ICT
Aansluitvoorwaarden

Hoogheemraadschap van Delfland

Concept

Versiehistorie

Basisgegevens

	Rol	Naam	Datum
Opgesteld	ICT Architect	Paul van Veen	Februari - 2024
Vastgesteld	CIO	Arwin de Beer	

Versiebeheer

Versie	**Datum**	**Auteur**	**Wijzigingen**
D1.0	Oktober 2023	Ashil Alemyar	Definitief
C1.1	Januari 2024	Paul van Veen	Upgrade
C1.2	Februari 2024	Paul van Veen	Review ICT-coördinator, Security Coördinator en Security Officer verwerkt
C1.3	Maart 2024	Paul van Veen	Review iAdvies verwerkt.
C1.4	Maart 2024	Paul van Veen	Tekst aanpassing
C1.5	13-03-2024	Paul van Veen	Opmerking iAdvies verwerkt

Toelichting versienummers:
C0.x = concept
D1.0 = Definitief

Vaststelling en periodieke validatie

Vastgestelde versie	**Datum vaststelling**	**Wie**	**Functie**
D1.0	30-10-2023	Arwin de Beer	CIO
D2.0		Arwin de Beer	CIO
Volgende validatie			
Classificatie	Intern		

Inhoud

1 Inleiding

1.1 Achtergrond

Informatievoorziening bestaande uit ICT, IFM en DMA, levert middelen en diensten ten behoeve van afdelingen/teams binnen het Hoogheemraadschap van Delfland en haar samenwerkingsverbanden.

Om de kwaliteit, continuïteit en de veiligheid van de ICT-voorzieningen te waarborgen zijn voorwaarden opgesteld die gelden voor ICT-middelen welke aansluiten worden op de infrastructuur van het Hoogheemraadschap van Delfland (HHD).

1.2 Doel

Dit document geeft richtlijnen voor aansluiting aan de infrastructuur en beschrijven de spelregels welke de kwaliteit, continuïteit (beschikbaarheid) en veiligheid van de infrastructuur waarborgen.

1.3 Scope

De ICT-infrastructuur bestaat uit hardware, operating-systeem software, netwerkvoorzieningen, kantoor- en proces automatisering software en dataopslag. De grafische (GIS) werkplek heeft een speciaal karakter en is buiten scope van dit document.

1.4 Eigenaarschap

Het eigenaarschap van dit document is belegd bij de afdelingsmanager van de afdeling ICT van het Hoogheemraadschap van Delfland.

1.5 Melding afwijkingsprocedure

Uitzonderingen op de in dit stuk gestelde voorwaarden kunnen via een formulier en gemotiveerd verzoek vooraf worden aangevraagd. De architectuur board zal de afwijking beoordelen en het resultaat terugkoppelen aan de aanvrager.
Bij afwijzing zal de ICT-architect dit motiveren op het afwijkverzoek. De aanvrager kan het resultaat voorleggen aan de CIO, waarbij de uiteindelijke beslissing genomen kan worden.

2 Vaststelling en wijziging

De aansluitvoorwaarden worden officieel vastgesteld door het iAdvies van het HHD.
Wijzigingen van de voorwaarden vinden plaats indien technische wijzigingen of wetgeving dit noodzakelijk maken.
In dat geval zal afdeling ICT en IFM de wijziging doorvoeren en het document opnieuw vastleggen bij het iAdvies. Het document wordt elke 6 maanden door de ICT-architect geëvalueerd en aangevuld met mogelijke nieuwe standaarden.

3 Publicatie

Deze aansluitvoorwaarden worden gepubliceerd op Hoogheemraadschap van Delfland Intranet, met vermelding van versienummer en datum van vaststelling. Bij de aanschaf van ICT-middelen kunnen deze aansluitvoorwaarden aan leveranciers worden verstrekt.

4 Authenticatie en autorisatie

4.1 Authenticatie

Authenticatie van nieuwe medewerkers en externe partijen vindt plaats aan de hand van een bij de HR-afdeling aangegeven boarding proces
Servicemedewerkers welke onderhoud of installatie moeten plegen aan de infrastructuur en hiervoor tijdelijk toegang hebben worden door de service desk geregistreerd op vertoon van een geldig Nederlands identiteitsbewijs.

4.2 Autorisatie

Voor technische autorisatie van gebruikers en systemen geldt het volgende:

4.2.1 Alle door HHD beheerde systemen zijn standaard lid van een domein.

4.2.2 Het root domein is HHDelfland.nl

4.2.3 Federatie met het domein is mogelijk.

4.2.4 Applicaties die buiten het netwerk van HHD aangeboden en beheerd worden dienen gebruik te maken federatieve technologie.

4.2.5 Federatie vindt plaats op basis van Oauth2.0 technologie.

4.2.6 HHDelfland maakt gebruik van Entra ID (voorheen Azure AD).

4.2.7 Schema aanpassingen worden getoetst bij de securityofficier en worden in het AD-design opgenomen.

4.2.8 Authenticatie vindt plaats via SAML2, Oauth2, Kerberos en LDAPS.

4.2.9 HHD-gebruikers zijn identificeerbaar via hun persoonlijke account.

4.2.10 HHD externe aansluitingen gebruiken Single Sign-on methodiek (SSO).

4.2.11 Applicaties welke geen SSO kennen dienen de gebruikers te identificeren op basis van het emailadres en bijbehorende wachtwoord. Hiervoor moet een aanvraag worden ingediend. Het wachtwoord moet ten minste voldoen aan het door HHD opgestelde wachtwoord beleid.

4.2.12 Functionaliteit welke buiten het interne netwerk van HHD aangeboden wordt dient beveiligd te worden door middel van Delfland Multi factor authenticatie (MFA).

4.2.13 Service Accounts kunnen nimmer interactief inloggen op systemen.

4.2.14 Beheer op servers vindt plaats met een separaat "named" beheer account welke herleid kan worden naar de gegevens van de beheerder welke werkzaamheden uitvoert.

4.2.15 Autorisatie voor beheerders wordt verstrekt op basis van minimale privileges om. Voor elke applicatie wordt een Roll Based Access Controll overzicht aangeleverd. De gebruikers worden met behulp van Thycotic Secret Server of PIM beheerd en geregistreerd. Informatiesystemen met een eigen domein worden geacht gebruik te maken van de door het HHD verstrekte gebruikerstoken met de geleverde autorisatie.

5 Datacenters

5.1 Datacenter toegang

5.1.1 Autorisatie om het DataCenter te betreden wordt verleend door de Afdeling ICT. De toegang dient aangevraagd te worden via de ServiceDesk ICT Werkzaamheden worden onder toezicht van Delfland ICT uitgevoerd.

5.1.2 Alle te plaatsen netwerk en server componenten in het Datacenter moeten geplaatst in de aangegeven racks volgens het geldende patchbeheerproces.

5.2 Core-switches

5.2.1 Op de core-switches worden alleen distributie- en of TOR-switches aangesloten.

5.2.2 Redundant koppelen op basis van SFP+ of hoger.

5.2.3 De te koppelen switch heeft redundante voedingen.

5.3 Distributie- en TOR-switches

5.3.1 Distributie switches leveren geen Power over Ethernet (PoE).

5.3.2 Het te koppelen device heeft afhankelijk van zijn functie redundante voedingen.

5.4 Access-switches

5.4.1 Een device wordt gekoppeld aan een access switch op basis van RJ45 en geldende standaard categorie bekabeling.

5.4.2 De netwerkpoort van het device dient te worden ingesteld op auto-sensing.

5.4.3 Het device krijgt door middel van een DHCP-server zijn IP-adres uitgedeeld.

5.4.4 Het device wordt op basis van zijn 802.1x of mac-adres geauthentiseerd.

5.4.5 Nadat het device is geauthentiseerd, krijgt het een netwerkprofiel toegewezen.

5.4.6 Een te koppelen/patchen device kan indien nodig worden gekoppeld op een PoE access-poort.

5.5 Externe toegang (derden)

5.5.1 Geautoriseerde externe gebruikers kunnen een aanvraag indienen voor externe toegang tot systemen van Delfland. Nadat deze aanvraag is geaccordeerd door de CISO, wordt er toegang verleend op basis van de remote diensten van VMWare.

5.6 Adressering

5.6.1 Interne Delfland IP adressering volgt adressering volgens IPv4: RFC 1918 (private ranges).

5.6.2 Server adressen zijn worden vastgelegd aan de hand van een IP-management proces

5.6.3 Client adressen worden met behulp van DHCP uitgegeven.

6 Wireless

6.1.1 Internettoegang is mogelijk binnen de kantoren van Delfland door gebruik te maken van PUBLICroam en GOVroam via het wifi-netwerk.

6.1.2 Wifi 802.11ac is de standaard.

6.1.3 Wi-Fi Protected Access II (802.1x) encryptie is vereist voor Wifi connecties.

7 Servers

7.1.1 Te installeren systemen (OS met applicatie(s)) dienen als basis te worden toegepast als virtual systeem (VM) op VMware ESXi. Alleen in uitzonderingsgevallen met goedkeuring van HHD ICT management kan een dedicated niet gevirtualiseerde server overwogen worden.

7.1.2 Systemen dienente voldoen aan de door HHD gestelde beschikbaarheids eisen.

7.1.3 Elk systeem dient te zijn voorzien van een separate management interface (voorbeeld: HP iLO, Dell DRAC)

7.1.4 De remote access aansluiting zal op een apart Out-of-Band Management netwerk worden aangesloten.

7.1.5 Om brede connectiviteit te waarborgen worden centrale DHCP- en DNS servers gebruikt voor de ip registratie en routering.
Dit betekent:
- Voor DNS wordt uitsluitend gebruik gemaakt van de centrale servers;

7.1.6 Het IP-adres van een server wordt statisch toegewezen;
- Applicaties maken gebruik van DNS namen.

7.1.7 Het te instaleren Windows OS heeft het hoogste versie welke vermeld is in de WILMA software catalogus.

7.1.8 Software voldoet aan de actuele HHD Software EOL strategie.

7.1.9 Windows updates worden geleverd met behulp van MECM of Intune.

7.1.10 Delfland biedt geen technische ondersteuning voor Linux OS distributies, tenzij het is onderdeel van de geleverde applicatie. (Toegang en support voor applicaties met een Linux distributie gebeurt op basis van afgesproken beheer documentatie).

7.1.11 Servers en netwerk worden gemonitord door 'Paessler Router Traffic Grapher' (PRTG) applicatie bij voorkeur agentless.

7.1.12 Te installeren servers eigendom van HHD of externe partijen volgen het HHD-asset managementproces.

8 Werkplekken

8.1 Laptops

8.1.1 Devices worden geregistreerd in Entra ID en Topdesk CMDB.

8.1.2 Drivers standaard beschikbaar binnen Microsoft Windows .

8.1.3 Geen automatische installatie van Drivers op werkplekken.

8.1.4 Operating System Windows 11

8.1.5 Antivirus door Microsoft Defender.

8.1.6 Aangesloten op HHdelfland domein policy. (intune).

8.2 Mobiele apparaten

Voor mobiel apparaten geld het volgende:

8.2.1 IOS of Android.

8.2.2 IPad of Tablet.

8.2.3 Iphone of Samsung smartphone.

8.2.4 Beheerd door Intune.

8.2.5 Delfland hanteert een N en N-1 beleid voor aanbieden van Mobiele OS waardoor altijd de meest recente versie of de eerstvolgende oudere versie van het product in gebruik is en volgt de HHD Software EOL strategie.

8.2.6 Mobiele apparaten dienen compliant te zijn met dit beleid en worden bij de niet-compliant status niet toegelaten.

9 Applicaties

9.1 Database

9.1.1 De database serverpoort wordt vastgesteld per instance en is bepaald door Delfland en geadministreerd.

9.1.2 Databases backup en policies vallen onder verantwoordelijkheid van Delfland ICT beheer.

9.1.3 Logbestanden zijn logisch gescheiden van de database bestanden en afgeschermd.

9.1.4 Log bestanden worden op aanvraag beschikbaar gesteld aan Delfland ICT beheer.

9.1.5 Delfland hanteert volgens HHD Software EOL strategie een N en N-1 beleid voor aanbieden van Database services.

9.1.6 Een administrator serviceaccount (domein account) en database account wordt gedeponeerd bij HHD ICT beheer.

9.1.7 Database diensten worden niet in de internet DMZ-zone geplaatst.

9.1.8 Geselecteerde geautoriseerde database diensten kunnen geplaatst worden in de PAKA DMZ.

9.1.9 Databases zijn niet rechtstreeks te benaderen voor gebruikers en beheerders.

9.1.10 Web server

9.1.11 Certificaten worden uitgegeven door Delfland of haar vertrouwde CA. Het beheer van certificaten is ondergebracht bij afdeling HHD ICT beheer.

9.1.12 Webapplicaties moeten worden voorzien van SSL Certificaten met tenminste SHA256 en een geldigheid van maximaal 1 jaar

9.1.13 Websites volgen het HHD-website beleid.

9.2 Front-end

9.2.1 Delfland ondersteunt browser applicaties op Microsoft Edge en Google Chrome.

9.2.2 Applicaties die externe office functionaliteiten vereisen moeten kunnen samenwerken met Microsoft O365.

9.2.3 Leverancier maakt voor zijn applicatie een “unattended install” package of container beschikbaar met installatie handleiding (versie/datum/owner).

9.2.4 Security patches worden in overleg met ICT doorgevoerd.

9.2.5 De reguliere update frequentie van de applicatie mag maximaal 1 keer per 3 maanden zijn. Dit wordt afgestemd tussen de functionele beheerder en ICT.

9.2.6 De applicatie mag op versie N en N-1 aangeboden worden. Oudere versies dienen binnen 3 maanden te worden vervangen door een nieuwe versie.

9.2.7 Het operating systeem is 64 bits.

9.2.8 Applicatie dient voor er autorisatie gebruik te maken van de domain, federatie authenticatie van HHDelfland.

9.2.9 Licenties mogen niet aan hardwarecomponenten gekoppeld zijn.

9.2.10 Applicatie distributie wordt gedaan met behulp van Intune.

9.2.11 Applicaties worden gemonitord door PRTG.

9.3 Back-end

9.3.1 Het onderhoud op de servers wordt uitgevoerd met de Microsoft Endpoint Configuration Manager (MECM) en VMWare vSphere van het Delfland.

9.3.2 De servers hebben standaard geen verbinding met het Internet, na goedkeuring van security coördinator kan een uitzondering hiervoor gemaakt worden.

9.3.3 De server heeft op de primaire root schijf (c:) system ondersteunende software staan. De applicatie wordt op een separate schijf geïnstalleerd. De data wordt op een door HHD geleverde netwerk schijf geplaatst.

9.3.4 Voor de server geldt het N, N-1 principe voor ondersteuning van het betreffende OS. (Volgt het HHD Software Life Cycle strategie document).

9.3.5 Als Hypervisor wordt VMWare ESX versie 7.x gebruikt. De applicaties dienen te kunnen draaien op VMWare ESX platform. (Volgt het HHD Software Life Cycle strategie document)

9.3.6 Servers/applicaties worden in het onderhoudsvensters gepatched.

9.3.7 Voor alle software (applicaties, OS, Drivers, Firmware, etc) is het vereist om gedurende de normale economische levensduur van de applicatie en hardware, wordt gepatched.

9.3.8 Vulnerability scanning vindt plaats met Tenable SC.

9.3.9 De applicatie dient gepatched te zijn op de laatste levels. Maximaal 3 maanden achter. Applicatiebeheerders en applicatie-eigenaars rapporteren aan SOC.

10 Back-up

10.1.1 Alle servers en instances worden geback-upt door middel van een standaard HHD back-up dienst (wordt geleverd door ProAct). Als er gebruik wordt gemaakt van producten die via de iData Agent kunnen worden geback-upte zal deze agent geïnstalleerd worden.

10.1.2 Backup /restore definities worden uitgevoerd aan de hand van een service recovery document (nog te maken). In geval van een leveranciersdienst dient de leverancier zelf aantoonbaar een backup mechanisme op te leveren. Hierover wordt apart een SLA afgesproken.

10.1.3 Voor de belangrijke applicaties (kroonjuwelen) wordt in samenwerking met de leverancier een herstelplan opgesteld en onderhouden.