Aanbesteding batterij opslagsysteem BAT Tilburg

Programma van Eisen

Datum: 27-03-2024

Inhoudsopgave

Programma van Eisen

1.1 Organisatie

Eisnummer	Omschrijving eis
E.1.1	Opdrachtnemer wijst een vaste contactpersoon en een 1e vervanger aan voor het BAT.
E.1.2	De specificaties van de locatie, lay-out/routering, gebruikte voertuigen, netaansluiting en laadobjecten, foto's/beeldmateriaal e.d. van de locatie zijn opgenomen in de bijlagen. Hier kunnen geen rechten aan worden ontleend en deze zijn informatief & indicatief. Inschrijver dient zijn inschrijving mede op dit PVE en bijlagen te baseren.
E.1.3	Opdrachtnemer is verantwoordelijk voor het gehele proces tussen opdracht en oplevering. Hieronder valt onder andere, maar niet gelimiteerd tot: het verzorgen van de benodigde vergunningen en/of meldingen (inclusief plaatsing keerwand, zie E.6.3), de schouw van de locatie, het vermelden van de nieuwe kabels in de KLIC. Inclusief noodzakelijk beheer en onderhoud.
E.1.4	De Opdrachtnemer is verantwoordelijk voor opruim- en herstelwerkzaamheden aan de omgeving na het plaatsen van de (eventuele) fundering en het batterijopslagsysteem.
E.1.5	De Opdrachtnemer toont aan dat het batterijopslagsysteem voldoet aan alle eisen, inclusief installatie, door middel van een opleverdocument alsmede productbladen/specificaties en een FAT en SAT.
E.1.6	De Opdrachtnemer draagt de integrale verantwoordelijkheid voor de coördinatie en afstemming met BAT (Bouw- en Aanlegteam) en, indien nodig, met Enexis, Fudura, Kenter, Maxem (EMS) en de installatieverantwoordelijke. Daarnaast dient de Opdrachtnemer alle andere relevante partijen te betrekken bij het proces.

1.2 Voorwaarden batterij garantie

Eisnummer	Omschrijving eis
E.2.1	De levensduur van het batterijopslagsysteem bedraagt ten minste 15 jaar.
E.2.2	De systeemgarantie, aangeboden door de opdrachtnemer in samenwerking met de leverancier, bedraagt 10 jaar. Dit omvat de garantie op alle onderdelen van het systeem, vanaf het moment van ingebruikname.
E.2.3	Het batterijopslagsysteem heeft een capaciteitsgarantie van 120 maanden of 6.000 cycli bij een ontlading van 90% (DOD).
E.2.4	Bij het bereiken van het einde van de levensduur (EOL) heeft de batterij nog steeds een minimale State of Health (SOH) van 70%, bij een temperatuur van 20 graden Celsius.
E.2.5	Mocht het batterijopslagsysteem gedurende de periode van 10 jaar onder het state of health niveau van 70% dalen (SoH), dan dient opdrachtnemer maatregelen en/of herstelwerkzaamheden uit te voeren zodat de minimale capaciteit weer op het gestelde niveau zit. Aan het einde van ieder kalender jaar, moet door opdrachtnemer het SOH aangetoond worden en gedeeld met opdrachtgever.

1.3 Fysieke batterij

Eisnummer	Omschrijving eis
E.3.1	De batterij moet voldoen aan de volgende normen Elektrische installatie: NEN1010, NEN3140. Veiligheid: PGS37-1, IEC-62477, IEC-62485, IEC-61000-6-2, IEC 9100-6-4, IEC 62619. Bescherming: IEC 60529. Overige: NEN-50549-1, NEN-50549-2
E.3.2	De hoogte van de batterij is maximaal 3 meter.
E.3.3	Bij een afstand van 1 meter produceert de batterij een geluidsniveau van maximaal 65 dB(A).
E.3.4	De batterij moet worden geaard via de netaansluiting of met eigen aarding. Aangesloten op bestaande kabels en leidingen.
E.3.5	De batterij dient te worden geplaatst binnen een gebied van 16 m^2. Zie paarse arcering in bijlage 2. De exacte locatie wordt in afstemming met de opdrachtgever bepaald.
E.3.6	De opdrachtnemer levert en plaatst aanrijbeveiliging conform EU norm NEN-EN 1317-2 of vergelijkbaar. Exact ontwerp van aanrijbeveiliging dient te worden vastgesteld in samenspraak met de opdrachtgever.

1.4 Functionaliteiten batterij opslagsysteem

Eisnummer	Omschrijving eis
E.4.1	Het geplaatste batterijopslagsysteem moet een nominale capaciteit van minimaal 1.200 kWh hebben. Deze capaciteit mag modulair worden opgebouwd.
E.4.2	Bij ontlading moet de omvormer een capaciteit van minimaal 500 kVA hebben, terwijl bij opname een capaciteit van minimaal 200 kVA vereist is.
E.4.3	De omvormer dient vloeistofgekoeld te zijn.
E.4.4	De C-waarde van het batterijopslagsysteem moet altijd voldoende zijn om de omvormercapaciteit te ondersteunen.
E.4.5	De batterij dient te werken met de kobaltvrije lithium-ijzerfosfaat (LFP of LiFePO4) batterijtechnologie.
E.4.6	De effectieve capaciteit van de batterij bij het begin van zijn levensduur (BoL) moet ten minste 900 kWh bedragen, rekening houdend met een diepte ontlading (DOD) van 90%.
E.4.7	De batterij is voorzien van peakshaving software.

1.5 Dataverbindingen en back-up

Eisnummer	Omschrijving eis
E.5.1	Het is vereist dat de batterij een bedrade dataverbinding (airgapped van het BAT-netwerk) heeft en tevens in staat is om via een 4G/5G-simkaart verbinding te maken.
E.5.2	De opdrachtnemer dient een telecomprovider te kiezen en is verantwoordelijk voor het opzetten en onderhouden van een correcte en veilige datacommunicatieverbinding. ;

E.5.3	Bij verlies van de communicatieverbinding onderneemt de batterij actieve herstelpogingen, zoals het resetten van het modem. Zolang er geen verbinding is, blijft de batterij deze herstelacties herhalen.

1.6 Locatie batterij

Eisnummer	Omschrijving eis
E.6.1	De batterij wordt geplaatst op het huidige perceel van de gemeente Tilburg, afdeling BAT, gelegen aan de Ceramstraat 6 te Tilburg. Eventuele civiele werkzaamheden en andere activiteiten die voortvloeien uit deze aanbesteding moeten ook binnen dit bestaande perceel plaatsvinden. Uitbreiding van het perceel is niet toegestaan.
E.6.2	De indicatieve inrichting en locatie van het te plaatsen batterijopslagsysteem zijn vastgelegd in bijlage 2. Deze keuzes zijn gebaseerd op de specificaties van de locatie, de lay-out, de routering, de gebruikte voertuigen, de netaansluiting en de ingeschatte laadobjecten en vermogensvraag. Het is belangrijk op te merken dat hieraan geen rechten kunnen worden ontleend.
E.6.3	Bij de installatie van de batterij moet rekening worden gehouden met een minimale afstand van 1,5 meter tot de keerwand die op de erfgrens staat. De keerwand (Legioblokken) wordt door de opdrachtgever geplaatst.

1.7 Installatie en plaatsing

1.7.1 Specificatie

Eisnummer	Omschrijving eis
E.7.1.1	Voor de plaatsing van de batterij kan de opdrachtnemer gebruikmaken van de aansluiting van BAT. De energiekosten worden echter niet verrekend met de opdrachtnemer. Betreft ‘bouwstroom’
E.7.1.2	Na verstrekken van de opdracht (definitieve gunning) moet het batterijopslagsysteem binnen 30 weken in werking zijn (werkend opgeleverd) inclusief inregelen en integratie met het Maxem EMS.
E.7.1.3	Bouwplaats ruimte beperkt tot bijlage, doorgang en werkvak beperkt.

1.7.2 Bekabeling en data

Eisnummer	Omschrijving eis
E.7.2.1	T.a.v het plaatsingsvlak zijn mantelbuizen opgenomen. Zie bijlage 6 voor positie van de mantelbuizen. Opdrachtnemer is verantwoordelijk voor het aansluiten van de BESS en toepassing van de juiste kabels en dikte van deze kabels. Hiervoor zal een stelpost opgenomen worden van **25.000 euro.** Dit is begroot voor het inkopen van de juiste kabels, het aanleggen, de benodigde lan bekabeling en overige noodzakelijke bekabeling. Deze kabels doorvoeren door de bestaande mantelbuizen. Het 2 zijdig aansluiten en herbestratings of kleine herstelwerkzaamheden die voortvloeien uit het aansluiten en doorvoeren van de kabels door de mantelbuizen. De stelpost omvat ook de bestratingswerkzaamheden rond de nieuw te plaatsen BESS.
E.7.2.2	Alle bekabeling buiten het gebouw dient te worden beveiligd met overspanningsbeveiliging en afgedekt met beschermband om graafschades te voorkomen. Bovendien moeten alle kabels gelabeld en gecodeerd zijn. De installatie van kabelgoten en doorvoeringen moet voldoen aan de norm OVS 61401.

E.7.2.3	Datakabels die naast voedingskabels worden gelegd, moeten een isolatiewaarde hebben die geschikt is voor de hoogst mogelijke optredende spanning in het kabeltracé.

1.8 Applicaties & security

Eisnummer	Omschrijving eis
E.8.1	Cyber security dient te voldoen aan het normenkader van de Baseline Informatiebeveiliging Overheid (BIO). Zie bijlage 9. Ook dient cyber security te voldoen aan Cloud computing Eisen en wensen. Zie bijlage 10. Eisen uit bijlage 9 gaan voor eisen uit bijlage 10.
E.8.2	De opdrachtgever is eigenaar van alle gegenereerde data.
E.8.3	De batterij en het BMS moeten kunnen communiceren met het Maxem EMS via Modbus TCP/IP. Kosten voor implementatie en integratie met het Maxem EMS zijn voor opdrachtnemer. Ook dient implementatie en intergratie binnen de oplevertermijn (zie E.7.1.2) afgerond te zijn.
E.8.4	De batterij is uitgerust met MID-gecertificeerde meters en communicatieprotocollen die voldoen richting HBE administrateur. Zie bijlage 7 voor MID-meters compatibel met MAXEM.

1.9 Brandveiligheid

Eisnummer	Omschrijving eis
E.9.1	De batterij voldoet aan de meest recente PGS-37-1 richtlijnen voor batterij opslagsystemen. Uitgangspunt uit de PGS-37-1 richtlijn is M9 brandwerendheid. M50 kan ivm het plaatsingsvlak niet worden toegepast.
E.9.2	Opdrachtnemer wordt geacht proactief met verzekeraar, opdrachtgever en brandweer af te stemmen en hiertoe indien nodig aanvullende mitigerende maatregelen in te passen als bevoegd gezag en/of verzekeraar hierom verzoekt.

1.10 Storingsdienst en preventief onderhoud

Eisnummer	Omschrijving eis
E.10.1	Meldingen kunnen op werkdagen worden doorgegeven aan verantwoordelijke opdrachtnemer en/of middels het EMS platform van Maxem.
E.10.2	Binnen een termijn van 1 werkdag dienen storingen onder te worden verholpen.
E.10.3	Alle geplande werkzaamheden moeten binnen de vastgestelde werkzame uren van 7:00 tot 17:00 worden uitgevoerd.
E.10.4	Opdrachtnemer is verantwoordelijk voor het opstellen van een onderhoudsovereenkomst die voorziet in het noodzakelijk preventief en regulier onderhoud voor het geleverde systeem. Hierbij is een onderhoudstermijn van 5+5+5 jaar van toepassing. Na iedere 5 jaar volgt een evaluatie moment. Hiertoe is maximaal 75.000 euro begroot (exclusief geoorloofde jaarlijkse indexatie conform CAO-Loonindex CBS ten gunste van opdrachtnemer).

1.11 Duurzaamheid

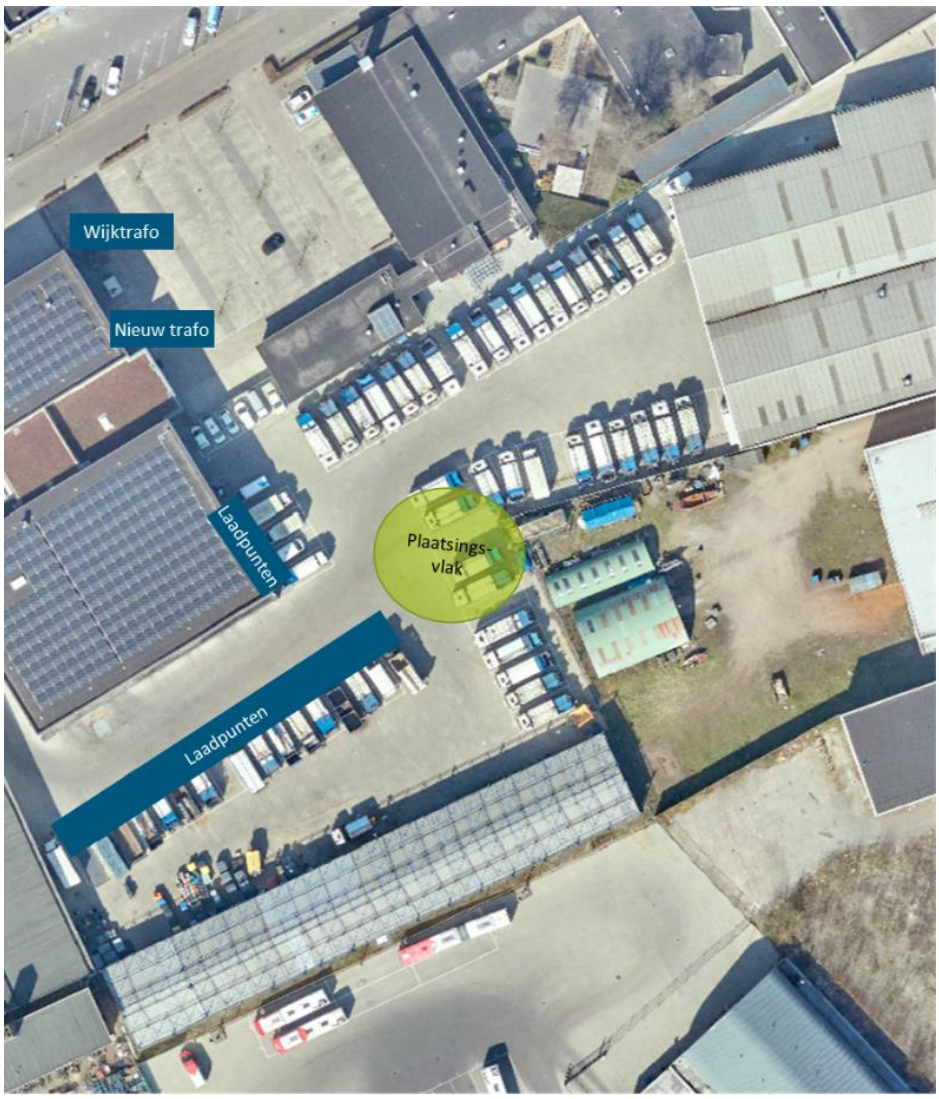
Eisnummer	Omschrijving eis
E.11.1	Het is verplicht dat de grondstoffen die worden gebruikt voor de productie van batterijen een duidelijke herkomstcertificatie hebben.
E.11.2	De opdrachtnemer verstrekt heldere informatie over hoe de End of Life-fase kan worden aangepakt, inclusief de benodigde stappen en verantwoordelijkheden.

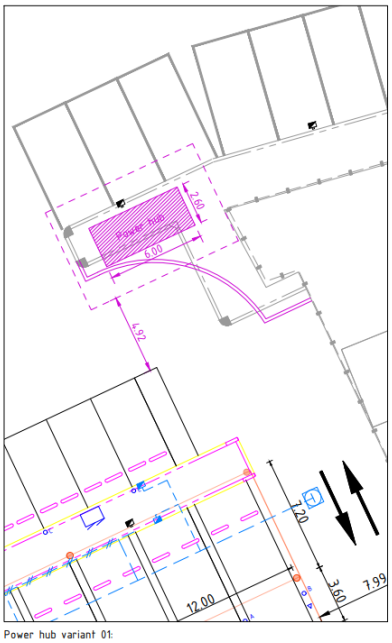
BIJLAGEN

Bijlage 1: Begrippenlijst

BAT	Brabants Afval Team, afdeling Gemeente Tilburg, Opdrachtgever.(OG)
BESS	Batterij-energieopslagsysteem
BOL	Begin of Life
BMS	Battery Management System
DC High Power	Laadpunten met een laadvermogen van minimaal 350 kW
DOD	Depth of Discharge
EMS	Energie Management Systeem
EOL	End of Life
EOS	Elektriciteit Opslag Systeem
FAT	Factory Acceptance Test (fabrieksafname)
HBE	Hernieuwbare Brandstof Eenheden
KLIC	Kabels en Leidingen Informatie Centrum
Laadobject	Fysiek object met meestal één of meerdere laadpunten.
Laadinfrastructuur	Het totaal van de infrastructuur behorend bij de laadpalen. Onder andere: hoofdaansluiting, laadpaal, laadpunt en bekabeling.
Laadpunt	De elektrische aansluiting op een laadobject waar de stekker wordt aangesloten. Een laadpunt kan meerdere connectoren bevatten, zodat verschillende typen stekkers gebruikt kunnen worden. Ondanks die meerdere connectoren, kan er maar één auto per laadpunt laden.
LCA	Levenscyclusanalyse
Load Balancing	Zorgt ervoor dat op paalniveau de beschikbare capaciteit (bijvoorbeeld 22kW) verdeeld wordt over twee ladende EV's. Hoe die verdeeld wordt is afhankelijk van respectievelijke laadsnelheden van de EV's. De sturing vindt plaats in de laadpaal.
MID	Measuring Instrument Directe
PV-systemen	Fotovoltaïsche installaties
SAT	Site Acceptance Test
Smart Charging	Smart charging of slim laden is een brede term, die wordt gebruikt om aan te duiden dat slimme technieken de laadtransactie op afstand kunnen aansturen. Minimaal betekent dit dat het opladen van elektrische auto's op het meest optimale moment gebeurt, wanneer bijvoorbeeld de kosten laag zijn en het aanbod van (duurzame) energie hoog.
SOH	State of Health

Bijlage 2: Bovenaanzicht BAT bedrijfsterrein





Power hub variant 01:

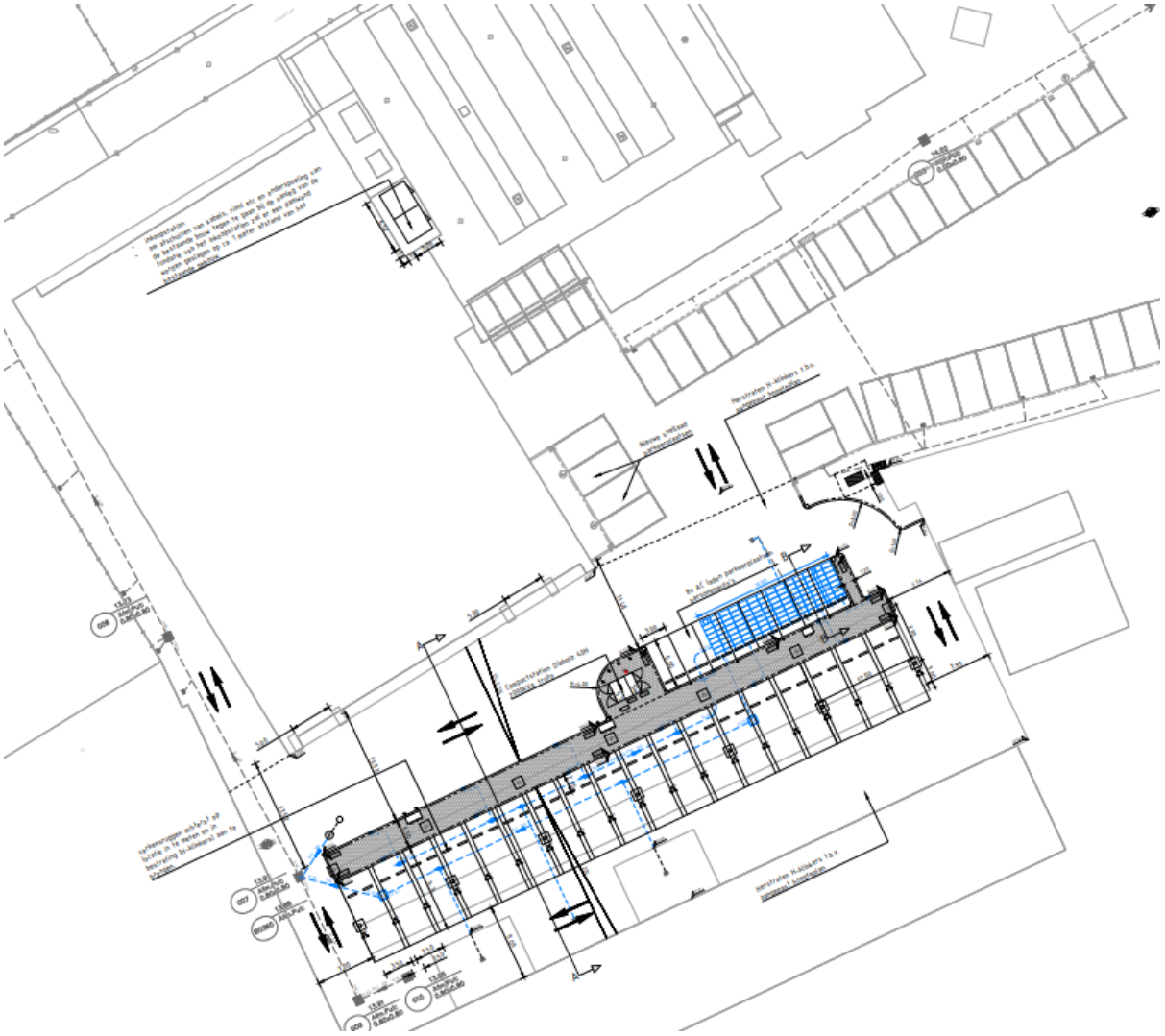
Bijlage 3: Overzicht wagenpark

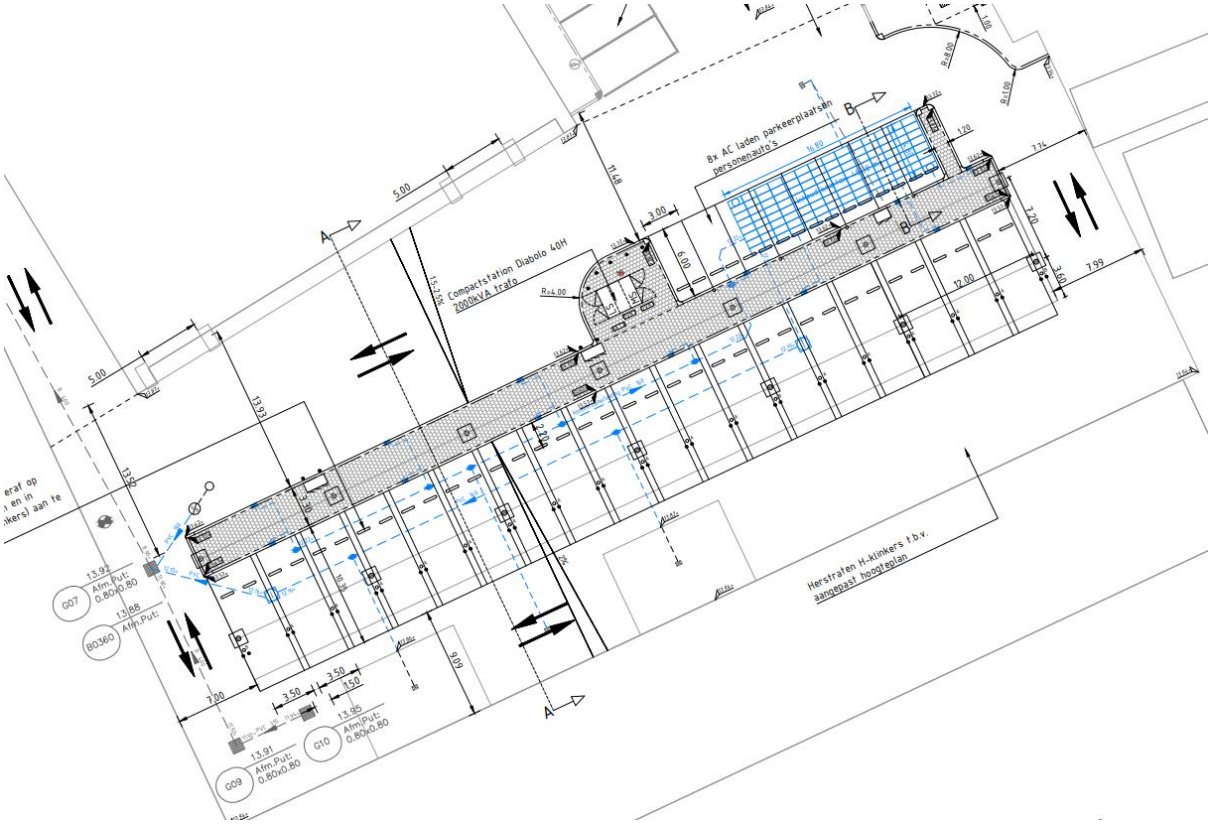
Park	type belading	Omschrijving	Eerste jaar elektrisch	chassistype
723	bestelauto	Nissan E-NV200	2015	E-NV-200
724	bestelauto	Nissan E-NV200	2015	E-NV-200
121	achterlader	daf/geesink	2021	75
	personenauto KR	via wagenparkbeheer	2021	up
	personenauto Davor	via wagenparkbeheer	2021	up
265	achterlader	scania/geesink/welvaarts/ctrace	2022	
266	achterlader	scania/geesink/welvaarts/ctrace	2022	
798	bakwagen		2022	scania
122	achterlader	Daf/geesink/ctrace	2023	75
123	achterlader	mercedes/geesink	2023	ECONIC 2629
189	duo belading	daf/haller/terberg	2023	FAG CF75
190	duo belading	daf/haller/terberg	2023	FAG CF75
191	duo belading	daf/haller/terberg	2023	FAG CF75
192	duo belading	daf/haller/terberg	2023	FAG CF75
400	kraaninzameling	scania/geesink/hmf/welvaarts	2023	P 280 B 6X2/4
405	kraaninzameling	Daf VDL kraantrechter	2023	
720	bus	Fiat Ducato	2023	Ducato
133	achterlader	DAFLF/Geesink/ctrace	2024	LF260
134	achterlader	DAFCF/Geesink/Ctrace	2024	CF290FAG
193	duo belading	scania/haller/terberg	2024	Lowliner
194	duo belading	scania/haller/terberg	2024	Lowliner
401	kraaninzameling	Volvo FM/ AJK/HMF/welvaart	2024	FM 8x2
402	kraaninzameling	Volvo FM/ AJK/HMF/welvaart	2024	FM 8x2
799	bus		2024	werkplaats
700	bus		2024	wasunit
	personenauto ipv 718-719	via wagenparkbeheer	2024	
	personenauto ipv 726	via wagenparkbeheer	2024	
	personenauto ipv 727	via wagenparkbeheer	2024	
	personenauto ipv 725	via wagenparkbeheer	2024	
195	duo belading	daf/Haller/Zoeller	2025	FAG CF75
	groei		2025	

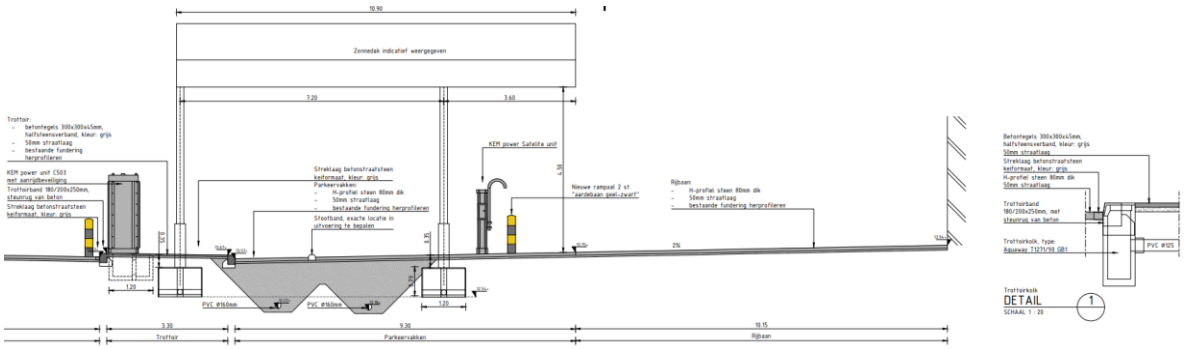
Bijlage 4: Beschrijving van bestaande assets

- 16 DC satellieten kempower (+- 50 kw)
- 3 DC satellieten kempower (+- 350 kw)
- Flexicharge ac palen (8 laadpunten, 4 dubbele laadpalen 22 kw)
- 2 sets zonnepanelen (carport en werkplaats) +- 350 KWP
- Raption 150 lader (2x 75 KW)

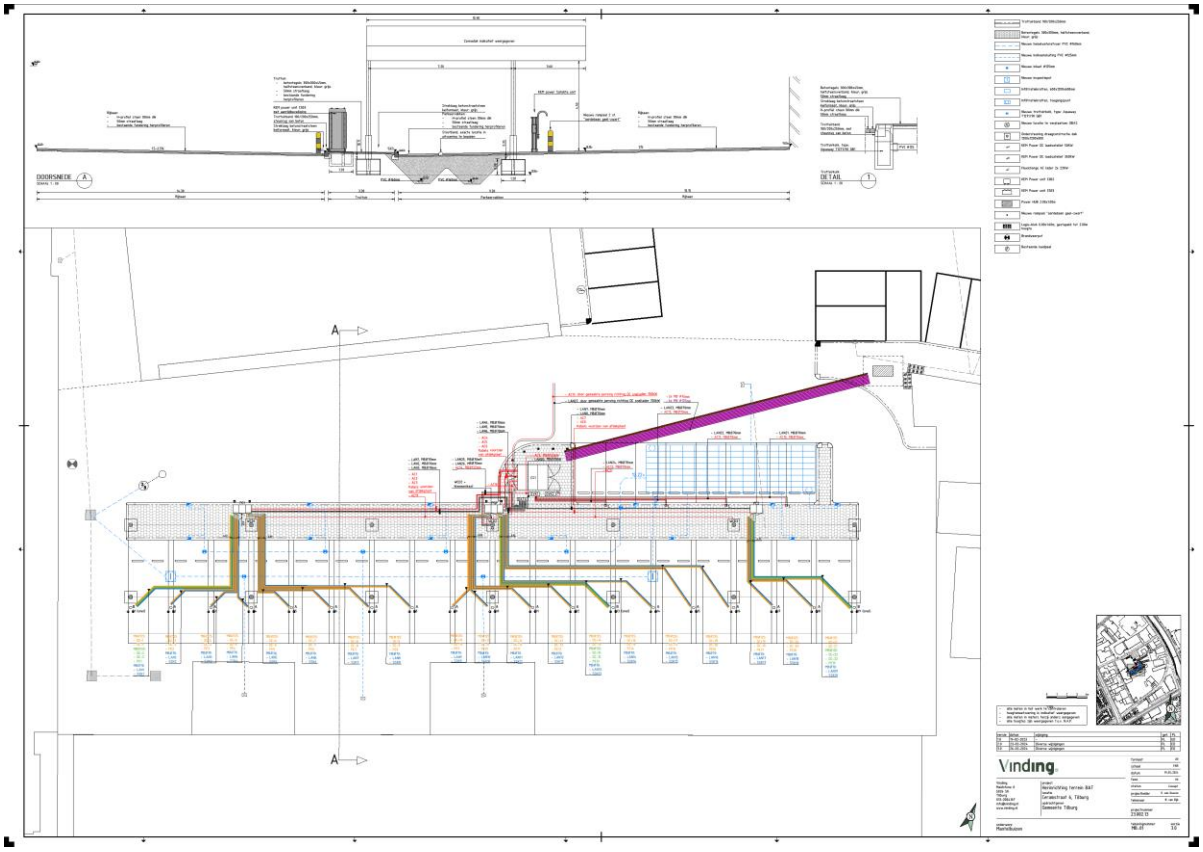
Bijlage 5: Lay-out, routering en nieuwe situatieschets

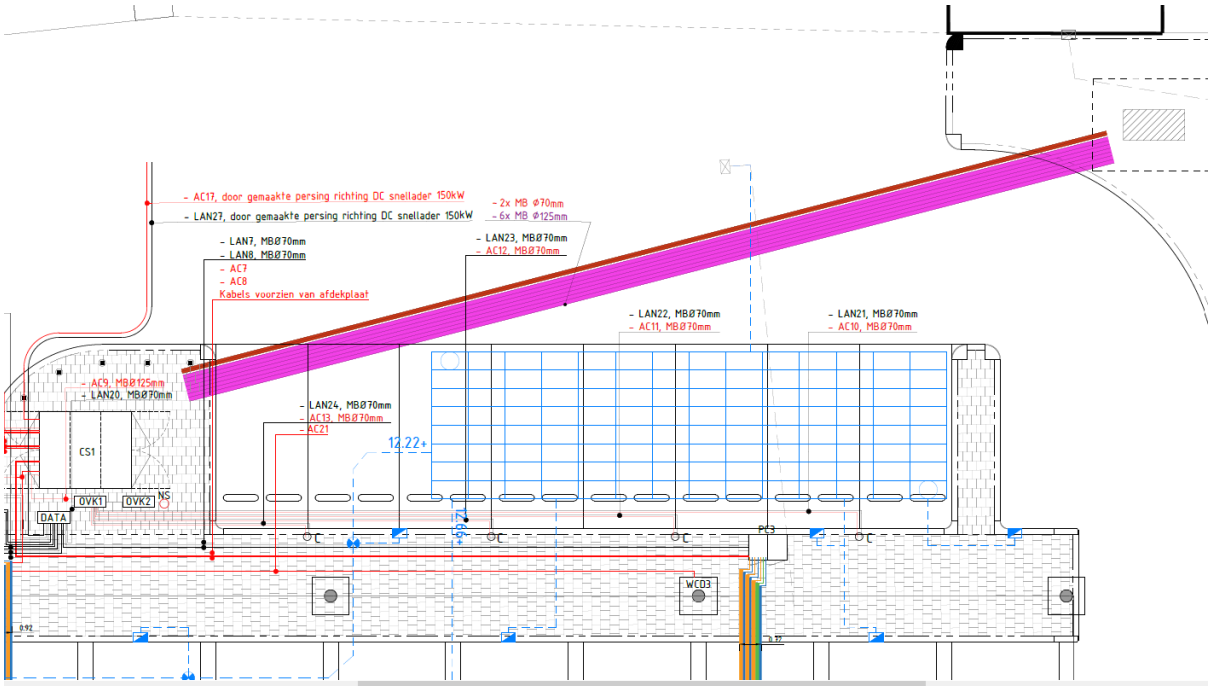



8x AC laden parkeerplaatsen personenauto's
Compactstation Diabolo 40H 200kVA trafo
Herstraten H-klinkers t.b.v. aangepast hoogteplan
G07
G10
G09
BO360
Afm.Put: 0.80x0.80


Zonnedak indicatief weergegeven
KEM power Satelite unit
Nieuwe rampaal 2 st. "aardebaan geel-zwart"
Trottoir
Parkeervakken
Rijbaan
DETAIL
SCHAAL 1 : 20

Bijlage 6: Mantelbuizen

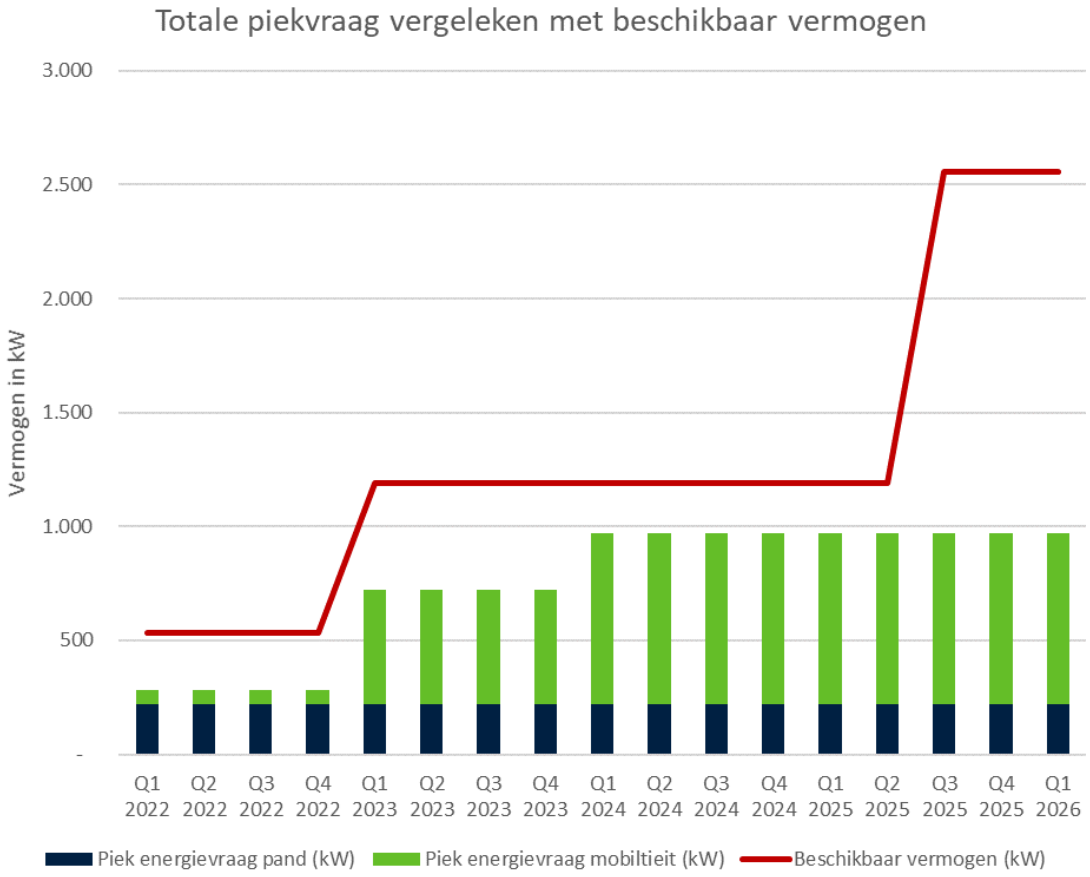


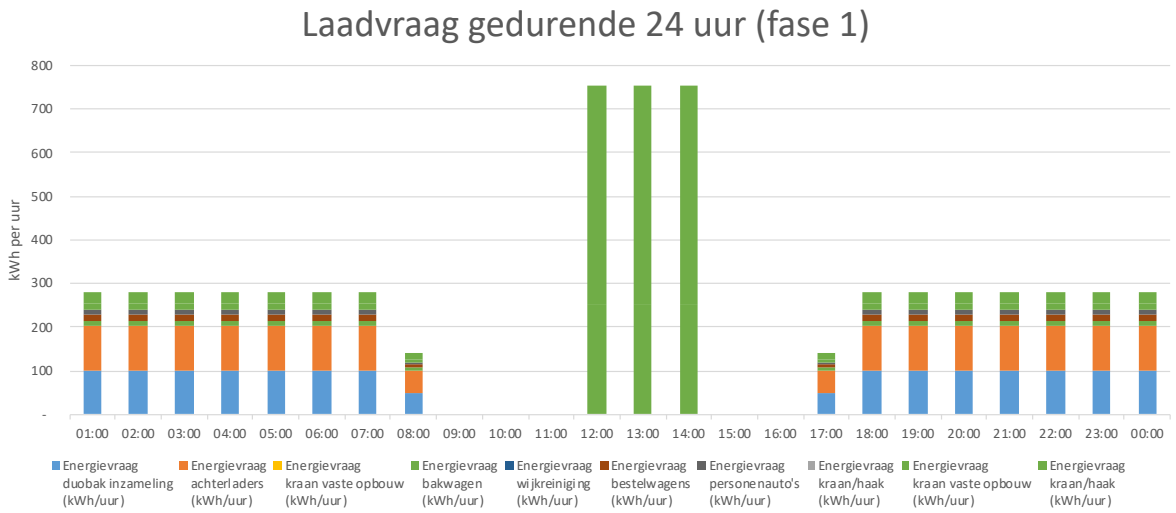


Bijlage 7: MID meters

	Manufacturer	**Type**
1	ABB	B23 112-10P
2	ABB	B24 112-100
3	ABB	A43 112-100
4	Controlin	SKD-005-M
5	Hager	ECR300C
6	Hager	ECR310D
7	Hager	ECR380D
8	Inepro	PRO380
9	Xemex	P1MB
10	Schneider Electric	PowerLogic PM5111
11	Sineax	DM5S

Bijlage 8: Netaansluiting en beschikbare vermogens





Bijlage 9: Kaders en normen beveiliging voor Industriële Automatisering

Voor overheden is de Baseline Informatiebeveiliging Overheid (BIO) de standaard.
Voor Industriële Automatisering is de functie van het object/systeem en de betrouwbaarheid van belang. Deze betrouwbaarheid en werking van apparatuur is niet concreet in de BIO geregeld en vraagt aanvullende normen.

De Europese standaard voor beveiliging van Industriële Automatisering is beschreven in de IEC 62443.

In de praktijk worden vaak de datanetwerken van de Kantoorautomatisering (KA) met die van Industriële Automatisering vervlecht. Een zuivere scheidslijn is dan ook niet meer te trekken tussen de KA en die van de Industriële Automatisering. De Industriële Automatisering wordt ook nog eens vaak vanuit een KA omgeving aangestuurd en/of beheerd en onderhouden waar de BIO verplicht is en waarop aanvullende controls en maatregelen nodig zijn voor de Industriële Automatisering.

Definities:

In onderstaande tabel worden een aantal afkortingen gebruikt. Hieronder worden de definities van deze afkortingen beschreven:

De afkorting ICS staat voor Industrial Control Systems of industriële controlesystemen.

Het gaat om meet- en regelsystemen die voor de aansturing van industriële processen of gebouwbeheersystemen worden gebruikt.

De afkorting SCADA staat voor Supervisory Control And Data Acquisition.
Het gaat om verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van systemen.

Categorie	Nr.	Omschrijving
Algemeen	AL1	Objectbeheerder dient 3 jaarlijks de opzet, het bestaan en de werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan de objecteigenaar en het Cybersecurity Beveiligingsplan bijgewerkt en voorgelegd te worden aan de objecteigenaar.
Fysiek Toegangsbeheer	FT1	Beschrijf de bouwkundige maatregelen met betrekking tot fysieke toegang. De volgende onderdelen komen hierin aan bod: Is er een sluitplan aanwezig? Wat is de mate van inbraakwerendheid in minuten?

		Is er een inbraaksignaleringssysteem aanwezig? Hoe is alarmopvolging ingericht (termijnen, middelen, interventie)? Is er een logboek voor de beveiligingsinstallatie aanwezig? Hoe zijn faciliteiten afgeschermd voor onbevoegden?
Logische Toegangsbeveiliging	LT1	De toegang voor de bedienaars en beheerders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend plaatsvindt, rol gebaseerd en op basis van het 'need to have' en 'segregation of duties' principe;
	LT2	De toegang voor de bedienaars en beheerders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend plaatsvindt, rol gebaseerd en op basis van het 'need to have' en 'segregation of duties' principe;
	LT3	De toegangsrechten van alle gebruikers dienen minimaal eenmaal per halfjaar te worden beoordeeld en geactualiseerd in een formeel proces. Opvolging van de bevindingen is gedocumenteerd en wordt behandeld als een beveiligingsincident.
	LT4	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik te worden gemaakt van de door de objecteigenaar beschikbaar gestelde diensten of goedgekeurde inrichting.
	LT5	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA-gegevens in principe in versleutelde vorm worden uitgewisseld en opgeslagen.
	LT6	Voor bedienaars, beheerders, software processen en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon, software proces of systeem.
	LT7	Standaard wachtwoorden moeten bij het in gebruik nemen van de systemen gewijzigd worden.
	LT8	Wanneer systemen met generieke accounts werken moet deze strikte uitzondering worden gemotiveerd, vastgelegd en de risico's in beeld gebracht.
	LT9	De logische toegang dient als volgt te worden ingevuld: a. Lokaal bediening – minimaal een user-ID en wachtwoord combinatie; Indien mogelijk twee factor authenticatie. b. Lokaal beheer en administrator accounts twee factor authenticatie ; c. Remote toegang voor beheer en onderhoud uitsluitend via een goedgekeurde centrale beveiligde voorzieningen.

Beveiligingsincidenten	BI1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel (zowel intern als extern) beveiligingsincidenten en zwakke plekken in de beveiliging zo snel mogelijk melden.
	BI2	Verantwoordelijkheden voor Cybersecurity zijn vastgesteld en gedeeld met de opdrachtgever.
	BI3	Indien het control systeem niet meer normaal kan functioneren als gevolg van een aanval, dient het control system naar een vooraf gedefinieerde veilige situatie te schakelen (bijvoorbeeld: unpowered, hold of fixed).
	BI4	Het ICS/SCADA systeem dient na onderbreking of falen terug te kunnen keren naar een bekende veilige staat.
	BI5	Het ICS/SCADA systeem en de bediening dienen te kunnen schakelen naar en van de geïnstalleerde noodstroomvoorziening zonder dat dit invloed heeft op de beveiligingsstatus van het object.
	BI6	In geval van een DOS-aanval dient het ICS/SCADA systeem in een beperkte modus te kunnen functioneren.
Verbindingen	VB1	Objectbeheerder draagt zorg voor en ziet erop toe dat alle datanetwerkverbindingen van het lokale objectnetwerk met het overkoepelende netwerk van de objecteigenaar strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten conform de aansluitvoorwaarden van de objecteigenaar. Toegang tot het systeem verloopt via de netwerken van de objecteigenaar.
	VB2	Gestreefd moet worden naar maximale inzichtelijkheid van de datanetwerkkoppelingen van de objecten. Alle datanetwerkkoppelingen dienen in kaart te worden gebracht, zodat altijd duidelijk is via welk datanetwerkpad een actor (uiteindelijk) een object zou kunnen binnendringen, beginnend vanuit het internet.
	VB2	Communicatie en functies van safety systemen zijn afgeschermd van overige communicatie.
CMDB	CM1	Objectbeheerder draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectdatanetwerken door middel van een Configuration Management Database (CMDB).
Systeem	SY1	De klokken van alle relevante informatie verwerkende systemen binnen een object behoren te worden gesynchroniseerd met één hiertoe aangewezen **centrale** referentietijdbron.
Netwerkkoppelingen en Cryptografie	NC1	Bij gebruik van cryptografie dient te worden gekozen voor cryptografische toepassingen die voldoen aan passende standaarden en is dit gedocumenteerd.

	NC2	Bij inzet van versleuteling (cryptografie) dient de gekozen versleuteling en de onderliggende algoritmes en instellingen uitsluitend de duiding “goed” te hebben zoals aangegeven in de meest actuele versie van het NCSC document “Richtlijnen voor Transport Layer Security”.
	NC3	Indien het configureren van de IA/PA/OT systemen op afstand plaatsvindt, dan dient dit over beveiligde verbindingen plaats te vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient daarbij vermeden te worden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring het onveilige communicatieprotocol worden ingezet, mits er een additioneel versleuteld kanaal wordt toegepast (SSL, TLS, IPSEC etc.). De gekozen versleuteling en de onderliggende algoritmes en instellingen dienen dan uitsluitend de duiding “goed” te hebben zoals aangegeven in de meest actuele versie van het NCSC document “Richtlijnen voor Transport Layer Security”.
Anti-malware	AM1	Er dienen een geborgde procedures en voorzieningen te zijn voor detectie van en preventie tegen malware.
	AM3	Antimalware voorzieningen moeten worden ingezet, waarbij aantoonbaar kan worden gemaakt dat de antimalware software correct is geïnstalleerd en geconfigureerd. De juiste werking dient hierbij te kunnen worden aangetoond.
	AM3	De anti-malware voorzieningen mogen geen invloed hebben op de werking en functionaliteit van in gebruik zijnde ICS/SCADA en ICT-systemen.
Hardening	HA1	ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen zijn gehardened. Dit is een onderdelen van het Security by Design principe.
	HA2	Minimale hardening maatregelen zijn: a. niet noodzakelijke datanetwerkservices uit te zetten; b. het verwijderen (patchen) van bekende kwetsbaarheden; c. alle poorten die niet nodig zijn te deactiveren/blokkeren; d. alle default “access points” te verwijderen; e. de default accounts uit te schakelen conform het wachtwoord beleid Indien uitschakelen niet mogelijk is dient het wachtwoord te worden aangepast; f. indien beschikbaar gebruik te maken van de security opties van leveranciers.
	HA3	Indien mogelijk dienen ICS/SCADA-systemen zodanig te worden (her)geconfigureerd dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet is toegestaan. Ook dient het gebruik van mobiele code beperkt te worden, waarbij het uitvoeren van mobiele code niet is toegestaan, tenzij:

		a. de afkomst van de mobiele code op voldoende wijze is geauthentiseerd en geautoriseerd; b. het versturen van mobiele code naar/van de ICS/SCADA systemen is geblokkeerd.
Patching	PA1	Alle externe ICT-systemen die gekoppeld worden aan de interne ICT en IA systemen dienen voorzien te zijn van alle recente beveiligingsupdates en patches.
	PA2	Indien patches niet kunnen worden uitgevoerd, dient de afweging hiertoe schriftelijk te worden vastgelegd voorzien van een risicoafweging, inclusief een mitigatievoorstel.
	PA3	Er is een geborgde procedure waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.
	PA4	Indien zowel de kans op misbruik als de verwachte schade hoog zijn (volgens de NCSC-classificatie voor kwetsbaarheidswaarschuwingen), wordt de betreffende patch ingepland voor implementatie. In de tussentijd worden op basis van een expliciete risicoafweging tijdelijke mitigerende maatregelen getroffen.
	PA5	Het uitvoeren van patches mag de beschikbare systeemresources niet zodanig beperken dat de normale softwareprocessen op de ICS/SCADA systemen hiervan zichtbaar hinder ondervinden.
Logging en Monitoring	LO1	Er wordt zorg gedragen voor en op toegezien dat: a. de loggegevens worden weggeschreven en opgeslagen in een apart bestand, dat alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; b. de logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen worden beschermd tegen verlies of wijziging; c. op basis van een expliciete risicoafweging de bewaarperiode van de logbestanden (van alle systemen met logvoorziening) wordt bepaald. Deze bewaartermijn is altijd tenminste drie maanden; d. loggegevens die zijn gebruikt voor incidentonderzoeken, op aparte media buiten de IA veilig te worden gesteld welke langer worden bewaard conform de bewaartermijnen die de (feiten)onderzoekers aangeven; e. er een overzicht is van alle logbestanden die worden gegenereerd; f. een (onafhankelijke) interne audit procedure ten minste elke 6 maanden toetst op het ongewijzigd bestaan van de logbestanden; g. het oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens, zo snel mogelijk wordt gemeld als

		beveiligingsincident via de procedure voor beveiligingsincidenten.
	LO2	Logregels bevatten minimaal de volgende gegevens: a. de gebeurtenis zelf; b. Benodigde informatie om de actie te kunnen herleiden tot een natuurlijk persoon, b.v. gebruikersnaam of een (systeem)-ID; c. component waarop de handeling werd uitgevoerd; d. het resultaat van de handeling; e. de datum en het tijdstip van de gebeurtenis; f. een doorlopende en unieke nummering per logregel.
	LO3	Indien het object niet permanent op een Security Operations Centre is aangesloten dient medewerking te worden verleend voor het incidenteel kunnen uitlezen van het lokale object netwerkverkeer of een specifiek deelnetwerk van het object middels de analyse poorten.
	LO4	Er dient een operationeel proces te zijn als onderdeel van het incidentmanagementproces voor het melden van incidenten aan, en de response op meldingen van, het SOC.
	LO5	Er dient voldoende ruimte te zijn voor audit opslag (logging), en maatregelen zijn genomen die de kans beperken dat de beschikbare ruimte overschreden wordt. Er dient tijdig een waarschuwing te worden gegeven indien de opslagcapaciteit op dreigt te raken.
	LO6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de objectverantwoordelijke/-beheerder.
Maatregelen gecontroleerd wijzigen	MW1	Er is een geborgde procedure voor het (laten) inventariseren en registreren van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB). Deze CMDB dient actueel te worden gehouden.
	MW2	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke situatie en afwijkingen in de CMDB worden gecorrigeerd.
	MW3	Er is een geborgde wijzigingsprocedure voor het doorvoeren van wijzigingen aan ICS/SCADA, ondersteunende ICT-systemen, beveiligings- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via een reguliere wijzigingsprocedure te verlopen.

	MW4	Bij noodwijzigingen die buiten het reguliere wijzigingsproces om zijn doorgevoerd als gevolg van incidenten met een bijzonder (urgent) karakter worden achteraf alsnog de gebruikelijke procedures gevolgd en de CMDB administratie bijgewerkt.
Back-ups	BA1	Systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging. Wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd. Met deze back-up moet men in staat zijn middels een volledige roll-back naar de werkende situatie terug te kunnen gaan. Indien back-ups gedurende de operationele fase van een object gemaakt moeten worden, dan mag dit het operationele proces niet verstoren.
	BA2	Er zijn gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.
	BA3	Er dient een recoveryplan te zijn, waarin zijn opgenomen: alle nodige voorzieningen voor back-up en herstel, kopieën van gegevens en programmatuur, evenals benodigde herstelmaatregelen na een incident zoals b.v. een besmetting met malware.

Bijlage 10: Cloud computing Eisen en Wensen informatie Beveiliging

GEMEENTE TILBURG

Cloud Computing
Eisen en Wensen InformatieBeveiliging

v1.71

Versiebeheer

Versie	Datum	Auteur	Status/Wijzigingen
1.50	7/6/16	Marius van Oers	Vastgesteld tijdens het I-managers overleg van de afdeling POI (huidig DAT).
1.51	16/1/17	Marius van Oers	Actualisatie web richtlijnen
1.52	18/7/17	Marius van Oers	Safe Harbor→EU/VS Privacy Shield. TLS/DKIM/DMARC/DANE beveiligingsopties. IBD en NCSC beveiligingsrichtlijnen.
1.53	09/08/18	Marius van Oers	Actualisatie web richtlijnen
1.54	22/08/18	Marius van Oers	TLS vereisten per IBD/NCSC richtlijnen.
1.55	06/02/19	Marius van Oers	WBP→AVG/GDPR
1.56	17/07/19	Marius van Oers	Remote sessie & BIG→BIG/BIO
1.57	24/7/19	Marius van Oers	NCSC Beveiligingsrichtlijnen Webapplicaties
1.58	15/8/19	Marius van Oers	Actualisatie en verwijdering van niet relevante items.
1.59	3/10/19	Marius van Oers	Sync geheimhouding en verwerkersovereenkomst
1.60	6/2/20	Marius van Oers	Actualisatie, Weblinks , SSLLABS
1.61	3/6/20	Marius van Oers	Actualisatie, eisen overgenomen uit B5 meetings.
1.62	3/6/20	Marius van Oers	Flowchart, Full & Mini eisen
1.63	4/6/20	Marius van Oers	Opmerkingen Terence
1.64	8/6/20	Terence van Gestel	Opmerkingen Perry
1.65	21/7/20	Marius van Oers	EU/VS Privacy Shield →SCC
1.66	8/10/20	Marius van Oers	Verduidelijking flowchart
1.67	4/11/21	Marius van Oers	Tilburgse technische veiligheids en inrichtingseisen voor webtoepassingen.
1.68	1/12/21	Marius van Oers	Port forwarding
1.69	23/6/22	Marius van Oers	Web Expertise Team
1.70	10/11/22	Marius van Oers	MS Graph protocol
1.71	28/2/23	Marius van Oers	API Gateway

Versie	Datum	Auteur	Status/Wijzigingen

- Cloud Computing Eisen en Wensen InformatieBeveiliging

Definitie Cloud Computing: we spreken van Cloud computing als toepassingen ter beschikking worden gesteld door gebruik van internettechnologie.

Cloud Computing raakt alle maatregelen die de gemeente Tilburg zelf moeten nemen in de eigen infrastructuur. Deze maatregelen worden vervolgens gedeeld door de Cloud- leverancier en door de gemeente Tilburg uitgevoerd.

Indien de gemeente Tilburg gebruikt maakt van Cloud-diensten dan blijft de gemeente Tilburg verantwoordelijk voor de juiste beveiliging van haar gegevens.

1.1 Inleiding

Dit document is bedoeld om tijdens trajecten richting Cloud partijen/contractanten (ten behoeve van bijvoorbeeld SAAS, PAAS, IAAS oplossingen etc.) van de gemeente Tilburg Eisen en Wensen m.b.t. Informatiebeveiliging te communiceren.

De antwoorden worden gebruikt om de bestaande beveiligingssituatie te beoordelen en of deze voldoet aan de voor gemeente Tilburg geldende compliancy mbt informatiebeveiliging.

Het beantwoorden van alle vragen en het geven van toelichtingen is verplicht.

Het daadwerkelijk voldoen aan de Eisen is verplicht.

Sommige van de onderstaande eisen zijn afkomstig uit het IBD (Informatie Beveiligingsdienst voor gemeenten) document m.b.t. Cloud Computing.

De eisen zijn realistisch en haalbaar.

Indien er aan een of meerdere eisen niet wordt voldaan dan kan dat gelden als knock-out criteria.

Dit is een algemeen document. Het kan daardoor voorkomen dat een bepaalde eis niet van toepassing is. Geef dit aan met argumentatie.

Aan een eis moet men voldoen, aan een wens mag men voldoen.

Bij de wensen ligt de lat iets hoger dan bij de eisen en kunnen partijen het verschil maken indien zij aantoonbaar kunnen laten zien dat ze aan bepaalde wensen voldoen.

Voor elke niet behaalde wens wordt er 0 punt toegekend.

Voor een behaalde wens worden er de specifiek bepaalde punten toegekend.

De scores geven inzicht in mate van beveiliging en kunnen onder andere dienen als basis voor een objectieve selectie van leveranciers m.b.t. Informatiebeveiligingsaspecten.

2.0 Algemene zakelijke informatie van de Contractant

- Leverancier:

- Product/dienst naam:

- Korte functionele beschrijving van de dienst:

- Contactpersoon:
  Adres:

  Telefoon:

  E-mail:

- Websites/weblinks die mogelijk gebruikt gaan worden. Waar loggen eindgebruikers en beheerders op in. En indien er koppelingen worden gelegd ten behoeve van system/service accounts/api koppelingen etc geef deze ook aan.

    1. Weblink voor Eindgebruikers :

    2. Weblink voor Beheerders :

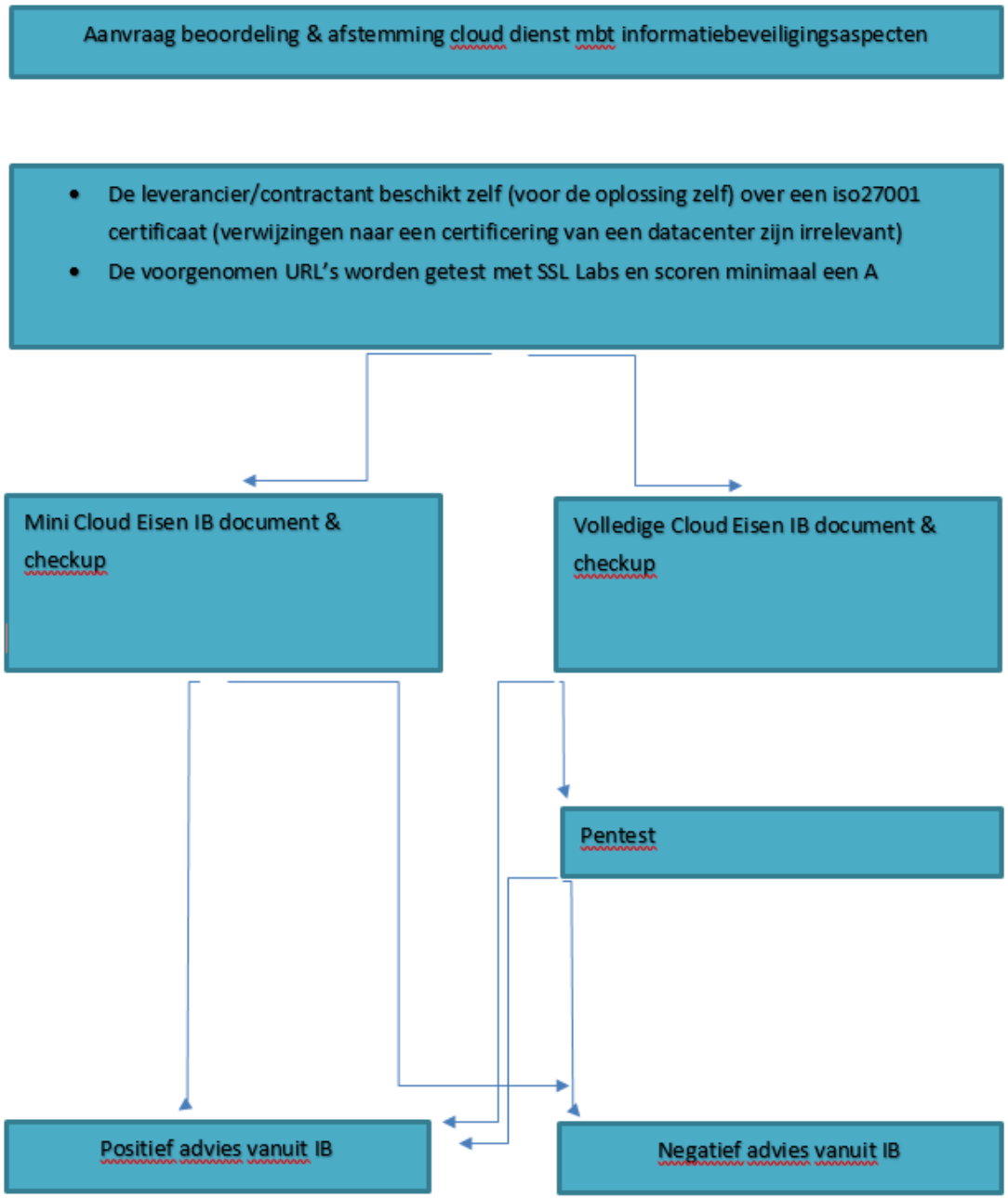
    3. Weblink voor System/Service accounts/api koppelingen etc :

- Heeft uw organisatie een ISO 27001/27002 verklaring van uw informatiebeveiliging?
  De onafhankelijk auditor dient te verklaren dat het systeem en de achterliggende processen voldoen. De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (in NL: Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud. Indien ja, dan ontvangen we graag een kopie hiervan.

2.1 Flowchart

Standaard worden de volledige eisen gesteld aan de Contractant (C – Full)
Als een leverancier zelf beschikt over een iso27001 certificaat en de voorgenomen url's een A score hebben op ssllabs dan hanteren we de mini eisen. (C-Mini)

We hanteren de volgende flowchart:



2.2 Eisen voor de Contractant

Om onderscheid te maken tussen eisen voor de contractant en interne (gemeente Tilburg) instructies zijn er kolommen toegevoegd:

C: Contractant (cloud leverancier)

T: gemeente Tilburg

Standaard worden de volledige eisen gesteld aan de Contractant (C – Full)
Als een leverancier zelf beschikt over een iso27001 certificaat en de voorgenomen url's een A score hebben op ssllabs dan hanteren we de mini eisen. (C-Mini)

	C Full	C Mini	T	Antwoord/toelichting door de contractant dat zij zich committeren aan de eis en voorzien van onderbouwing.
1. Gemeente Tilburg heeft het recht om audits te mogen (laten) uitvoeren over alle afspraken.	X	X	X	
2. De contractant/ hoofdaannemer moet ervoor zorgen dat eventuele onderaannemer(s) dezelfde waarborgen biedt bij de uitvoering van de overeenkomst als de hoofdaannemer. Rechten en plichten blijven bij de hoofdaannemer. Onderaannemer werkt uitsluitend onder verantwoordelijkheid van hoofdaannemer. Dit is ook op datahosting (via een andere partij) van toepassing	X	X		

3. Opdrachtnemer is gehouden tot geheimhouding van alle gegevens die zij verwerkt.	X	X		
4. Naleving van alle relevante wet- en regelgeving is verplicht.	X	X	X	
5. Autorisaties dienen transparant te zijn, er dient in 1 overzicht een duidelijke autorisatietabel met rollen/functies en bijbehorende rechten te zijn. Role Based Acces Control dient ingericht te zijn. (“RBAC”) Autorisaties zijn ingericht op basis van “need to know” : alleen personen die informatie nodig hebben voor het uitvoeren van hun werkzaamheden hebben toegang. Rechten dienen te worden toegekend volgens het “Least Priviliges” principe.	X	X	X	

6. Er dient strikte functiescheiding te zijn. Bijvoorbeeld voor een persoon die zowel een reguliere gebruiker is als beheerder. Beheer en Functioneel gebruik dient gescheiden te zijn.	X	X	X	
7. Er zijn maatregelen ingevoerd om de dreiging tegen te gaan dat informatie wordt misbruikt door uw personeel en (onder)aannemers. Bijvoorbeeld het ongeoorloofd inzien van diensten en gegevens dient voorkomen te worden.	X			
8. Er zijn maatregelen ingevoerd om het ten onrechte verstrekken van informatie aan onbevoegden te voorkomen.	X			
9. Met betrekking tot remote sessies: Het gebruik van RDP (remote desktop protocol) is niet toegestaan tenzij dit - bij uitzondering - niet anders kan en deze aantoonbaar sterk beveiligd is met bijvoorbeeld TLS	X	X	X	

beveiliging in combinatie met een RDS Gateway of een VPN/SSH tunnel. Publieke port forwarding is niet toegestaan. Diensten dienen binnen een beveiligde omgeving te worden aangeboden. Eventuele koppelingen dienen enkel via veilige verbindingen te verlopen. Directe koppelingen met lokale hardware tijdens remote sessies zijn niet toegestaan, als voorbeeld geen lokale usb support tijdens een remote sessie. Afstemming en goedkeuring hieromtrent dient vooraf plaats te vinden met CISO/ISO en Architectuur en Technisch Beheer van de Gemeente Tilburg.				
10. Er is een informatiebeveiliging risico analyse uitgevoerd met opvolging van te nemen maatregelen uit deze analyse.	X	X	X	
11. Er zijn maatregelen getroffen om de dreiging van hack/inbreuk of kwaadaardige software aan te pakken.	X			

12. Hardening van systeem en proces is ingericht en toegepast (bijvoorbeeld uitschakelen van ongebruikte services en poorten).	*X*			
13. De contractant hanteert een actief patchmanagementbeleid waarbij kritische/hoog risico kwetsbaarheden binnen een week (deze termijn is in lijn met de IBD/NCSC richtlijn) worden opgelost.	*X*	*X*		
14. *Indien in overleg de contractant e-mail mag versturen namens gemeente Tilburg moet dit afgestemd worden met* een tactisch IT adviseur. Met betrekking tot techniek wordt gestuurd richting het gebruik van e-mail sub domeinen (bijvoorbeeld factuur@extern.tilburg.nl).	*X*	*X*	*X*	
15. De contractant past actuele beveiligingsopties toe, zoals aangegeven door de IBD en NCSC.	X	X	X	

Zo dienen de in sectie (2.0 Algemene zakelijke informatie van de Contractant) opgegeven weblinks goed (“groen”) te scoren op **https://www.internet.nl/** De eisen staan uitgewerkt in de bijlage van het beleid websites. **Servicepunt - Beleid websites** Let op dit is een interne link en niet extern benaderbaar. De afstemming hieromtrent gebeurt door de aanvragende partij, de desbetreffende business unit van gemeente Tilburg, welke contact zoekt met het expertiseteam websites, dit kan onder andere via het e-mail adres: **websites@tilburg.nl**				

16. De in sectie (2.0 Algemene zakelijke informatie van de Contractant) opgegeven weblinks scoren minimaal een A rating op ssllabs.com. https://www.ssllabs.com/ssltest/ De afstemming hieromtrent gebeurt door de aanvragende partij, de desbetreffende business unit van gemeente Tilburg, welke contact zoekt met het expertiseteam websites, dit kan onder andere via het e-mail adres: **websites@tilburg.nl**	X	X	X	
17. De in sectie (2.0 Algemene zakelijke informatie van de Contractant) opgegeven weblinks voldoen aan de Tilburgse beleidsregels voor websites, met name de “veiligheids en inrichtingseisen webtoepassingen.” De eisen staan uitgewerkt in de bijlage van het beleid websites. **Servicepunt - Beleid websites** Let op dit is een interne link en niet extern benaderbaar. De afstemming hieromtrent gebeurt door de	X	X	X	

aanvragende partij, de desbetreffende business unit van gemeente Tilburg, welke contact zoekt met het expertiseteam websites, dit kan onder andere via het e-mail adres: **websites@tilburg.nl**				
18. De contractant heeft aantoonbaar maatregelen ingevoerd om de kans dat informatie kan worden onderschept tijdens transport/overdracht door onbevoegden te minimaliseren.	X			
19. De contractant volgt en voldoet aan de actuele beveiligingsrichtlijnen van de IBD en NCSC. https://www.informatiebeveiligingsdienst.nl/ https://www.ncsc.nl/	X	X		
20. Indien de gemeente Tilburg het nodig acht dient het gebruik van Certificaten ondersteund te worden.	X	X		

21. De informatievoorziening (gegevens) van gemeente Tilburg dient logisch gescheiden te zijn van andere partijen.	X	X		
22. Data classificatie van gemeente Tilburg onderscheidt 4 niveaus: publieke, interne, vertrouwelijke en geheime data. Bij vertrouwelijke data is data encryptie sterk aanbevolen. Bij geheime data zijn zowel multi-factor authenticatie voor toegang als data encryptie verplicht.	*X*	*X*	*X*	
23. Vooraf dienen de eisen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid (BIV) helder te zijn doorgegeven aan de leverancier/contractant zodat passende maatregelen en serviceniveaus kunnen worden afgesproken (in contract/sla), ingericht en bewaakt.			X	
24. Back-up en uitwijk voorzieningen, Continuïteit van het systeem. De contractant heeft aantoonbaar maatregelen getroffen om in het geval van een incident of calamiteit de afgesproken informatievoorziening binnen de afgesproken termijn weer operationeel te hebben.	X	X	X	

Gemeente Tilburg is verantwoordelijk voor het aangeven van deze termijn op basis van onze business continuïty documentatie.				
25. De Tilburgse voordeur dient gebruikt te worden voor identificatie/authenticatie. *Single sign on dient ondersteund te worden, ter voorkoming van een wildgroei van username/password combinaties.* *Momenteel via Microsoft ADFS en/of Microsoft AzureAD.*	X	X	X	
26. De contractant heeft aantoonbaar maatregelen ingevoerd ten behoeve van sterke user authenticatie voor toegang tot de data. U overlegt een beschrijving van de wijze van user authenticatie voor toegang tot data.	X			
27. Multi factor authenticatie (MFA) dient ondersteunt te worden. Voorkeur voor Microsoft Authenticator.	X	X	X	
28. Het is mogelijk om de toegang tot de applicatie te beperken tot IP-adressen van het netwerk van de gemeente Tilburg indien MFA niet mogelijk is.	X	X		

29. Het wachtwoordbeleid van de gemeente Tilburg dient opgevolgd te worden.	X	X	X	
30. Generieke accounts dienen zo veel mogelijk beperkt te worden. Uitgangspunt is gebruik van persoonlijke accounts.	X	X	X	
31. Wachtwoorden dienen veilig opgeslagen te worden. Geef in de toelichting aan welke waarborgen genomen zijn voor het veilig opslaan van wachtwoorden	X	X	X	
32. De samenwerking met ketenpartners wordt belangrijker. Het uitwisselen van informatie (bestanden) en toegang tot data-bronnen (via API's) dient juist ingeregeld te zijn. Voor vertrouwelijke informatie is encryptie van data in ruste optioneel. Voor geheime data is encryptie van data in ruste verplicht.	X	X	X	
33. De cloud provider is verplicht hoog risico beveiligings incidenten binnen een dag te melden aan de gemeente Tilburg.	X	X	X	
34. De cloud provider is verplicht zo spoedig mogelijk beveiligingsincidenten op te lossen, doch maximaal binnen 1 week.	X	X		

35. De gemeente Tilburg heeft het recht om logging gegevens op te vragen en in te zien. Indien gemeente Tilburg gebruik maakt van een centrale log infrastructuur (zoals bijvoorbeeld met SIEM oplossingen) dan dient de logging van de contractant - waar mogelijk - aan te sluiten op de centrale logging van de gemeente Tilburg.	X	X	X	
36. De externe informatievoorziening is ondergebracht binnen de EER (Europese Economische Ruimte)	X	X		
37. Indien er gebruik wordt gemaakt van Microsoft Azure Kubernetes/K8s dan dient de leverancier de Microsoft Azure Security Baseline for Azure Kubernetes Service te volgen en hieraan aantoonbaar te voldoen.	X	X		

Azure security baseline for Azure Kubernetes Service | Microsoft Learn				
38. U geeft grafisch (.jpg), schematisch, technisch en volledig aan op welke wijze verbindingen zijn dan wel worden gemaakt tussen de gemeente Tilburg Infrastructuur en de aangeboden(cloud) omgeving. Een eventueel extern datacenter is schematisch ook weergegeven. Dit omvat onder andere: • Type verbindingen; • Wijze van toegang; • Serverbenamingen/IP nummers; • Encryptie methoden (bijv. TLS, Clientcertificaten); • Wijze van endpoint beveiliging (bijv. OAuth 2.0 voor API's)	X	X		

• Netwerkpoorten voor verkeer; Encryptie techniek voor dataopslag;				
39. Iedere API wordt ontsloten via het integratieplatform van de Gemeente Tilburg. De API Gateway is hiervoor het verplichte functionele bouwblok. De API Gateway biedt onder andere de volgende functies: • Toegangscontrole • Throttling • Logging	x	x	x	
40. In principe kan er geen sprake zijn van direct cloud-cloud verkeer zonder tussenkomst van de gemeente Tilburg. In het geval hier wel sprake van is dan aangeven welke verkeerstromen dit zijn en wat voor data dit betreft. Verdere afstemming is nodig met een Tactisch IT adviseur alsmede een Architect.	x	x	x	

41. Data ontsluiting van M365 en overige data door applicaties van de contractant dient via het Microsoft GRAPH protocol plaats te vinden en niet via het oude EWS (Exchange Web Services) protocol. Ook hier geldt: gebruik van moderne identificatie en authenticatie methoden, role based access, least privileges.	x	x	x	

---

*Wensen voor de **Contractant***

42. Heeft uw organisatie een ISAE3402 (SOC1) verklaring van uw informatiebeveiliging?
    De onafhankelijk auditor dient te verklaren dat het systeem en de achterliggende processen voldoen. De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (NL:Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud.

    Indien ja, dan ontvangen we graag een kopie hiervan. (+10 punten)

43. Heeft uw organisatie een ISO 27001/27002 verklaring van uw informatiebeveiliging?
    De onafhankelijk auditor dient te verklaren dat het systeem en de achterliggende processen voldoen. De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (NL:Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud.
    Indien ja, dan ontvangen we graag een kopie hiervan. (+7 punten)

44. Laat uw organisatie met regelmaat (jaarlijks/om de 2 jaar) penetratietest(s) en/of vulnerability scan(s) uitvoeren op de infrastructuur – waarbij de aangeboden dienstverlening aantoonbaar in scope is - door een onafhankelijke (met gecertificeerde ethical hackers etc) partij? Indien ja, dan ontvangen we graag een kopie van het meest recente rapport wat minimaal een management samenvatting bevat met bevindingen geclassificeerd in risico's. Dit aangevuld door de leverancier mbt de aangegeven huidige status van de geconstateerde bevindingen en oplossingstermijnen. (+4 punten)

45. Heeft het datacenter een ISO 27001 verklaring van uw informatiebeveiliging?
    De verklaring dient te zijn verstrekt door een derde partij die zich houdt aan de norm voor auditors (NL:Norea). De verklaring dient recent te zijn en is maximaal 2 jaar oud.

    Indien ja, dan ontvangen we graag een kopie hiervan. (+2 punten)

Ter referentie:

- Een SOC 2 verklaring geeft in het algemeen meer zekerheid over de werking van controls en de ISO27001 over het managementsysteem van informatiebeveiliging
- ISAE3000
- SOC2/SOC3
- ISO 27017 is een internationale norm voor cloudbeveiliging
- ISO 27018 is een internationale norm voor privacy- en gegevensbescherming toegespitst op leveranciers van clouddiensten die persoonlijke gegevens namens hun klanten verwerken.

Bijlage x: Compatible Modbus kWh-meters with Energy Controller

Back in the days our Energy Controler was compatible for our local Load Balancing solution (Dynamic Load Balancing) with just one

manufacturer of Modbus kWh-meters: ABB. Nowadays we understand that our strength results from being widely applicable and also retrofit

whenever we support the following manufacturer brands and types of Modbus kWh-meters via either Modbus RTU (Remote Terminal Unit)

or Modbus TCP (Transmission Control Protocol).

Overview of compatible Modbus RTU kWh-meters with Energy Controller

Overview of compatible Modbus TCP kWh-meters with Energy Controller

1 ABB B23 112-10P

2 ABB B24 112-100

3 ABB A43 112-100

4 Controlin SKD-005-M

5 Hager ECR300C

6 Hager ECR310D

7 Hager ECR380D

8 Inepro PRO380

9 Xemex P1MB

10 Schneider Electric PowerLogic PM5111

11 Sineax DM5S

Manufacturer Type

1 Landis+Gyr E650 with CU-XE module

2 Metcom MCS301

3 Janitza UMG 604-PRO

4 Phoenix Phoenix Contact EEM-MA371