

# Karakterisering ICT-infrastructuur Gemeenten Vlissingen en Middelburg.

Versie V17, 9 oktober 2020.

## Algemeen.

De gemeenten Middelburg en Vlissingen hebben de ICT-infrastructuur gezamenlijk vormgegeven. Kernbegrippen daarbij zijn: gezamenlijk gebruik van ICT-componenten, virtual servers, serverbased computing, interne hosting, non-dedicated servers, een vergaand beveiligd, gesegmenteerd netwerk en een gecentraliseerd technisch beheer. De gezamenlijke ICT-infrastructuur wordt beheerd door de I&A Samenwerking Middelburg en Vlissingen. On-premise installatie van informatiesystemen (ook websites) heeft de voorkeur en zowel infrastructuur als beheerorganisatie zijn daar op ingericht.

Het blijkt niet vanzelfsprekend te zijn dat software in de ICT-infrastructuur van Middelburg en Vlissingen (volledig) kan functioneren. Ook is niet elk licentiemodel technisch of financieel/juridisch even goed inpasbaar op de 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 een eerste inschatting maken van de geschiktheid van zijn software voor deze omgeving. Daarbij is het belangrijk om te realiseren dat bij incompatibiliteit de infrastructuur in principe niet zal worden aangepast aan de software.

De eerste indruk zal in bepaalde gevallen niet voldoende zijn om met zekerheid te kunnen vaststellen of software wel of niet in de ICT-infrastructuur volledig zal kunnen functioneren. Vaak zal gedegen overleg op technisch niveau, of zelfs een testinstallatie (pilot), nodig zijn om deze zekerheid te verkrijgen. Indien een situatie daar om vraagt, zal dit nadere onderzoek deel uitmaken van een marktverkenning of selectieprocedure.

De ICT-infrastructuur is continu aan veranderingen onderhevig. Principes zullen langzaam en weinig veranderen, maar gebruikte technieken en - vooral - versies zullen regelmatig veranderen. Volgens de GIBIT wordt van leveranciers verwacht dat zij zich, voordat er aanbiedingen worden gedaan, voldoende op de hoogte hebben gesteld van de ICT-omgeving (inclusief applicatielandschap) van de gemeente om te zorgen dat de aanbieder (zonder meerkosten) geschikt is om in die omgeving naar behoren te functioneren. Dit document is bedoeld om leveranciers een eerste indruk te geven van de karakterisering en is per definitie niet voldoende volledig en actueel om een beroep op te doen vanuit deze z.g. analyseplicht zoals in de GIBIT opgenomen.

## Servers.

Een farm van ca. 60 (virtuele) terminalservers voorzien van Citrix XenApp 7 1909 worden geboort vanaf dezelfde virtuele bootdisk, de z.g. Golden Image, met behulp van Citrix PVS. Alle terminalservers zijn dus identiek wat betreft instellingen en software. Het gebruikte operating system is Windows Server 2016 en de applicaties worden gestart vanaf de golden disk en geladen in het RAM geheugen van een terminalserver. Ca. 1200 werkplekken, uitgerust met thin clients, en een flink aantal remote/mobile werkplekken worden via loadbalancing verbonden met een willekeurige terminalserver in de farm waarop met behulp van een token en wachtwoord kan worden ingelogd.

Front- en backend van applicaties (2- en 3-tier, webenabled etc.) worden zo veel mogelijk op verschillende servers gehost. De terminalservers zullen in elk geval het frontend verzorgen, voor de rest worden applicatie- en databaseservers ingezet. Ook deze laatste zijn non-dedicated, dus meerdere applicaties (of databases) delen een server. Applicatie- en databaseservers hebben Windows 2016 of 2019 x64 als operating system. De servers worden elke maand voorzien van Windows Updates. Na installatie mogen er geen handmatige acties nodig zijn om de software goed te laten functioneren.

Alle back-end servers zijn gevirtualiseerd via VMWare vSphere 6.7. De Citrix Xenapp servers zijn gevirtualiseerd via XenServer.

Software (inclusief services) mag nooit draaien met administrator rechten.

## Databases.

Ondersteunde databases zijn voornamelijk SQLServer Standard Edition 2012 (overgang naar 2017 is gestart), SQL Enterprise 2017 en (vanaf 1-1-2021) Oracle 19 Enterprise Edition.

Omdat Oracle 11 en 12 niet meer ondersteund worden per 1-1-2021 is het van belang om voor implementaties die nog in 2020 moeten plaatsvinden samen met I&A Samenwerking te kijken welke Oracle-versie geïnstalleerd gaat worden.

Zoals gezegd delen verschillende databases, van verschillende applicaties/leveranciers, de resources van de (non-dedicated) databaseservers. Het is dus niet mogelijk om resources exclusief te reserveren voor een bepaalde database.

## Clients.

Het merendeel van de gebruikers logt middels thin clients in op de terminalservers.

Slechts bij onvermijdelijke uitzondering worden fat clients (PC's) ingezet als workstation. Deze workstations zijn voorzien van Windows 7 x64 (uiterlijk per 1 januari 2021 is dit Windows 10). Software die per se op deze workstations moet draaien wordt niet rechtstreeks geïnstalleerd, maar na installatie op een centrale package omgeving via RES Automation Manager als package gedistribueerd naar de workstations.

Medio 2020 zal ook VDI ingezet gaan worden en zullen de fat clients hier naartoe migreren. Alle VDI workstations worden geboot vanaf dezelfde bootdisk, de z.g. Golden Image, met behulp van Citrix PVS. Alle VDI workstations zijn dus identiek wat betreft instellingen en software.

De software mag nooit draaien met admin-rechten.

Met behulp van RES VDX worden de lokale (op de fat client draaiende) en de centrale (op de terminalservers draaiende) omgeving geïntegreerd waarbij het onderscheid in omgevingen voor de gebruiker verdwijnt. In feite wordt de lokale software vanuit de Citrix sessie op de terminalserver, gestart op de lokale PC.

Bij geen enkel workstation (thin of fat) bestaat de mogelijkheid om via USB, Bluetooth, WiFi etc. verbindingen te maken met andere devices of netwerken.

Gebruikers hebben geen administrator rechten op workstations, servers etc.

## Netwerkbeveiliging.

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

Datacommunicatie van buiten naar binnen loopt altijd via onze reverse proxy en of firewall. Servers mogen niet zomaar naar buiten communiceren, in uiterste gevallen alleen naar een bekende en passend beveiligde destination.

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

Alle gebruikers delen een 500 mb/s up en down internetverbinding voor alle internetverkeer. Toegang tot public Cloud services zoals DropBox, iCloud, OneDrive etc. vanuit het netwerk is niet toegestaan. De gemeenten maken gebruik van een eigen corporate cloud o.b.v. Nextcloud.

Bij dataverbindingen naar externe partijen zoals landelijke voorzieningen en leveranciers wordt er altijd gebruik gemaakt van OpenTunnel als Enterprise ServiceBus. Aansluitingen op MijnOverheid worden ook via OpenTunnel gerealiseerd. Alleen de protocollen TLS 1.2 en 1.3 worden gebruikt.

## Websites

Vanuit de eigen infrastructuur wordt een aantal extern bereikbare (openbare) websites gehost. Hiertoe zijn in de infrastructuur voor bepaalde typen websites (vertrouwelijkheid, performance, gebruikte technieken, ...) speciale voorzieningen getroffen. Aan de ene kant betekent dit dat bepaalde websites on-premise gehost kunnen worden (voorkeur), aan de andere kant kan het zijn dat bepaalde websites niet in deze infrastructuur passen.

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 de richtlijnen van het NCSC gevolgd. Daarvoor benodigde informatie wordt door de leverancier aangeleverd.

## Software.

Standaard software is MS Office 2013 23 (met outlook/Exchange), laatste of 1-na laatste versie FireFox, laatste of 1-na laatste versie Edge (met Chromium Open Source als basis).

Voor Unified Communications wordt gebruik gemaakt van Skype.

Standaard schermresolutie is 1920 x 1080 of 1920 x 1200.

Single Sign On wordt ondersteund op basis van ldap, Kerberos en ADFS.

Niet-versleutelde authenticatiestings zijn - ook binnen het netwerk - niet toegestaan.

## Remote support.

24\*7 remote toegang tot systemen, bijvoorbeeld via een VPN is niet toegestaan.

Installaties, updates, tests, configuraties, troubleshooting etc. 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.

~~~~~