan de software c.q. applicatie van de leverancier.

Concreet betekent dit dat functionaliteit in de software of diensten die afhankelijk is van niet door ons werkplekconcept of onze infrastructuur ondersteunde technieken of componenten niet gerealiseerd kan worden c.q. beschikbaar zal zijn na implementatie. Als zich dit bij uw product voor kan doen, dan dient u dat als leverancier bij een inschrijving of andere aanbieding vooraf aan te geven.

De informatie in dit document zal niet altijd voldoende zijn om met zekerheid te kunnen vaststellen in hoeverre er sprake is van incompatibiliteit. Het is de verantwoordelijkheid van de leverancier om bij twijfel op dit punt dit voorafgaand aan een aanbieding kenbaar te maken.

Dwingend werkplekconcept.

De gemeenten Middelburg en Vlissingen zitten in de overgangsfase naar een nieuw werkplekconcept. Dit concept gaat uit van mobiele en vaste werkstation op basis van Windows 11 Enterprise in combinatie met Microsoft 365. Toegang tot overige (vak)applicaties wordt op een universele manier geboden via een webbrowser[1] middels HTML5, zonder applicatie specifieke webbrowser plug-ins.

Het concept streeft een situatie na waarin een werkstation met een "kale" webbrowser voor een medewerker voldoende is om volledig gebruik te kunnen maken van alle voor het werk benodigde informatie- en communicatiesystemen.

Dit betekent o.a. dat:

- Alle nieuw aan te schaffen c.q. te vervangen applicaties volledig webbased moeten zijn, dus volledig moeten kunnen functioneren op basis van enkel de webbrowser, zonder aanvullende lokale software of plug-ins, op de werkstations;
- Applicaties die afwijken van bovenstaande kenmerken (bijvoorbeeld gebruik maken van Java, RDP, VDI of andere "remote" of SBC technieken) niet meer in gebruik zullen worden genomen, ongeacht waar deze gehost zijn;
- Hosting van applicatie die aan genoemde eisen voldoen zowel in onze eigen infrastructuur (onder beheer van de I&A Samenwerking) als in een door de leverancier verzorgde infrastructuur acceptabel is;
- "Office" functionaliteit van applicaties gebaseerd is en blijft op Microsoft 365.

[1] laatste of 1-na laatste versie Edge (met Chromium Open Source als basis)

Clients.

Het nieuwe werkplekconcept is gebaseerd op Managed Windows 11 Enterprise laptops en gaat uit van via een webbrowser aangeboden (HTML5) applicaties, zonder applicatie specifieke webbrowser plug-ins. Slechts bij onvermijdelijke uitzondering kan na overleg en akkoord, met en van de adviseur Automatisering van I&A, software op de laptop worden geïnstalleerd.

Applicaties worden in dat geval niet rechtstreeks geïnstalleerd, maar na installatie op een centrale package omgeving (Application Workspace) gedistribueerd naar de laptops of mobile workstations (applicaties voor grafische vormgeving). Applicaties via Application Workspace packages (MSI) worden toegekend op groepsniveau zonder losse plugins of runonce. Voor het goedkeuren (allowlisting) van applicaties wordt gebruik gemaakt van Windows Defender Application Control (WDAC). WDAC wordt toegepast op apparaat niveau. Bij geen enkel werkstation bestaat de mogelijkheid om via USB storage te benaderen. Gebruikers hebben geen administrator rechten op werkstations.

Alle clients (zowel Windows als iOS) worden beheerd met behulp van MDM via Intune. Hierbij wordt gebruik gemaakt van Microsoft hardening policies en Microsoft Defender for Endpoint. Persoonlijke gebruikershardware wordt niet ondersteund. Conditional Access policies zijn actief en 2 factor authenticatie wordt afgedwongen. Authenticatie op de Windows apparaten gebeurt met Windows Hello for Business.

Office.

Standaard software Microsoft 365, waarbij voor Unified Communications gebruik wordt gemaakt van Microsoft Teams calling (Vodafone Calling in Office365) en voor bepaalde groepen Anywhere365 als add-on.

Kenmerken infrastructuur.

De gemeenten Middelburg en Vlissingen hebben de ICT-infrastructuur gezamenlijk vormgegeven. Ook Orionis Walcheren maakt gebruik van deze infrastructuur. Deze gezamenlijke ICT-infrastructuur wordt beheerd door de I&A Samenwerking.

Voor die gevallen waarbij er voor het inzetten van een extern gehoste applicatie interactie met de gemeentelijke ICT-infrastructuur nodig is (bijvoorbeeld een BRP- of datawarehouse-/BI-koppeling), of waarbij het de bedoeling is dat de applicatie in de gemeentelijke ICT-infrastructuur wordt gehost, worden hier de meest basale kenmerken van die infrastructuur beschreven.

Servers.

OS en virtualisatie

Voor lokaal te hosten webapplicaties en de daarbij horende databases worden applicatie- en databaseservers ingezet. Deze zijn non-dedicated, dus meerdere webapplicaties (of databases) delen een server. Webapplicatie- en databaseservers hebben als operating systeem:

- Windows 2022 of 2025 x64
- Ubuntu 24.x of 26.x

Alle back-end servers zijn gevirtualiseerd via VMWare vSphere 8.0.3.

De servers worden elke maand voorzien van (Windows en Ubuntu) Updates. Na installatie mogen er geen handmatige acties nodig zijn om de software goed te laten functioneren.

Lokale software en daarbij horende services mogen nooit draaien met administrator rechten.

Mail Server

Wij vereisen niet alleen mailstandaarden op externe mailservers, maar staan ook geen whitelisting toe van externe accounts.

Server applicaties.

Het algemene uitgangspunt is dat geïnstalleerde software up-to-date hoort te zijn, ten tijde van installatie en dat ook hoort te blijven.

Databases.

Op de database servers worden databases gehost van verschillende applicaties/leveranciers. Het is dus niet mogelijk om resources exclusief te reserveren voor een bepaalde database.

Ondersteunde databases zijn:

- SQL Enterprise 2025
- Oracle 19 Enterpise Edition (op basis van Melodies)

Backup.

Backup vindt plaats via CommVault, voor zowel de on-premise als de Microsoft 365 omgeving.

Netwerk en beveiliging.

Datacommunicatie van binnen naar buiten (naar buiten het gemeentelijk netwerk) loopt altijd via onze authenticated firewall.

Datacommunicatie van buiten naar binnen loopt altijd via onze reverse proxy en of firewall. Servers mogen niet naar buiten communiceren, in uiterste gevallen alleen naar een bekende en passend beveiligde destination. De te ontsluiten websites mogen geen gebruik maken van Websockets.

Applicatieservers (w.o. databaseservers) zitten in verschillende netwerksegmenten. Datacommunicatie tussen deze servers wordt gecontroleerd en beperkt door een firewall.

Het netwerk is volgens het dual stack principe ingericht en tegelijk actief op applicatieniveau. Door zowel IPv4- als IPv6-protocollen te ondersteunen bieden we flexibiliteit en interoperabiliteit en waardoor een soepele overgang mogelijk is van IPv4 naar IPv6.

Het netwerk kent meerdere zoneringen:

- Backendservers
- Reverse proxy
- DMZ
- Site-to-site VPN (via onze Firewalls)
- WAN
- Client vlans (distributienetwerken / SBC / VDI)

Daarnaast zijn de volgende overige kenmerken van toepassing:

- Proxy / firewall / wifi / switching / DPI / security profiles
- Intern Firewall cluster (NGFW)
- Extern firewall cluster (NGFW zoals webfiltering / DPI / IPS/IDS / authenticatie op groepsniveau / proxy functionaliteit / AV)
- Maken gebruik van een 3tier netwerk
- Web Application Firewalling / allowlist / denylist
- MAC authenticatie / 802.1x (certificaat preferred). Device certificaat via I&A voor authenticatie op gemeentelijke infrastructuur.
- Internet / Site-to-site VPN / Diginetwerk
- Direct acteren op NCSC/ IBD / leveranciers high/high incidenten en ingericht kwetsbaarheden management. Leverancier voert periodiek audits uit en overlegt rapportages.

Internet en koppelingen.

Toegang tot public Cloud services zoals WeTransfer, DropBox, iCloud, etc. vanuit het netwerk is niet toegestaan. De gemeenten maken gebruik van Microsoft Onedrive.

Bij dataverbindingen tussen het gemeentelijk netwerk en externe landelijke voorzieningen wordt gebruik gemaakt van het besloten Diginetwerk (Logius). Bij koppelingen tussen on-premise applicaties en die van leveranciers wordt er altijd gebruik gemaakt van OpenTunnel als Enterprise ServiceBus, waarbij voor gegevens uit de BRP OpenTunnel wordt aangesloten op onze databroker key2DDS van Centric.

Protocollen en certificaten

- Alleen het protocol TLS 1.3 wordt gebruikt. HTTP-koppelingen zijn altijd op basis van certificaten, dus HTTPS.
- Voor de beveiliging van koppelingen gebruiken wij PKI-overheidscertificaten.

Openbare Websites.

Onafhankelijk van de hosting-variant moeten openbare websites toegankelijk zijn voor de archiveringssoftware van onze archiefdiensten, veelal gebaseerd op webcrawlers en andere geautomatiseerde onderzoeks- en inventarisatieprocessen. Voor het ontsluiten van websites worden zowel intern als in de cloud de richtlijnen van het NCSC gevolgd. Daarvoor benodigde informatie wordt door de leverancier aangeleverd.

De leverancier is verantwoordelijk voor het aanvragen en vervangen van website certificaten. Advies is om gebruik te maken van het ACME protocol.

Remote support.

24*7 remote toegang tot systemen, bijvoorbeeld via een VPN is niet toegestaan.
Installaties, updates, tests, configuraties, troubleshooting etc. van lokale installaties worden waar mogelijk on-site uitgevoerd. Alle acties tijdens deze activiteiten worden automatisch gelogd. In geval van calamiteiten kan voor troubleshooting gebruik worden gemaakt van Remote Access.

RDP/ beheer via webinterface / Steppingstone

- Functioneel beheer via webinterfaces
- Functioneel beheer via Stepping Stone Server
- Applicatie updates op aanvraag via TeamViewer

Overig.

- Standaard schermresolutie is 1920 x 1080 of 1920 x 1200.
- Single Sign On wordt ondersteund op basis van SAML-authenticatie via Entra ID.
- Niet-versleutelde authenticatiestrings zijn, ook binnen het netwerk, niet toegestaan.