Bijlage C: Programma van Eisen: TA-WAN

1. Inleiding

De looptijd van het huidige WAN-contract nadert zijn einde waardoor een aanbesteding voor een nieuw TA-WAN nodig is. Het huidige WAN voldoet ten aanzien van pure connectiviteit maar voldoet niet overal aan huidige richtlijnen met betrekking tot inrichting van kritische infrastructuren.
Ten aanzien van beschikbaarheid en performance zullen benoemde eisen niet veel afwijken van de huidige omgeving. Om echter te voldoen aan richtlijnen als BIO, CISR en NIS2 zijn aanvullende eisen opgenomen. Dit document bevat de details voor de gevraagde dienstverlening en de bijbehorende eisen.

2. Project omschrijving

Hoogheemraadschap van Delfland (HHD) doet een aanbesteding voor een managed dienstverlening die zorgt, gedurende 7 dagen per week en 24 uur per dag, voor een hoog beschikbaar en beveiligd Wide Area Network (WAN) in de door het hoogheemraadschap Delfland beheerde gebieden.

Het beheerde landschap omvat momenteel ongeveer 360 locaties, “buiten” locaties genoemd. “Buiten” locaties zijn locaties zoals stuwen of gemalen, vaak met beperkte infrastructuur zoals alleen een industriële kast waar de besturing en bediening in is ondergebracht. De locaties behoren tot kritische infrastructuur. Locaties zijn te verdelen in functionele groepen ten behoeve van de waterketen (zuivering), watersysteem (regulatie) en waterveiligheid(veiligheid). Typische locatie-types zijn gemalen, stuwen en meetpunten.

De gevraagde dienstverlening omvat:

- Managed WAN services
- Connectiviteit tussen de HHD-datacenters en "buiten” locaties
- Onderlinge connectiviteit tussen een beperkt aantal “buiten” locaties
- WAN segmentatie voor functionele locatie-groepen

HHD verwacht van de gecontracteerde leverancier hardware, levering, opbouw, implementatie en beheer. Tijdens de migratie dient bereikbaarheid en beschikbaarheid van de totale WAN, oud en nieuw, gegarandeerd te worden.

2.1. Confidentieel

Alle informatie in dit document en wat uitgewisseld wordt gedurende het aanbestedingstraject dient als confidentieel behandeld te worden.

3. TA-WAN dienstverlening

In dit hoofdstuk is beschreven waarvoor de gevraagde dienst voor gebruikt wordt. De dienst wordt in de aanbesteding uitgevraagd met een aantal eisen waar de aanbieder aan moet voldoen

3.1. Gevraagde dienst

Voor het in hoofdstuk 2 beschreven project vraagt Hoogheemraadschap van Delfland (HHD) een geïntegreerde en volledig beheerde Wide Area Network-dienst (WAN-dienst) af. De gecontracteerde leverancier levert zowel de technische infrastructuur als het volledige beheer ervan gedurende de gehele contractperiode. De dienstverlening dient zodanig te worden ingericht dat continuïteit, beschikbaarheid, veiligheid en schaalbaarheid van het HHD-WAN gewaarborgd zijn.

Omvang van de Gevraagde Dienstverlening

De gevraagde dienstverlening omvat in ieder geval de volgende onderdelen:

1. Managed WAN Services

De leverancier levert een end-to-end beheerde WAN-dienst, inclusief de benodigde hardware, software, monitoring, configuratie, rapportage, lifecycle-management en ondersteuning. De dienst wordt proactief beheerd en voldoet aan de kwaliteits- en beschikbaarheidseisen die zijn opgenomen in het Programma van Eisen.

2. Connectiviteit via Hub-Spoke architectuur

Het WAN wordt door de leverancier ingericht op basis van een Hub-Spoke model, waarbij connectiviteit wordt gerealiseerd tussen:

- De HHD-datacenters, en
- Alle "buiten"-locaties van HHD.

Een nadere technische toelichting op deze architectuur is opgenomen in de paragraaf *Centrale connectiviteit*.

3. Onderlinge connectiviteit tussen geselecteerde buitenlocaties

Voor een beperkt aantal objecten is directe onderlinge connectiviteit vereist. De leverancier voorziet in deze aanvullende verbindingen conform de nadere beschrijving in de paragraaf *Directe koppeling tussen Objecten*.

4. Beschikbaarheid op basis van Belangscore

Alle locaties worden door HHD ingedeeld volgens een vooraf vastgestelde Belangscore, die de minimale vereiste beschikbaarheidsniveaus bepaalt.
De leverancier levert en beheert het WAN conform de normen en prestatieindicatoren in de *Beschikbaarheidstabel*.

5. WAN-segmentatie

Het WAN moet worden ingericht met logische segmentatie voor verschillende functionele locatiegroepen, zoals beschreven in het Programma van Eisen. Deze segmentatie draagt bij aan beveiliging, performance en beheersbaarheid van het netwerk.

6. Hechte samenwerking en governance

De dienstverlening omvat een structurele, transparante en samenwerkingsgerichte manier van werken. De leverancier werkt intensief samen met HHD binnen het overeengekomen governance-model, zoals verder gespecificeerd in het Programma van Eisen. Dit omvat in elk geval:

- Reguliere afstemmingsoverleggen,
- Heldere escalatiemechanismen,
- Gezamenlijke roadmap-ontwikkeling,
- Proactieve advisering.

Gecombineerde Levering van Hardware, Implementatie en Beheer

HHD verwacht dat de gecontracteerde leverancier verantwoordelijk is voor:

- Levering van de benodigde WAN-hardware,
- Fysieke opbouw en installatie,
- Configuratie en ingebruikname,
- Migratie van bestaande verbindingen,
- Beheer en monitoring gedurende de volledige contractduur.

Tijdens de Migratiefase

Tijdens de migratie van het huidige WAN naar de nieuwe oplossing moet ononderbroken bereikbaarheid en beschikbaarheid van het totale WAN worden gegarandeerd. Zowel de oude als de nieuwe infrastructuur moeten tijdens de transitie parallel kunnen functioneren, zonder verstoring van bedrijfsvoering, processen of dienstverlening.

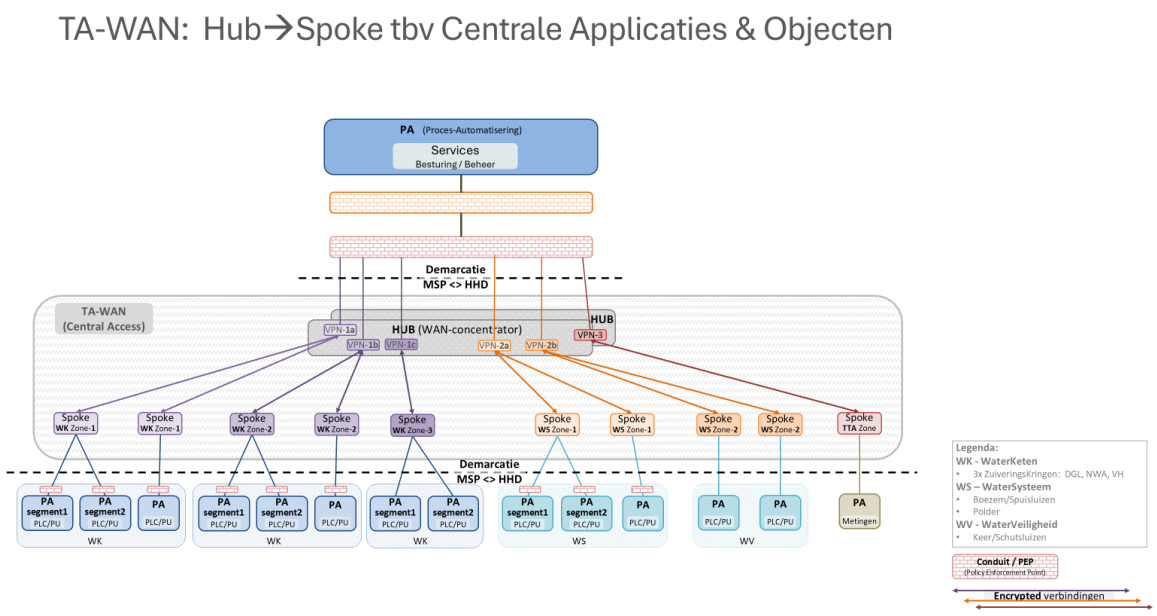
De leverancier documenteert de migratiestrategie, inclusief risico’s, mitigerende maatregelen, fallback-scenario’s en communicatieafspraken, als onderdeel van het implementatieplan.

3.2. Centrale connectiviteit

Ten behoeve van centrale services zoals besturing, beheer, monitoring en datacollectie omvat de TA-WAN dienstverlening beveiligde, encrypted connectiviteit tussen datacenters en objecten/kunstwerken. Objecten/kunstwerken worden verder aangeduid als “buiten” locaties en zijn verdeeld over verschillende functiegroepen.

- Functie groepen in de WAN dienen van elkaar gescheiden te zijn.
- Onderlinge communicatie tussen “buiten” locaties alleen via centrale PEP’s (Policy Enforcement Point) in beheer van HHD.

Grafische weergave:



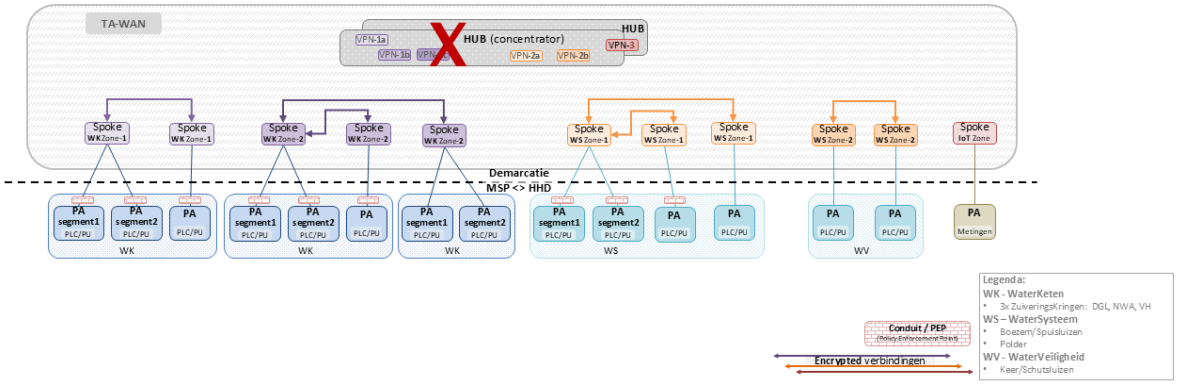
3.3. Directe koppeling tussen Objecten

Een aantal groepen objecten hebben operationeel onderlinge afhankelijkheden. Een beperkt aantal buiten locaties hebben een regionale rol voor andere locaties. Spoke locaties dienen dan ook direct met elkaar te kunnen communiceren zonder tussenkomst van de centrale Hub. Deze spoke-spoke connecties dienen eveneens beveiligd en encrypted te zijn. *Er zijn nu ongeveer 25 groepen met max 5 aangesloten sub-locaties*

Grafische weergave:

TA-WAN: Spoke→Spoke tbv directe koppeling tussen objecten

Een beperkt aantal spoke-locaties hebben regionaal onderlinge afhankelijkheden:
- Directe verbindingen tussen spoke-locaties; onafhankelijk van hub connectiviteit
- Encryptie is vereist



3.4. Huidige dienst omschrijving

TA verbindingen zijn telecommunicatie aansluitingen (TA) richting buiten locaties zoals gemalen, sluizen, stuwen, rioolgemalen of andere veldobjecten. Deze verbindingen zorgen ervoor dat data (zoals waterstanden, pompinformatie, storingsmeldingen) en besturingssignalen veilig en betrouwbaar heen en weer gaan tussen het kunstwerk en de centrale PA-systemen.

De TA-WAN netwerkinfrastructuur bij Delfland bestaat uit een beheerde IP-VPN dienst, opgezet met draadloze 4G en vaste ADSL-verbindingen. De datacenters in Rotterdam en Delfland zijn ook onderdeel van deze VPN doordat twee CPE's (Customer Provider Edge) van de IP-VPN verbonden zijn met de Perimeter firewalls van Delfland.

4. Lijst van Eisen

4.1. Functionele Eisen

Category	Eis	Omschrijving	Prioriteit
Functioneel	1.1	**Centrale applicaties & diensten**	
Functioneel	1.1.1	De managed serviceprovider (MSP) draagt zorg voor hoog beschikbare IP-connectiviteit tussen centrale datacenter locaties en buiten object (kunstwerk) locaties.	Essentieel (must)
Functioneel	1.1.2	De MSP implementeert een Hub-Spoke model voor communicatie tussen datacenters en buiten locaties, ook wel objecten dan wel kunstwerken genoemd.	Essentieel (must)
Functioneel	1.1.3	De MSP waarborgt in de WAN deze scheiding/isolatie per compartiment door WAN segmentatie (VPN) toe te passen. De MSP kan initieel uitgaan van een maximum van **10** segmenten/VPNs. Argumentatie: HHD heeft een standaard die verschillende functionele geïsoleerde compartimenten (eiland-groepen) beschrijft.	Essentieel (must)
Functioneel	1.1.4	De MSP sluit de verschillende WAN-segmenten (logisch) gescheiden aan op de centrale conduits/Policy Enforcement Points (PEPs) van HHD	Essentieel (must)
Functioneel	1.1.5	De MSP waarborgt dat buitenlocaties onderling niet kunnen communiceren, tenzij deze locaties behoren tot vooraf door HHD aangewezen objectgroepen met een operationele afhankelijkheid. Voor deze uitzonderingsgroepen moet de MSP beveiligde en versleutelde spoke-spoke communicatie faciliteren. Alle overige communicatie vanaf buitenlocaties wordt via de HUB gerouteerd naar de centrale conduits/Policy Enforcement Points (HHD-beheerd).	Essentieel (must)
Functioneel	1.1.6	De MSP zorgt voor WAN-beschikbaarheid van een locatie die voldoet aan de eisen uit de “Belangscore” tabel; In de beschikbaarheidstabel (3.7) zijn de karakteristieken voor incident, SLA en response-oplostijden opgenomen	Essentieel (must)
Functioneel	1.1.7	HHD blijft voor de LAN-infra haar eigen private IPv4 adresreeksen gebruiken. LAN IPv4 omnummering is geen optie.	Essentieel (must)
Functioneel	1.1.8	De MSP ondersteunt gedurende het contract IPv4 aanpassingen en uitbreidingen van het HHD IPv4-plan.	Essentieel (must)
Functioneel	1.1.9	De MSP beheert de toegang tot de devices en heeft het overzicht van de personen die toegang hebben tot deze devices en kan binnen 2 uur de credentials van deze personen wijzigen zodat ongewenste toegang tot een minimum beperkt wordt.	Essentieel (must)

De omgeving van HHD bestaat uit verschillende functionele werkgebieden. Ten aanzien van toegang, scheiding en isolatie van de werkgebieden zijn er additionele security gerelateerde eisen.

Category	Eis	Omschrijving	Prioriteit
Functioneel	1.2	**Directe koppeling objecten**	
Functioneel	1.2.1	De MSP draagt zorg voor directe onderlinge IP-connectiviteit voor een aantal gespecificeerde groepen van object (kunstwerk) locaties.	Essentieel (must)
Functioneel	1.2.2	De MSP implementeert de onderlinge directe communicatie binnen de gespecificeerde groepen van objecten onafhankelijk van connectiviteit met de centrale datacenter-hub.	Essentieel (must)
Functioneel	1.2.3	De MSP zorgt voor WAN-beschikbaarheid die voldoet aan de eisen uit de “Belangscore” tabel; Zie eis 1.1.6	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Functioneel	1.3	**Beveiliging**	
Functioneel	1.3.1	De MSP zorgt voor encryptie op de netwerk-laag (encryptie-in-transit). Argumentatie: HHD maakt nog gebruik van applicatie protocollen zonder versleuteling	Essentieel (must)
Functioneel	1.3.2	De MSP implementeert encryptie op alle Wan-verbindingen; CPE<>CPE	Essentieel (must)
Functioneel	1.3.3	De MSP implementeert encryptie zowel op Hub-Spoke communicatie als op de onderlinge communicatie tussen objecten (buiten locaties)	Essentieel (must)
Functioneel	1.3.4	De geimplenteerde encryptie-protocollen moeten voldoen aan de aanduiding “Goed” in het NCSC-document “Richtlijnen voor Transport Layer Security”	Essentieel (must)
Functioneel	1.3.5	De MSP waarborgt dat alle door haar geleverde en/of beheerde netwerkcomponenten (waaronder switches, routers, firewalls, draadloze infrastructuur, netwerkmanagementsoftware en firmware) die direct een koppeling of in verbinding staan met het Netwerk van HHD geschikt zijn voor toepassing binnen vitale infrastructuur en ondersteuning bieden aan processen met classificatie BIV-Midden en BIV-Hoog conform de BIO voor HHD De MSP voldoet hierbij aan de volgende eisen: 1. Netwerkapparatuur, firmware en beheersoftware zijn niet afkomstig uit landen, of van leveranciers, die door de Nederlandse overheid (waaronder de Nationaal Coördinator Terrorismebestrijding en Veiligheid) of door de Europese Unie zijn aangemerkt als hoog risico voor nationale veiligheid, digitale weerbaarheid of vitale infrastructuur. 2. De MSP waarborgt dat de volledige leveringsketen (hardware, firmware, software, updates en support): a. Aantoonbaar transparant en verifieerbaar is; b. Vrij is van ongewenste statelijke of niet-statelijke beïnvloeding conform hetgeen in de NCTV rapport is vermeld; c. Geen verplichtingen kent die ongeautoriseerde toegang tot netwerken of gegevens mogelijk maken.	Essentieel (must)
Functioneel	1.3.6	De MSP moet alle loggegevens die voortkomen uit het beheer, gebruik en functioneren van de netwerkdiensten uitsluitend verwerken, opslaan en bewaren binnen de Europese Economische Ruimte (EER). Logging mag niet worden opgeslagen of verwerkt buiten de EER, en mag niet toegankelijk zijn voor partijen die onder niet-Europese jurisdicties vallen. De MSP moet aantoonbare maatregelen treffen om te voldoen aan de geldende Europese wet- en regelgeving op het gebied van informatiebeveiliging en gegevensbescherming, waaronder minimaal: • End-to-end beveiliging van logdata tijdens transport en opslag; • Strikte toegangscontrole en rolgebaseerde autorisatie op alle logging- en beheerplatformen; • Bewaking op integriteit, beschikbaarheid en vertrouwelijkheid van loggegevens; • Het voorkomen van ongeautoriseerde toegang door derde partijen of buitenlandse overheden.	Essentieel (must)

		De MSP moet op verzoek van HH Delfland kunnen aantonen dat alle logging- en dataverwerkingslocaties volledig binnen de EER vallen en voldoen aan relevante normenkaders (zoals ISO 27001 of gelijkwaardig).	

4.2. Inkoop Eisen

Category	Eis	Omschrijving	Prioriteit
Functioneel	1.4	**Inkoop**	
Functioneel	1.4.1	De MSP levert een separate prijsopgave per geboden oplossing voor de verschillende belangscores Argumentatie: Exacte aantallen voor locaties met belangscore-x (=1,2,3) zijn nog niet bekend.	Belangrijk (should)
Functioneel	1.4.2	De MSP dient voor elke belangscore een beschrijving van de geboden oplossing aan te leveren.	Belangrijk (should)
Functioneel	1.4.3	De MSP mag voor de prijsopgave uitgaan van (zie hoofdstuk 4.6 voor eisen belangscores): - Belangscore-**1: 42** locaties - Belangscore-**2: 221** locaties - Belangscore-**3: 76** locaties *(+ 17 categorie-2, zonder vast energievoorziening)*	Belangrijk (should)

4.3. Technische Eisen

In de categorie technisch zijn eisen en karakteristieken benoemd voor:

- CPE Hardware
- Protocollen
- Demarcatie
- WAN en redundantie
- Performance en bandbreedte

Category	Eis	Omschrijving	Prioriteit
Technisch	2.1	**Apparatuur**	
Technisch	2.1.1	Apparatuur-eisen "Datacenter": Afmetingen CPE: (H x W x D): 9.05 (2RU) x 44.5 x 60 (Cm)	Essentieel (must)
Technisch	2.1.2	Apparatuur-eisen "Datacenter": CPE is voorzien van een redundante powersupply.	Essentieel (must)
Technisch	2.1.3	Apparatuur-eisen "Datacenter": CPE koeling heeft een Back-to-Front airflow of Front-to-Back airflow.	Essentieel (must)
Technisch	2.1.4	Apparatuur-eisen "Inpandig": Afmetingen CPE ma6.ximaal: PTO conform tekening PTO, bijlage 6.7	Essentieel (must)
Technisch	2.1.5	Apparatuur-eisen "Inpandig": Mogelijkheid voor aansluiting op UPS met output van 230 AC	Essentieel (must)
Technisch	2.1.6	Apparatuur-eisen "Inpandig": Mogelijkheid voor aansluiting op UPS met output van 24 Volt DC	Essentieel (must)
Technisch	2.1.7	Apparatuur-eisen "Inpandig": 19-inch rackmount kit moet beschikbaar zijn	Belangrijk (should)
Technisch	2.1.8	Apparatuur-eisen "Inpandig": Voldoet aan ETSI EN 300 019-2-3 Specification T 3.3: Not temperature-controlled locations	Belangrijk (should)
Technisch	2.1.9	Apparatuur-eisen "Buitenkasten": Afmetingen CPE maximaal: PTO spec bijlage 6.8	Essentieel (must)
Technisch	2.1.10	Apparatuur-eisen "Buitenkasten": Mogelijkheid voor aansluiting op UPS met output 24 Volt DC	Essentieel (must)
Technisch	2.1.11	Apparatuur-eisen "Buitenkasten": Voldoet aan ETSI EN 300 019-2-3 Specification T 3.4: Sites with heat-trap	Belangrijk (should)
Technisch	2.1.12	De MSP biedt de optionele oplossing van "ruggedized" apparatuur als deze apparatuur in buitenkasten wordt geplaatst	Belangrijk (should)
Technisch	2.1.13	De CPE maakt alleen gebruik van passieve koeling(bijvoorbeeld geen ventilator)	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Technisch	2.2	**LAN**	
Technisch	2.2.1	WAN/CPE ondersteunt IPv4 protocollen	Essentieel (must)
Technisch	2.2.2	WAN/CPE ondersteunt IPv6 protocollen	Belangrijk (should)
Technisch	2.2.3	Demarcatie "Datacenter(s)": 1x fysieke koppeling per datacenter op firewall	Essentieel (must)
Technisch	2.2.4	Demarcatie "Datacenter(s)": Koppelingvlak 1Gb; RJ45/UTP	Essentieel (must)
Technisch	2.2.5	Demarcatie "Datacenter(s)": Meerdere logische Layer-3 koppelingen naar centrale firewall	Essentieel (must)
Technisch	2.2.6	Demarcatie "Datacenter(s)": IPv4 BGP Routing protocol is vereist. De BGP-koppeling zal prefixes accepteren zowel in als uit.	Essentieel (must)
Technisch	2.2.7	Demarcatie "Datacenter(s)": Datacapturing/packet inspection op CPE is geblokkeerd en uitgeschakeld	Essentieel (must)
Technisch	2.2.8	Demarcatie "buitenLocaties": Logisch koppelvlak is een layer-2 koppeling; CPE fungeert als default-gateway	Essentieel (must)
Technisch	2.2.9	Demarcatie "BuitenLocaties": Fysiek koppelvlak is RJ45/UTP	Essentieel (must)
Technisch	2.2.10	Demarcatie "BuitenLocaties": Aansluiten legacy apparatuur moet mogelijk zijn (10/100 Mb, half-/full-duplex; zonder auto-negotation)	Essentieel (must)
Technisch	2.2.11	Demarcatie "Buiten Locaties": Netwerk segmentatie op LAN-niveau moet toegepast kunnen worden; Vlan implementatie op basis van 802.1q protocol	Essentieel (must)
Technisch	2.2.11	Demarcatie "BuitenLocaties": Bij toepassing van LAN-segmentatie moeten segmenten ook van elkaar geisoleerd kunnen worden	Essentieel (must)
Technisch	2.2.12	Demarcatie "Buiten Locaties": Alleen apparatuur wat ge-identificeerd en ge-authoriseerd is mag op het netwerk geactiveerd worden	Essentieel (must)
Technisch	2.2.13	Demarcatie "Locaties": Security op basis van MAC-adres verificatie (huidig) moet geimplementeerd worden; geavanceerdere authenticatie methodes; zoals 802.1x met Certificaten/MAB, moet toepasbaar zijn.	Essentieel (must)
Technisch	2.2.14	Demarcatie "BuitenLocaties": Huidig IPv4 default-gateway adres moet door de MSP op de CPE gehandhaafd blijven.	Essentieel (must)
Technisch	2.2.15	Demarcatie "Buiten Locaties": Datacapturing/packet inspection op CPE is geblokkeerd en uitgeschakeld	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Technisch	2.3	**WAN**	
Technisch	2.3.1	Locatie ontsluiting "Belangscore-**0** (=Datacenter(s))": Redundantie naar HHD HA-Datacenter	Essentieel (must)
Technisch	2.3.2	Locatie ontsluiting "Belangscore-**0** (=Datacenter(s))": Glasvezel WAN-aansluiting	Essentieel (must)
Technisch	2.3.3	Locatie ontsluiting "Belangscore-**1**": Redundante WAN-verbindingen	Essentieel (must)
Technisch	2.3.4	Locatie ontsluiting "Belangscore-**1**": Redundante CPE-hardware	Belangrijk (should)
Technisch	2.3.5	Locatie ontsluiting "Belangscore-**1**": Primaire ontsluiting bedraad (volgens huidig schema)	Essentieel (must)
Technisch	2.3.6	Locatie ontsluiting "Belangscore-**2**": Redundante WAN-verbindingen	Essentieel (must)
Technisch	2.3.7	Locatie ontsluiting "Belangscore-**2**": Huidige bedrade aangesloten locaties voorzien van een bedrade, primaire, WAN-verbinding	Essentieel (must)
Technisch	2.3.8	Locatie ontsluiting "Belangscore-**3**": Huidige bedrade aangesloten locaties voorzien van een bedrade WAN-verbinding	Belangrijk (should)
Technisch	2.3.9	Alle verbindingen, inclusief draadloos, dienen gekoppeld te zijn aan een "**private**" infrastructuur.	Essentieel (must)
Technisch	2.3.10	De "private" infrastructuur, zowel als de APN, is alleen toegankelijk voor geautoriseerde gebruikers en niet publiek toegankelijk.	Essentieel (must)
Technisch	2.3.11	Signaalsterkte voor draadloze verbindingen op alle locaties dienen te voldoen aan de classificatie "goed"; kwalitatief sterk signaal zonder "dropouts" - Signal Strength **RSRP (dBm) ≥ -90 dBm** Good --> Excellent - Signal Quality **RSRQ (dB) ≥ -8 dB** Good --> Excellent - Signal to Noise **SINR/SNR ≥ 10 dBm** Good --> Excellent	Essentieel (must)
Technisch	2.3.12	De MSP biedt mobiele verbindingen die alleen gebruik maken van moderne technologieën en is minimaal 4G.	Essentieel (must)
Technisch	2.3.13	Indien signaalsterkte van de primaire mobiele provider niet afdoende is dienen alternatieven als "blindspot" preventie aangeboden te worden, zoals bv buiten- of richtantennes, signaalversterkers, roaming of multi-network-SIM (in uiterste noodzaak).	Essentieel (must)
Technisch	2.3.14	Bij toepassing van buitenantennes dienen deze vandalismebestendig/hufterproof te zijn zoals bv puck antennes	Essentieel (must)
Technisch	2.3.15	Bandbreedte "Belangscore=**0**": 100Mb/s	Essentieel (must)
Technisch	2.3.16	Bandbreedte "Belangscore=**1**": ≥ 10Mb/s	Essentieel (must)
Technisch	2.3.17	Bandbreedte "Belangscore=**2/3**": ≥ 2Mb/s	Essentieel (must)
Technisch	2.3.18	Voor **bedrade** aansluitingen moet de netwerk latency **<50**ms zijn	Belangrijk (should)
Technisch	2.3.19	Voor **draadloze** aansluitingen moet de netwerk latency **<200**ms zijn	Belangrijk (should)
Technisch	2.3.20	Voor draadloze aansluitingen dient bij voorkeur gebruik gemaakt te worden van eSIM	Belangrijk (should)
Technisch	2.3.21	Voor locaties zonder vaste energievoorziening (Locatie ontsluiting belangscore-3 & "Energie-zuinig") moet de optie van alleen een fysieke SIM-kaart, zonder managed device, aangeboden worden.	Belangrijk (should)
Technisch	2.3.22	De fysieke SIM-kaarten voor "Locatie ontsluiting belangscore-3" & "Energiezuinig" moeten aangesloten zijn op de private APN(s) van HHD	Essentieel (must)
Technisch	2.3.23	De MSP dient voor alle verbindingen gebruik te maken van Europese (datacom) provider(s)	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Technisch	2.4		
Technisch	2.4.1	Voor optimale beschikbaarheid kan een **automatische** (geplande) volledige router-reset geïmplementeerd worden. Toepassing in de volgende omstandigheden: 1) Verlies mobiele verbinding gedurende een vastgestelde tijdsslot (30min) 2) Verlies van LAN-connectiviteit (link-status) gedurende een vastgestelde tijdsslot (30min) Argumentatie: Meeste locaties zijn onbemand. Beperken van noodzakelijke locatie bezoeken.	Belangrijk (should)
Technisch	2.4.2	Voor optimale beschikbaarheid, kan een volledige router-reset **op afstand** geïnitieerd worden. Toepassing in de volgende omstandigheden: 1) Vanuit beheer standpunt door de MSP zelf 2) Op initiatief van HHD via de selfservice portal binnen de afgesproken SLA-tijd van (2 uur)	Essentieel (must)
Technisch	2.4.3	De MSP managed apparatuur is ge-"hardened" conform CIS hardening best-practices	Essentieel (must)
Technisch	2.4.4	De MSP managed apparatuur is niet publiekelijk toegankelijk	Essentieel (must)
Technisch	2.4.5	De MSP voorziet de devices per buitenlocatie van een uniek paswoord	Essentieel (must)
Technisch	2.4.6	De MSP kan bij cyber risico's de wachtwoorden vervangen binnen 1 dag tijd, zodat niet geautoriseerde gebruikers geen toegang tot de communicatieapparatuur	Essentieel (must)
Technisch	2.4.7	Bij gevonden kwetsbaarheden in de managed apparatuur wordt HHD geïnformeerd. Operationeel risico en benodigde acties zijn onderdeel van de communicatie naar HHD.	Essentieel (must)
Technisch	2.4.8	De MSP waarborgt dat toegepaste hardware en software gedurende de contractduur volledig ondersteund is. Dit omvat ten minste het beschikbaar zijn van beveiligingsupdates, patches en technische ondersteuning.	Essentieel (must)
Technisch	2.4.9	Beveiligingsupdates en patches worden door de MSP tijdig geïnstalleerd. N**a voorafgaand overleg en afstemming met opdrachtgever** doet de MSP een concreet voorstel voor implementatie, met inachtneming van overeengekomen onderhoudsvensters en impact op de bedrijfsvoering.	Essentieel (must)

4.4. Operationele Eisen

In de categorie operationeel zijn eisen en karakteristieken benoemd voor:

- Dienstverlening
- Monitoring
- Rapportage
- Richtlijnen

Category	Eis	Omschrijving	Prioriteit
Operationeel	3.1		
Operationeel	3.1.1	Locatie "Belangscore **0 & 1**": De MSP zorgt voor proactieve monitoring op primaire en secundaire verbindingen	Essentieel (must)
Operationeel	3.1.2	Locatie "Belangscore **0 & 1**": De MSP zorgt voor automatische ticket generatie en melding aan HHD IT-Servicedesk bij verstoringen	Essentieel (must)
Operationeel	3.1.3	De MSP biedt HHD een "selfservice" portaal met actuele beschikbaarheid en status informatie, voor **alle** locaties	Essentieel (must)
Operationeel	3.1.4	De MSP biedt HHD een "selfservice" portaal waarmee bandbreedte gebruik inzichtelijk wordt.	Belangrijk (should)
Operationeel	3.1.5	Bij calamiteiten binnen het HHD-domein kan een aanpassing van de MAC-authenticatie noodzakelijk zijn. De MSP dient hiervoor minimaal een "fast-solution" proces (<1 uur) ingericht te hebben.	Essentieel (must)
Operationeel	3.1.6	De MSP biedt HHD een "Selfservice" portaal voor wijzigen van de MAC-Authenticatie op een buiten-locatie	Belangrijk (should)
Operationeel	3.1.7	In geval van calamiteiten dienen locaties dienen direct geïsoleerd of afgeschakeld te kunnen worden. De MSP moet hiervoor minimaal een "fast-solution" proces (<1 uur) ingericht te hebben.	Essentieel (must)
Operationeel	3.1.8	De MSP biedt HHD een "Selfservice" portaal voor isoleren locaties en/of blokkeren SIM	Belangrijk (should)
Operationeel	3.1.9	De MSP biedt HHD een "Selfservice" portaal voor initiatie van een "router-reset op afstand"	Belangrijk (should)
Operationeel	3.1.10	De MSP dient de redundantie (Verbinding en hardware) van een locatie te monitoren en, bij uitval, de redundantie te herstellen volgens de waarden uit de “Belangscore” tabel;	Essentieel (must)
Operationeel	3.1.11	De MSP heeft de mogelijkheid om monitoring en status gegevens beschikbaar te stellen via een API	Wens (could)
Operationeel	3.1.12	De MSP moet mobiele verbindingen (4G/5G) leveren binnen marktconforme termijnen die passen bij kritische infrastructuur. De volgende levertijden zijn vereist: • Spoedlevering met vooraf geconfigureerde router en SIM: maximaal 2 werkdagen. • Standaard zakelijke levering: maximaal 7 werkdagen. De MSP moet HH Delfland in staat stellen om een mobiele verbinding als tijdelijke of redundante voorziening direct inzetbaar te maken bij storingen, calamiteiten of migraties.	Essentieel (must)
Operationeel	3.1.13	De MSP moet vaste verbindingen op basis van bestaande infrastructuur leveren binnen de volgende termijnen: • DSL/ kabel: maximaal 15 werkdagen. • Glasvezel indien al aanwezig in het gebouw: maximaal 15 werkdagen De MSP moet vooraf aangeven of de fysieke infrastructuur aanwezig is en welke levertijdcategorie van toepassing is.	Essentieel (must)
Operationeel	3.1.14	Voor nieuwe, dedicated verbindingen die fysieke aanleg vereisen, moet de MSP de volgende levertijden kunnen realiseren: • Glasvezel op bestaande infrastructuur: maximaal 5 weken. • Nieuwe glasvezelverbinding met graafwerk en/of tracé: maximaal 14 weken. • Complexe WAN-infrastructuur of multi-site-omgevingen: maximaal 6 maanden.	Belangrijk (should)

		De MSP moet HH Delfland tijdig informeren over benodigde vergunningen, civiele werkzaamheden en afhankelijkheden die de levertijd beïnvloeden.	
Operationeel	3.1.15	De MSP moet een leverstrategie toepassen die waarborgt dat kritische locaties van HH Delfland binnen een korte termijn operationeel zijn. De volgende fasering is verplicht: • Week 1: mobiele 4G/5G-fallback verbinding operationeel. • Week 2–6: primaire vaste verbinding actief (DSL/kabel/bestaand glas). • Week 12+: volledige redundantie opleveren (tweede glasvezel of alternatieve provider/route).	Essentieel (must)
Operationeel	3.1.16	De MSP moet HH Delfland voorzien van: • Een actuele en realistische opleverplanning per locatie; • Tijdige meldingen van afwijkingen in levertijd; • Inzicht in afhankelijkheden (graafwerk, KLIC, netbeheerder, vergunningen, etc.); • Een escalatieproces wanneer levertijden dreigen te worden overschreden.	Essentieel (must)
Operationeel	3.1.17	Voor locaties die onderdeel zijn van kritische processen (bijv. gemalen, zuiveringen, OT/SCADA-locaties), moet de MSP garantie op tijdige oplevering bieden door: • Het standaard inzetten van een mobiele verbinding als tijdelijke primary; • Het parallel voorbereiden van vaste infrastructuur; • Het toepassen van redundantie volgens best practice (glas + mobiel of dual glasvezel).	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Operationeel	3.2		
Operationeel	3.2.1	Connectie onderbrekingen, bewust en onbewust, van zowel primaire als secundaire verbindingen, voor **alle** locaties, worden gelogged en bewaard gedurende 2 jaar.	Essentieel (must)
Operationeel	3.2.2	Over een periode van 2 jaar is historie informatie betreffende beschikbaarheid, **signaalsterkte** en bandbreedte beschikbaar en opvraagbaar. Zowel voor primaire als secundaire verbindingen.	Belangrijk (should)
Operationeel	3.2.3	De MSP levert een maandelijkse rapportage van issues/incidenten en RTO voor **alle** locaties; inclusief kortstondige onderbrekingen; Rapportage inclusief een tijdslijn (grafiek).	Essentieel (must)
Operationeel	3.2.4	De MSP levert een maandelijkse rapportage van het bandbreedte gebruik voor alle locaties met bedrade verbindingen; Rapportage inclusief een tijdslijn (grafiek).	Belangrijk (should)
Operationeel	3.2.5	De MSP levert een jaarlijkse SLA rapportage van issues/incidenten, Response- en oplostijden betreffende alle locaties.	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Operationeel	3.3		
Operationeel	3.3.1	De MSP heeft voor de dienstverlening een Single point of Contact beschikbaar.	Belangrijk (should)
Operationeel	3.3.2	De MSP beschikt over een escalatie process voor RTO/SLA issues	Essentieel (must)
Operationeel	3.3.3	Bij gelijktijdige uitval van **10 of meer** locaties wordt opgeschakeld naar een RTO van **4** uur ongeacht de individuele RTO-afspraken.	Belangrijk (should)
Operationeel	3.3.4	De MSP dient alle On-Site activiteiten aan te melden aan HHD IT-Servicedesk	Essentieel (must)
Operationeel	3.3.5	De MSP mag On-Site activiteiten alleen uitvoeren na goedkeuring van HHD, volgens bestaande HHD-processen.	Essentieel (must)
Operationeel	3.3.6	De MSP mag On-Site activiteiten alleen uitvoeren onder begeleiding van HHD-personeel (alle objecten zijn CSIR-weerstandsniveau 1 of 2)	Essentieel (must)
Operationeel	3.3.7	De MSP dient communicatie van dienstverlening en ondersteuning te leveren in de Nederlandse taal.	Essentieel (must)
Operationeel	3.3.8	Alle dienstverlening dient vanuit Europese centra uitgevoerd te worden; Incl. NOC/SOC	Essentieel (must)
Operationeel	3.3.9	De MSP verleent de dienstverlening volgens de Nederlandse en Europese wetgeving.	Essentieel (must)
Operationeel	3.3.10	De MSP voldoet aan de Wet beveiliging netwerk- en informatiesystemen (**Wbni**)	Essentieel (must)
Operationeel	3.3.11	De MSP voldoet aan de CSIR-versie 3.0 richtlijnen	Essentieel (must)
Operationeel	3.3.12	De MSP voldoet aan de BIO2 richtlijnen	Essentieel (must)
Operationeel	3.3.13	De MSP overhandigt jaarlijks een ISAE 3402 Type II of SOC 2 assurance-verklaring die betrekking heeft op de volledige dienstverlening aan HHD	Essentieel (must)

4.5. Implementatie Eisen

Bij implementatie ligt de focus op een probleemloze migratie:

- Parallel WAN; oud/nieuw
- Migratie en installatie; draaiboeken en planning
- PoC

Category	Eis	Omschrijving	Prioriteit
Implementatie	4.1		
Implementatie	4.1.1	HHD verwacht van de gecontracteerde leverancier (MSP) hardware, levering, opbouw, implementatie en beheer.	Essentieel (must)
Implementatie	4.1.2	De MSP garandeert tijdens de gehele migratie bereikbaarheid en beschikbaarheid van de totale WAN, zowel voor locaties gekoppeld aan het bestaande WAN als aan het nieuwe WAN.	Essentieel (must)
Implementatie	4.1.3	De MSP levert, per geboden oplossing één generiek migratieplan aan.	Essentieel (must)
Implementatie	4.1.4	De MSP levert: Een generiek migratiedraaiboek voor de standaard migratieaanpak, inclusief teststappen, acceptatiecriteria en fallback-procedure. 1. Een locatietype-specifieke uitwerking voor groepen standaardlocaties (Belangscore 2 en lager). 2. Een projectspecifiek maatwerkdraaiboek voor alle kritische locaties (Belangscore 1), inclusief volledig test- en opleverprotocol en uitgewerkte fallback-scenario's. 3. Het draaiboek wordt vooraf ter goedkeuring aan HHD aangeboden.	Essentieel (must)
Implementatie	4.1.4	De MSP neemt operationele testen van de gemigreerde productie omgeving op in het draaiboek.	Essentieel (must)
Implementatie	4.1.5	De MSP dient bij implementatie rekening te houden met "natte" seizoen(en). De MSP dient flexibel te plannen afhankelijk van weersomstandigheden en Go/NoGo momenten vast te leggen.	Essentieel (must)
Implementatie	4.1.6	Bij calamiteiten kunnen geplande werkzaamheden aan de WAN-infra die invloed hebben op de Bedrijfsvoering van Delfland tot vlak voor de aanvang door HHD geannuleerd worden.	Essentieel (must)
Implementatie	4.1.7	Indien Opdrachtgever (HHD) deze uiterlijk 24 uur vooraf aan de geplande werkzaamheden annuleert, kan de Opdrachtnemer (MSP) geen kosten in rekening brengen	Essentieel (must)
Implementatie	4.1.8	"Datacenter(s)": De centrale HUB dient binnen kantooruren aangesloten en geactiveerd te worden: Activiteiten plannen altijd in overleg met HHD.	Essentieel (must)
Implementatie	4.1.9	"Buitenlocaties" De migraties van objectlocaties (belangscores 1–3) worden uitgevoerd tijdens kantooruren, maandag t/m vrijdag, bijvoorbeeld 07:00–17:00 uur. De definitieve tijdvakken worden in overleg met HHD vastgesteld.	Essentieel (must)
Implementatie	4.1.10	"Buiten Locaties": De MSP planned migraties van gegroepeerde objecten op dezelfde dag	Essentieel (must)
Implementatie	4.1.11	"Buiten Locaties": De MSP voert migraties uitsluitend uit onder begeleiding van HHD-personeel	Essentieel (must)
Implementatie	4.1.12	"Buiten Locaties": Een migratie op een locatie is pas afgerond als het draaiboek voor die locatie afgetekend is.	
Implementatie	4.1.13	"Datacenter(s)": De MSP moet de CPE afmonteren in een 19-inch rack van HHD	Essentieel (must)
Implementatie	4.1.14	"Datacenter(s)": De MSP monteert de apparatuur in het door HHD opgegeven rack en op de juiste rackpositie	Essentieel (must)
Implementatie	4.1.15	"Datacenter(s)": De MSP monteert de apparatuur volgens de in het datacenter geldende airflow richtlijnen.	Essentieel (must)
Implementatie	4.1.16	"Datacenter(s)": HHD levert de patch-kabel vanaf de FW tot in het 19-inch rack van de CPE	Essentieel (must)

Implementatie	4.1.17	"Buiten Locaties": De MSP monteert de apparatuur op de door HHD opgegeven positie	Essentieel (must)
Implementatie	4.1.18	"Buiten Locaties": De MSP levert een patch-kabel op lengte vanaf de CPE naar HHD-infra	Essentieel (must)
Implementatie	4.1.19	"Buiten Locaties": De MSP configureert het koppelvlak naar de aan te sluiten HHD-apparatuur als een untagged LAN-interface.	Essentieel (must)
Implementatie	4.1.20	MSP stelt samen met opdrachtgever een exit strategie op na afsluiten overeenkomst. Wanneer de overeenkomst afloopt is MSP bereid om een soepele overdracht te bewerkstelligen. De exit strategie wordt net zoals de SLA en het DAP onderdeel van de overeenkomst.	Essentieel (must)

Category	Eis	Omschrijving	Prioriteit
Implementatie	4.2	PoC	
Implementatie	4.2.1	De MSP toont voor elke door hem aangeboden technische oplossing die in het veld wordt ingezet aantoonbaar de werking, prestaties en beschikbaarheid aan binnen een door HHD goedgekeurde Proof-of-Concept (PoC) omgeving. De PoC moet per oplossing de volledige end-to-end functionaliteit demonstreren, inclusief connectiviteit, configuratie, beveiliging, beheerfunctionaliteit en operationeel gedrag onder realistische omstandigheden.	Essentieel (must)
Implementatie	4.2.2	De MSP gebruikt voor de PoC het generieke implementatie draaiboek	Essentieel (must)
Implementatie	4.2.3	De PoC wordt uitgevoerd in de test-opstelling van HHD in Vlaardingen	Essentieel (must)
Implementatie	4.2.4	De leverancier voert de Proof-of-Concept (PoC) uit met volledig aangesloten en door HHD beschikbaar gestelde testapparatuur, zodat de PoC representatief is voor de feitelijke productieomgeving van HHD.	Essentieel (must)
Implementatie	4.2.5	Per geboden oplossing levert de MSP een testplan aan met uitgevoerde testresultaten	Essentieel (must)
Implementatie	4.2.6	Testplannen wordt in onderling overleg, tussen MSP en HHD, definitief gemaakt.	Essentieel (must)
Implementatie	4.2.7	De MSP deelt de testresultaten, voor accordering, aan de opdrachtgever, HHD.	Essentieel (must)

4.6. Beschikbaarheidstabel

Belangscore	Response	RTO Connectiviteit	RTO Redundancy	Max incidenten per Jaar	SLA periode	Redundante Verbinding	Redundante Hardware
0 (HA-Datacenters)	15 min.	2 uur	8 uur	2x	24x7, Jaar	Ja	Ja
1	1 uur	4 uur	Next Day	4x	24x7, Jaar	Ja	Ja
2	2 uur	24 uur (NBD)	nvt	6x	5x10 (8-18u), Jaar	Ja	MSP-defined
3	4 uur	5 dagen	nvt	12x	5x10 (8-18u), Jaar	Nee	Nee

Wanneer een gevraagde Belangscore niet volledig geleverd kan worden, mag de MSP een oplossing aanbieden op basis van een lagere belangscore, mits dit vooraf expliciet wordt gemeld aan HH Delfland.

Indien een specifiek aspect binnen een belangscore (bijvoorbeeld RTO, SLA-periode, redundantie of maximaal aantal incidenten) niet geleverd kan worden, dan geldt voor dat aspect de waarde van de eerstvolgende lagere belangscore. De Belangscore van de locatie zelf wijzigt hierdoor niet; uitsluitend het betreffende aspect wordt naar beneden bijgesteld.

5. Afkortingen

Afkorting	Betekenis
(e)SIM	(Embedded) Subscriber Identity Module
APN	Access Point Name
BIO	Baseline Informatiebeveiliging Overheid
CPE	Customer Provider Edge
CSIR	CyberSecurity ImplementatieRichtlijn
DAP	Dossier Afspraken en Procedures
DFA	Dossier Financiele Afspraken
FW	Firewall
HHD	Hoog Heemraadschap Delfland
IoT	Internet of Things
MAB	MAC Authentication Bypass
MAC(-address)	Media Access Control (address)
MSP	Managed Service Provider
NCSC	Nationaal Cyber Security Centrum
PEP	Policy Enforcement Point
PoC	Proof of Concept
RSRP (dBm)	Reference Signal Received Power
RSRQ (dB)	Reference Signal Received Quality
RSSI (dBm)	Received Signal Strength Indicator
RTO	Return Time Object
SINR	Signal to Interference-plus-Noise Ratio
SLA	Service Level Agreement
SNR	Signal to Noise Ratio
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network
WK	WaterKeten
WS	WaterSysteem
WV	Waterveiligheid
TTA	Things of TA (interne IoT netwerk)

6. Bijlagen

6.1. CSIR

https://www.cert-wm.nl/csir
https://www.cert-wm.nl/documenten-marktpartijen
https://cuatro.sim-cdn.nl/certwm/uploads/csir-3.4-definitief-concept-20210914.pdf?cb=eKtH4fdi

6.2. BIO-2

https://www.bio-overheid.nl/category/producten/bio
https://www.bio-overheid.nl/media/cs5ctudu/20250924-baseline-informatiebeveiliging-overheid-2-bio2-v12-def.pdf

6.3. NCSC – TLS

https://www.ncsc.nl/cybersecurity-themas

6.4.

https://www.ncsc.nl/transport-layer-security

6.5. Wbni

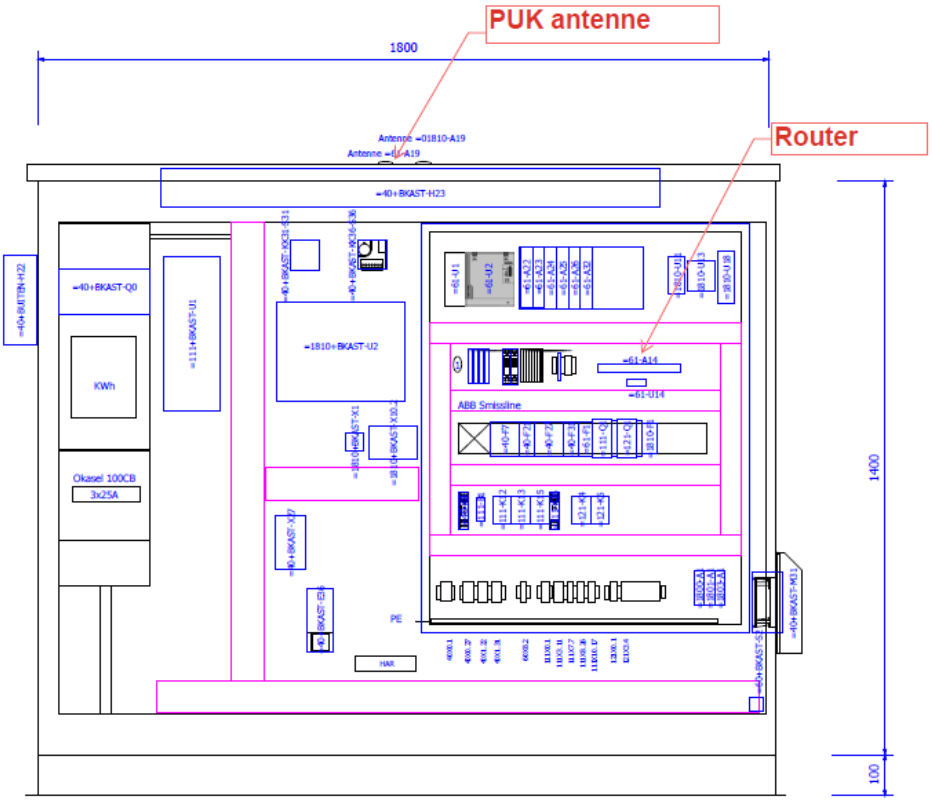
https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners

6.6. NIS2

https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555

6.7. Binnenkast

6.8. Buitenkast



7. Referenties