



2025



Programma van eisen

Primaire Storage en SAN

Zaakmap: INCS 70317

Datum: 12-05-2025



Inhoud

1	Inleiding	3
2	Programma van Eisen	4
	Scope van de opdracht	4
	Algemeen	4
	Inventarisatie van de huidige situatie	8
	Het maken van een ontwerp conform de huidige situatie	9
	Levering van hardware	10
	Implementeren en Migreren van de huidige situatie naar de nieuwe situatie	10
	Opleiden van beheerders van de gemeente	12
	Consultancy	13
	Hardware	13
	Storage Area Network	14
	Primaire Storage appliances	16
	Beheer	19
	Beveiliging	20
	Service levels	22
	Communicatie	27
	Projectmanagement	29
	Nadere offertes bij projecten en/of meerwerk	30
	Facturatie	31
	Beëindiging contract/ Retransistie	33

1 Inleiding

Dit is het programma van eisen behorend bij de Europese aanbesteding Primaire Storage- en Storagenetwerk-apparatuur en diensten

De aanleiding voor deze aanbesteding is het aflopen van de huidige overeenkomst voor de Primaire storage en Storage Netwerk dd. 1-1-2026. Ook geldt dat het einde van de technische levensduur is bereikt.

Het doel is om de storage en storagenetwerkcomponenten uiterlijk 01-01-2026 te hebben vervangen, geïmplementeerd en de data te hebben gemigreerd.

2 Programma van Eisen

Scope van de opdracht

Nr.	Omschrijving eis
SCO 1	<p>Opdrachtnemer is, in nauwe samenwerking met de opdrachtgever, verantwoordelijk voor de volgende zaken:</p> <ul style="list-style-type: none">A) Inventarisatie van de huidige situatie;B) Het maken van een ontwerp (globaal en in detail) conform de huidige situatie, rekening houdend met de toekomstige ontwikkelingen zoals de verhuizing van één van de datacentra;C) Het maken van een plan van aanpak voor de implementatie van de nieuwe oplossing inclusief een risicoanalyse;D) Leveren van hardware, software en licenties t.b.v. de nieuwe oplossing;E) Het opstellen van een acceptatie test in afstemming met en met goedkeuring van de opdrachtgever;F) Het implementeren van de nieuwe oplossing en inpassen in de bestaande ICT-infrastructuur;G) Het begeleiden van de opdrachtgever bij het migreren van data naar de nieuwe oplossing;H) Opleiden van beheerders van de gemeente;I) Onderhoud;J) Consultancy. <p>Deze onderwerpen zijn verderop in het PvE uitgewerkt.</p>

Algemeen

Nr.	Omschrijving eis
ALG 1	De opdrachtnemer levert en implementeert on premises Primaire Storage.
ALG 2	Op 01-01-2026 moet de door opdrachtnemer aangeboden oplossing in productie zijn.
ALG 3	De opdrachtnemer garandeert dat gedurende de contractperiode de aangeboden oplossing wordt onderhouden, ondersteund en doorontwikkeld.

Nr.	Omschrijving eis
ALG 4	IPv4 en IPv6 dienen ondersteund te worden en om te kunnen communiceren via IPv4-only, via IPv6-only en via dual-stack netwerken. Als de software netwerkparameters in haar lokale of remote server-instellingen bevat, dan moet de software ook de configuratie van IPv6-parameters ondersteunen. Alle functies die via IPv4 worden aangeboden moeten ook via IPv6 beschikbaar zijn. De opdrachtgever/eindgebruiker mag geen verschil ervaren wanneer de software via IPv4 of IPv6 communiceert, tenzij dit een expliciet voordeel voor de gebruiker oplevert.
ALG 5	De oplossing moet aangesloten kunnen worden op de bestaande server infrastructuur.
ALG 6	Alle componenten van de oplossing die zijn voorzien van eigen voedingen dienen een redundante voeding te hebben.
ALG 7	Het nieuwe storage netwerk zal gebaseerd zijn op Fibre Channel technologie.
ALG 8	De nieuwe oplossing zal naast de bestaande oplossing worden opgebouwd, waarna een transitie zal plaatsvinden.
ALG 9	Het ontwerp dient uiterlijk 1 week na definitieve gunning ter goedkeuring worden aangeboden. De hardware, software en licenties dienen uiterlijk zes weken na definitieve gunning de goedkeuring van het definitieve ontwerp geleverd te worden.
ALG 10	Uiterlijk twee weken na levering van de Hardware dient de oplevering van de configuratie plaats te vinden en de migratie te starten.
ALG 11	De documentatie en "userinterfaces" van alle onderdelen van de voorziening zijn volledig beschikbaar in minimaal de Engelse taal.
ALG 12	Oplossing voldoet aan de vereisten van forum standaardisatie gedurende de looptijd van het contract (zie: https://www.forumstandaardisatie.nl/open-standaarden).
ALG 13	Leverancier levert installatiebestanden die voorzien zijn van een vertrouwd certificaat.
ALG 14	De opdrachtnemer levert een technische architectuurplaat op hoofdlijnen met alle componenten, koppelvlakken, disaster/recovery.
ALG 15	De opdrachtnemer draagt zorg voor een installatieverslag na elke installatie en wijziging. Daarin is in elk geval opgenomen: een netwerktekening met gebruikte protocollen en poorten en aangepaste documentatie en architectuurplaten.
Informatiebeveiliging en privacy	

Nr.	Omschrijving eis
ALG 16	De opdrachtnemer houdt zich aan alle wet- en regelgeving (Nederlandse en Europese) aangaande privacybescherming m.b.t. de door hem geleverde oplossing en diensten. Denk bijvoorbeeld aan rechten van betrokkenen, anonimiseren, dataminimalisatie, verwijderen van gegevens, bewaartermijnen, etc. Alle wet- en regelgeving zoals de GDPR/AVG zijn leidend in geval van tegenstrijdigheden met andere eisen, wensen of voorstellen van opdrachtnemer.
ALG 17	De gegevens van gemeente worden alleen in de EER opgeslagen.
ALG 18	De infrastructuur en organisatie van leverancier zijn adequaat beveiligd volgens ISO 27001 of vergelijkbaar. Leverancier is bij gunning en gedurende de hele contractperiode gecertificeerd voor ISO 27001 en overhandigt het certificaat met verklaring van toepasselijkheid ten tijde van het sluiten van de overeenkomst. Het gevraagde certificaat dient opgeleverd te worden als Nederlandstalig document.
ALG 19	De gemeente heeft toestemming om zelf een pentest te (laten) uitvoeren.
ALG 20	De opdrachtnemer verleent medewerking aan het uitoefenen van controle door of namens gemeente op bewaring en gebruik van data en naleving van procedures.
ALG 21	Op verzoek van de gemeente werkt opdrachtnemer altijd mee aan een risicoanalyse op de informatiebeveiliging.
ALG 22	Voor veilige bestandsuitwisseling via mail tussen opdrachtgever en opdrachtnemer accepteert opdrachtnemer de oplossing die opdrachtgever biedt welke compliant is aan de NTA 7516 (op dit moment Zivver). Indien leverancier een oplossing ter beschikking heeft kan dit na goedkeuring van bevoegd ICT-manager van de opdrachtgever als alternatief dienen.
ALG 23	De opdrachtnemer zorgt voor een gedegen technische beveiliging (voor het verwerken van persoonsgegevens) in relatie tot specifieke wetgeving. Denk bijvoorbeeld aan de Wpg (Wet politiegegevens).
ALG 24	Het systeem voldoet aan de vereisten die de AVG en de Archiefwet stellen. Dit houdt in dat de gemeente zelf de bewaartermijnen kan instellen, rekening houdend met afwijkende bewaartermijnen in de AVG/Archiefwet.
ALG 25	Alle calamiteiten gerelateerd aan de opdracht (voorbeeld kwetsbaarheidsmeldingen) zijn verwerkt in de aanbieding.

Nr.	Omschrijving eis
ALG 26	<p>Indien de leverancier werkzaamheden op afstand dient te verrichten kan via Teamviewer toegang tot het domein van Purmerend worden verkregen. Ondersteuning is hierbij op een afgesproken moment waarbij de werkzaamheden onder supervisie van opdrachtgever worden uitgevoerd. Indien opdrachtnemer een alternatieve oplossing ter beschikking heeft kan dit na goedkeuring van bevoegd ICT-manager van de gemeente als oplossing dienen.</p> <p>Of de beschikbaarheid remote mag, is afhankelijk van het vraagstuk van de gemeente. Dit wordt per keer bepaald.</p>
ALG 27	<p>De Opdrachtnemer heeft alleen onder begeleiding van beheerders van de gemeente, toegang tot de voorziening. De beheerders van Opdrachtnemer die beheeracties uitvoeren op de voorziening dienen in bezit te zijn van een geldige VOG (passend bij de opdracht), en dienen de integriteitsverklaring voor externen (zie bijlage 10) van de gemeente te tekenen.</p>
Wachtwoordbeleid en accounts	
ALG 28	<p>De voorziening biedt de mogelijkheid om te werken met lokale beheeraccounts.</p>
ALG 29	<p>De voorziening ondersteunt in het inrichten van verschillende rollen en rechten voor beheerders.</p>
ALG 30	<p>De voorziening moet een functie hebben waarbij een sessie met de beheerinterface wordt beëindigd na een, bij voorkeur vrij in te stellen, termijn van inactiviteit.</p>
ALG 31	<p>Als op de voorziening enkel vanaf het lokale netwerk ingelogd kan worden, dan dwingt het systeem een wachtwoord af van ten minste 25 vrij te kiezen karakters waaronder het gebruik van een hoofdletter, cijfer en leesteken.</p>
ALG 32	<p>Het systeem ondersteunt het afdwingen van een maximale gebruiksduur van een wachtwoord.</p>
ALG 33	<p>De applicatie moet een functie hebben waarmee time-outs op het aantal foutieve inlogpogingen worden ondersteund. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.</p>
ALG 34	<p>De applicatie moet beheerders de mogelijkheid geven om hun wachtwoord te kunnen wijzigen. Beheerders van de opdrachtgever moeten de wachtwoorden van andere beheerders kunnen wijzigen.</p>
ALG 35	<p>Het gebruik van de wachtwoorden van de voorziening in de organisatie moet door beheeraccounts gecontroleerd/beheerd kunnen worden.</p>
ALG 36	<p>Wachtwoorden in de voorziening worden als salted hash opgeslagen.</p>

Nr.	Omschrijving eis
ALG 37	Basic Authentication is niet toegestaan.
Vernietigen gegevensdragers	
ALG 38	Opdrachtnemer laat alle hardware welke vervangen wordt bij de implementatie van de voorziening achter bij de gemeente. De gemeente draagt aansluitend zelf zorg voor een veilige vernietiging van de gegevensdragers.
ALG 39	Als het tijdens de contractperiode noodzakelijk is datadragende componenten van de te leveren oplossing te vervangen, zullen de vervangen datadragende componenten achterblijven bij de opdrachtgever.
ALG 40	Als het tijdens de contractperiode noodzakelijk is niet-datadragende componenten van de te leveren oplossing te vervangen, zal de vervangen apparatuur worden ingenomen door de opdrachtnemer en ontdaan van alle configuratiegegevens en andere kenmerken die de componenten mogelijk aan de opdrachtgever kunnen koppelen. Opdrachtnemer draagt zorg voor het wissen van de nog aanwezige data en voorziet gemeente hierbij van een verklaring van vernietiging.
ALG 41	Opdrachtnemer kan door de gemeente worden verzocht om compatibele gegevensdragers waarop gegevens van de gemeente staan te laten overschrijven conform de BLANCCO-methode. De gemeente bepaalt welk versienummer van BLANCCO Network Device Eraser hiervoor gebruikt moet worden. Na overschrijving van de gegevensdrager(s) levert opdrachtnemer het BLANCCO-certificaat aan bij de gemeente (ICT-manager).
ALG 42	Opdrachtnemer verschaft aan de gemeente onverwijld het certificaat van overschrijving, vernietiging en/of transport. Dit dient te gebeuren binnen 24 kantooruren.

Inventarisatie van de huidige situatie

Nr.	Omschrijving eis
INV 1	Zie de leidraad voor een globale beschrijving van de huidige situatie. Als onderdeel van de planningsfase zal opdrachtnemer een gedetailleerde inventarisatie uitvoeren van de bestaande omgeving als basis voor de ontwerpen en implementatieplannen.

Het maken van een ontwerp conform de huidige situatie

Als onderdeel van de inschrijving op deze aanbesteding dient Opdrachtnemer een ontwerp van de storage appliances en fibre channel infrastructuur aan te leveren (zie ook gunningscriterium Ontwerp en Inrichting (K1)). Deze paragraaf beschrijft de eisen die worden gesteld aan het ontwerp.

Nr.	Omschrijving eis
ONT 1	<p>Het ontwerp voldoet aan volgende punten:</p> <ul style="list-style-type: none">A) Het ontwerp bevat alle producten (waaronder storage appliances en storagenetwerkapparatuur), inclusief aantallen merk en type die op de verschillende locaties zullen worden toegepast;B) De storage appliances dienen zelf ook hoog beschikbaar te zijn dmv dubbele voedingen, controllers etc. en de toepassing van spiegel, RAID of andere technieken;C) Synchrone replicatie en andere technologieën (als HyperSwap/Metro Cluster) zorgen voor een active-active situatie, waardig aan een twin datacenter concept;D) Moet geschikt zijn, mits goed beheerd door de gemeente, om op jaarbasis een 24 * 7 beschikbaarheidspercentage te halen van minimaal 99,99%;E) Alle verbindingen door het publieke domein (internet, fibre tussen locaties) dienen encrypted te zijn;F) Best practices van de productleveranciers worden toegepast;G) Is toekomstgericht zodat bijvoorbeeld quantum resistente encryptie kan worden toegepast;H) Voldoet aan de bestaande kaders voor informatiebeveiliging bij de overheid, waaronder de Baseline Informatiebeveiliging Overheid (BIO);I) Het voor de opdrachtgever mogelijk maakt om in de toekomst te voldoen aan nieuwe verplichtingen die de NIS 2.0 richtlijn gaat voorschrijven;J) Het ontwerp leidt tot een zogeheten twin datacenter netwerk met:<ul style="list-style-type: none">a. Twee hoogbeschikbare fibre channel fabrics.b. Twee hoogbeschikbare storage appliances opererend als een Active-Active cluster. <p>Let op Dit ontwerp is een conceptontwerp. Na gunning wordt dit ontwerp in samenwerking met de gemeente verder uitgewerkt, aangepast en vastgesteld.</p> <p>In het gunningscriterium vragen we inschrijver op basis van de informatie uit deze aanbesteding, zijn kennis en ervaring en inschatting van de huidige situatie een conceptontwerp te maken. Dit ontwerp geeft de gemeente een beeld van de kennis, kunde, prijzen en mogelijkheden van de Inschrijver. De inschrijver zal op basis van die criteria worden beoordeeld.</p>

Nr.	Omschrijving eis
	Na gunning wordt er gezamenlijk een ontwerp opgesteld. Het ingediende ontwerp kan daarbij als basis dienen, echter is dit niet per definitie leidend voor het uiteindelijke ontwerp.
ONT 2	Opdrachtnemer levert voor de oplevering in de productieomgeving een Nederlands- of Engelstalige handleiding voor de medewerkers van de gemeente op.

Levering van hardware

Nr.	Omschrijving eis
HWR 1	Opdrachtnemer levert hard- en software die fabrieksnieuw is (niet refurbished/re-used) en enkel afkomstig uit officiële kanalen.
HWR 2	Opdrachtnemer levert hardware voorzien van de meest recente (door leverancier geadviseerde) en voor productie vrijgegeven firmware.
HWR 3	De fysieke leveringen van de hardware op locatie van de gemeente geschieden maximaal twee (2) werkdagen voor plaatsing/installatie. Dit in overleg met en met goedkeuring van de gemeente op een door de gemeente nader te bepalen in pandige plek. Alle verpakkingsmaterialen worden door Opdrachtnemer meegenomen en afgevoerd via haar eigen afvalstromen. Let op: De opslagruimte is beperkt. De gemeente stelt opslagruimte in alle redelijk- en mogelijkheid beschikbaar.

Implementeren en Migreren van de huidige situatie naar de nieuwe situatie

Nr.	Omschrijving eis
IMP 1	Opdrachtnemer stelt een projectleider aan die gedurende het hele project alsmede de gehele migratiefase als aanspreekpunt fungeert voor de gemeente. Van de projectmanager wordt verwacht dat hij de werkzaamheden uitvoert zoals beschreven in het hoofdstuk Projectmanagement in dit document.

Nr.	Omschrijving eis
IMP 2	<p>Opdrachtnemer is leidend in en verantwoordelijk voor het in overleg met de opdrachtgever:</p> <ul style="list-style-type: none"> A. Opstellen van concept en definitieve versie van de ontwerpen en het migratieplan; B. Ontwerpen en plannen van de migratie naar de nieuwe storageinfrastructuur; C. Het begeleiden van de medewerkers van de opdrachtgever met de migratie naar de nieuwe infrastructuur; D. Opstellen van test- en acceptatieplannen; E. Opstellen en uitvoeren van een communicatieplan in samenwerking met de gemeente; F. Opstellen en uitvoeren van een trainingsplan voor beheerders van de gemeente.
IMP 3	<p>De implementatie en migratie dienen zo te worden georganiseerd dat er minimale verstoringen optreden in het bedrijfsproces. In overleg met de gemeente worden de momenten bepaald waarop werkzaamheden worden verricht die het bedrijfsproces kunnen verstoren. De opdrachtnemer dient hierbij rekening te houden dat dit type werkzaamheden in de avonduren, vakanties en/of weekenden uitgevoerd moeten worden.</p>
Opzetten van een acceptatieomgeving	
IMP 4	<p>Van de Opdrachtnemer wordt verwacht dat:</p> <ul style="list-style-type: none"> A) (delen van) de voorziening tijdelijk opgebouwd worden naast de huidige situatie; B) De tijdelijke omgeving dient een representatief beeld te geven van de uiteindelijke voorziening; C) In deze tijdelijke omgeving vindt een acceptatietest plaats. De uitslag van de acceptatietest is input voor het besluit of de nieuwe omgeving live gezet kan worden; D) Als uit de acceptatietest restpunten komen, dan worden deze voor live-gang opgelost waarna opnieuw een acceptatietest zal worden uitgevoerd; E) De finale acceptatie vindt plaats in de live-omgeving; F) Opdrachtnemer is leidend in en verantwoordelijk voor het in overleg met de opdrachtgever opstellen van het acceptatietestplan; G) In overleg met de opdrachtgever wordt een afspraak gemaakt voor de finale acceptatie. H) De opdrachtnemer bevestigt het verzoek tot oplevering schriftelijk. I) De finale acceptatie is zo gepland dat de uiterste opleverdata niet overschreden worden en is randvoorwaardelijk voor de start van de live-gang (migratie).

Nr.	Omschrijving eis
Migreren van de huidige naar de nieuwe situatie	
IMP 5	Nadat de acceptatie is geaccepteerd door de opdrachtgever, wordt de migratie (live-gang) voorbereid volgens het eerder opgestelde migratieplan;
IMP 6	Het is de bedoeling dat de opdrachtgever zelf, onder begeleiding van de opdrachtnemer, de migratie uitvoert nadat samen met de opdrachtnemer een werkwijze is vastgesteld.
IMP 7	Als onderdeel van het project levert Opdrachtnemer de technische ontwerpen en architectuur van de geïmplementeerde oplossing.

Opleiden van beheerders van de gemeente

Nr.	Omschrijving eis
OPL 1	De systeembeheerders van de opdrachtgever (4 personen) dienen te worden getraind en opgeleid door een authorized training partner van aangeboden oplossing zodat de systeembeheerders direct voor acceptatie van het desbetreffende onderdeel van de voorziening in staat zijn om het dagelijks beheer en monitoring uit te voeren. Dit betekent dat de systeembeheerders de geïmplementeerde situatie moeten begrijpen en voldoende kennis hebben van de managementomgeving(en) voor het beheren van de voorziening. Opdrachtnemer draagt zorg voor organisatie van deze opleidingen.
OPL 2	Opleiding en training wordt in het Engels of Nederlands gegeven en documentatie is in het Engels of Nederlands beschikbaar.
OPL 3	De opleiding zal plaatsvinden in Nederland en tijdens normale kantoortijden.
OPL 4	Tijdens implementatie zal door systeembeheerders/netwerkbeheerders van de gemeente meegelopen worden en vindt er "training on the job" plaats van de inrichting zoals vastgelegd in het design.

Consultancy

Onder consultancy valt het op verzoek van de gemeente adviseren met betrekking tot ICT-vraagstukken, gerelateerd aan de scope van de gevraagde dienstverlening.

Dit kunnen bijvoorbeeld vragen zijn over gewenste functionaliteit en /of aanpassingen (changes), het beschikbaar maken van (nieuwe) functionaliteiten, of input leveren met betrekking tot projecten met een aspect op gebied storage en storage netwerken.

Nr.	Omschrijving eis
CON 1	Opdrachtnemer verzorgt, zowel gevraagd als ongevraagd, strategisch advies (advies op het vlak van zowel innovatie als kwaliteitsverbetering) tijdens periodiek in te plannen overleg.
CON 2	De gemeente wil op verzoek advies inwinnen bij een technisch expert/adviseur over bepaalde functionaliteit of vraagstukken. Deze expert/adviseur dient binnen 1 werkweek na het verzoek van de gemeente beschikbaar te zijn. Deze werkzaamheden worden tegen de overeengekomen uurtarieven verrekend.
CON 3	Wanneer uit het advies projecten voortkomen zullen deze apart worden aangeboden door middel van een nadere offerte. Deze nadere offerte is onderdeel van deze aanbesteding en voldoet altijd aan het gestelde in de aanbestedingsstukken en de inschrijving van Opdrachtnemer zoals de tarieven.
CON 4	Opdrachtneming zal, in woord en geschrift, de Nederlandse of Engelse taal bezigen voor consultancy werkzaamheden.

Hardware

Nr.	Omschrijving eis
	Updates
HW 1	De geleverde producten dienen minimaal gedurende 6 jaar na levering voorzien te worden van security-updates.
	Logging
HW 2	De oplossing moet logs kunnen versturen naar een centrale logaggregatie oplossing binnen de on-premises omgeving van de gemeente.

Nr.	Omschrijving eis
HW 3	<p data-bbox="352 499 1034 533">De voorziening legt een audit trail vast over het gebruik.</p> <ul data-bbox="501 555 1385 1108" style="list-style-type: none"> <li data-bbox="501 555 1385 734">• De oplossing beschikt over een niet-muteerbare audit trail met daarin minimaal de gebeurtenis; de benodigde informatie die nodig is om een incident met hoge mate van zekerheid te kunnen herleiden tot het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. <li data-bbox="501 741 1385 846">• Deze audit trail bevat alle handelingen welke door beheerders worden verricht zoals raadplegen, aanmaken, muteren en verwijderen. <li data-bbox="501 853 1385 958">• Vastlegging vindt minimaal plaats op gebruikersniveau en -rol, tijdstip en verrichte actie en is inzichtelijk voor zowel beheerders als de CISO van de gemeente. <li data-bbox="501 965 1385 1108">• De voorziening ondersteunt dat de logbestanden ten behoeve van de audit trail gedurende een door de gemeente nader te bepalen periode bewaard worden waarna het mogelijk is deze uit de voorziening te verwijderen.
HW 4	De beheerder kan de logs exporteren als CSV bestand.

Storage Area Network

Nr.	Omschrijving eis
SAN 1	De fabrikant van de Storage Area Netwerkapparatuur die Opdrachtnemer aanbiedt is een bewezen leider in de industrie op het gebied van Fibre Channel netwerken.
SAN 2	De opdrachtnemer dient gecertificeerd te zijn voor de levering, implementatie en onderhoud van de aangeboden producten.
SAN 3	De opdrachtnemer zal voldoende voedingskabels leveren van het juiste type. De door de gemeente gebruikte PDUs in de datacentra bieden ruimte voor stekkers van het type IEC14 en IEC20.
SAN 4	Het Storage Area Network zal zijn gebaseerd op fibre channel switched fabric technologie.
SAN 5	De geleverde fibre channel switches zullen minimaal 32Gbps FC (Gen 6 of hoger) ondersteunen.
SAN 6	Alle aangeboden switches zijn van hetzelfde merk. Dit mag afwijken van het merk van de Storage Appliances.

Nr.	Omschrijving eis
SAN 7	<ul style="list-style-type: none"> • De oplossing zal, per fabric en per locatie, minimaal 32 poorten kunnen leveren aan hosts. • Iedere switch zal 4 poorten beschikbaar hebben voor intra- en interzone koppelingen. • Het is niet noodzakelijk alle switchpoorten te voorzien van een transciever, zie eisen SAN 8, SAN 9 en SAN 10.
SAN 8	In totaal zullen er 67 SFP+ FC-32Gb multimode modules worden geleverd om servers en back-up appliances aan te sluiten.
SAN 9	In totaal zullen er 16 SFP+ multimode modules worden geleverd geschikt voor de maximale poortsnelheid van de switch om de storage appliances aan te sluiten (dus: Gen7=64Gb/s).
SAN 10	In totaal zullen er 8 SFP+ singlemode (1310 nm) modules worden geleverd geschikt voor de maximale poortsnelheid van de switch tbv de intersite-links (dus: Gen7=64gb/s).
SAN 11	De oplossing zal twee of meer fabrics bevatten, resulterend in redundante paden tussen host en storage.
SAN 12	De fabrics zullen "stretched" zijn over beide locaties; FC Routing lijkt niet noodzakelijk/wenselijk in deze situatie.
SAN 13	De oplossing moet aangesloten kunnen worden op de bestaande server infrastructuur. De huidige koppelvlakken zijn FC: 8 en 16Gbps.
SAN 14	De oplossing zal ook FC endpoints met een lijnsnelheid van 16Gbps accepteren.
SAN 15	De oplossing zal ook FC endpoints met een lijnsnelheid van 8Gbps accepteren.
SAN 16	De bestaande servers zullen niet worden voorzien van nieuwe Fibre Channel HBA's.
SAN 17	De Ethernetaansluitingen voor beheerdoeleinden zullen snelheden van 1Gbps ondersteunen.
SAN 18	Alle switchpoorten die uitgerust zijn met een transciever zullen gelicentieerd zijn voor deelname aan de switched fabrics in de daartoe benodigde rol.
SAN 19	Alle gebruikte transciever modules zullen zijn gecertificeerd door de switchfabrikant voor gebruik in betreffende switch voor het beoogde doel.
SAN 20	De verbinding tussen hoofd en uitwijk locatie zal voor beide fabrics redundant zijn.
SAN 21	Er zijn in totaal 4 OS1 OS2 dark fibre glasvezelparen beschikbaar voor de intersite koppeling.
SAN 22	De opdrachtgever maakt geen gebruik van DWDM of vergelijkbare technieken.

Nr.	Omschrijving eis
SAN 23	Eventuele extended fabric licenties en benodigde buffer credits zullen deel uitmaken van de aanbidding.
SAN 24	FC-NVMe (NVMe over Fibre channel) moet tot de ondersteunde protocollen behoren.
SAN 25	De apparatuur zal een koelluchtstroom hebben van voor (poortzijde) naar achter (front to back). Dit in verband met de inrichting van de computerzalen.
SAN 26	De SAN apparatuur zal zijn klok kunnen synchroniseren met meerdere tijdbronnen middels ntp.
SAN 27	De tijd zal worden bijgehouden in UTC, maar worden gepresenteerd in de lokale tijdzone.

Primaire Storage appliances

Nr.	Omschrijving eis
PS 1	De fabrikant van de storage appliances die Opdrachtnemer aanbiedt dient zich te bevinden in het "Leaders quadrant" van het Gartner Magic Quadrant for Primary Storage Platforms, 17 september 2024.
PS 2	De opdrachtnemer dient gecertificeerd te zijn voor de levering, implementatie en onderhoud van de aangeboden producten.
PS 3	Het koppelvlak met de storage netwerk switches zal 32 of 64 Gb/s Fibre Channel zijn, al naar gelang van de geleverde switches.
PS 4	De opdrachtnemer zal voldoende voedingskabels leveren van het juiste type. De door de gemeente gebruikte PDUs in de datacentra bieden ruimte voor stekkers van het type IEC14 en IEC20.
PS 5	De onlinestorageoplossing zal enterprise-grade zijn en gebaseerd op flash geheugen (All-Flash technologie).
PS 6	Alle aangeboden storage appliances zijn van hetzelfde merk. Dit mag afwijken van het switch merk.
PS 7	In geval van een multi-tier oplossing worden datablokken automatisch verplaatst tussen de verschillende flash tiers aan de hand van I/O patronen (auto tiering).
PS 8	De dataopslag eenheden (SSD's, NVMe, FCM etc) zullen "self encrypting" zijn.
PS 9	De dataopslageenheden zullen van zodanige kwaliteit zijn dat er gedurende de contractperiode geen merkbare slijtage of prestatieniveauvermindering zal zijn.

Nr.	Omschrijving eis
PS 10	LUNs zullen standaard verdeeld worden over alle opslageenheden (binnen 1 tier; geen hotspots).
PS 11	LUNs moeten kunnen worden toegewezen aan meerdere servers.
PS 12	Het moet mogelijk zijn om Microsoft VSS compliant snapshots te maken.
PS 13	Het moet mogelijk zijn van meerdere LUNs gelijktijdig consistente snapshots te maken (consistency groups).
PS 14	Snapshots mogen geen negatieve performance impact hebben.
PS 15	De minimale netto bruikbare omvang van de datacapaciteit is bij levering 100TB ¹ per locatie (in totaal dus 200TB).
PS 16	De omvang van de datacapaciteit is uit te breiden tot 150TB netto per locatie in dezelfde oplossing (zonder daarvoor enclosures, trays of controllers toe te voegen) waarbij de prestatie en beschikbaarheidskarakteristieken niet negatief mogen worden beïnvloed.
PS 17	Wanneer de opgegeven datacapaciteit inclusief data deduplicatie en/of compressie is dan moet de capaciteit zoals genoemd in PS 15 en PS 16 gegarandeerd worden door de leverancier.
PS 18	De capaciteit van alle dataopslagmodules dient in zijn geheel te kunnen worden verdeeld over LUNs, ongeacht het type schijf. Een LUN kan dus bestaan uit dataopslagmodules van verschillende typen of capaciteit.
PS 19	Indien er per locatie meer dan één appliance nodig is om aan de capaciteitsbehoefte te voldoen, zullen deze zich voordoen als één appliance.
PS 20	De beoogde oplossing dient minimaal 40000 sustained front-end IOPS te kunnen verwerken bij gemiddeld 32KB block grootte bij een verdeling van 60% read en 40% write voor een capaciteit van minimaal 50TB. De responsetijd over de gehele capaciteit zal altijd <5ms zijn.
PS 21	Indien noodzakelijk kunnen FC koppelingen gebundeld worden (MPIO) om tot meer bandbreedte te komen.
PS 22	De storage omgeving is verdeeld over twee locaties primair en secundair.
PS 23	De onlinestorageoplossing moet data zowel synchroon als asynchroon kunnen repliceren tussen de beide locaties (tussen beide storageappliances).

¹ De gemeente hanteert hier een decimale interpretatie; 1TB is 10³GB is 10⁶MB

Nr.	Omschrijving eis
PS 24	Replicatie mag geen merkbare invloed hebben op de performance.
PS 25	Replicatie zal plaatsvinden over fibre channel.
PS 26	In geval van synchrone replicatie moet het mogelijk zijn om beide spiegel delen gelijktijdig te beschrijven (active-active).
PS 27	In geval van asynchrone replicatie dient de interval instelbaar te zijn.
PS 28	De status (en voortgang) van de replicatie moet zichtbaar zijn in de beheer GUI van iedere appliance afzonderlijk. In het geval van een gefedereerde beheer GUI dient de replicatie status daar ook af te lezen te zijn.
PS 29	Verstoringen aan de replicatie dienen middels email en snmp traps te worden gemeld. De benodigde MIB's worden meegeleverd.
PS 30	Replicatie dient per LUN te kunnen worden ingeregeld en geconfigureerd.
PS 31	Per LUN dient het replicatietype te kunnen worden ingesteld.
PS 32	Het moet mogelijk zijn om willekeurig van de richting, replicatie te kunnen opzetten (LUN 1 van Site A -> Site B, LUN 2 van Site B -> Site A).
PS 33	Alle netwerk en Fibre channel koppelingen zullen redundant uitgevoerd zijn.
PS 34	NVMe-of (Fibre Channel) moet tot de ondersteunde protocollen behoren.
PS 35	Binnen de storage appliance zal voldoende reservecapaciteit per type dataopslagmodule beschikbaar zijn om in geval van de uitval van een opslag component onmiddellijk te kunnen starten met het herbouwen.
PS 36	Datadragers zullen zodanig zijn gegroepeerd dat uitval van maximaal twee eenheden uit dezelfde "raid group" niet leidt tot dataverlies.
PS 37	De storage appliances zullen zijn voorzien van redundante voedingen.
PS 38	In geval van stroomuitval dient de data die in volatiele cache geheugen staat consistent te kunnen worden opgeslagen zodat bij stroomherstel een commit naar dataopslagenheid kan plaatsvinden.
PS 39	Ingeval van herstel van de stroomvoorziening dient de oplossing zelfstandig op te starten en online te komen.
PS 40	De storage processoren en controllers dienen redundant uitgevoerd te zijn (active/active).
PS 41	De storage apparatuur zal zijn klok kunnen synchroniseren met meerdere tijdsbronnen middels ntp.

Nr.	Omschrijving eis
PS 42	De tijd zal worden bijgehouden in UTC, maar worden gepresenteerd in de lokale tijdzone.
PS 43	Alle opgeslagen data zullen versleuteld zijn.
PS 44	De versleuteling zal plaatsvinden in hardware van de betreffende storage module.
PS 45	De encryptie en decryptie processen hebben geen invloed op de performance.
PS 46	De toegepaste encryptie zal AES-256 en derhalve quantum resistent zijn.
PS 47	Symmetrische "Data Encryption Keys" zullen de appliance nooit verlaten.
PS 48	De Data Encryptie Keys zullen met een quantum-veilig "key-encapsulation method" worden beveiligd (ML-KEM - FIPS-203).
PS 49	Er moeten "immutable" kopieën van LUNs gemaakt kunnen worden, liefst periodiek en automatisch.

Beheer

Vanuit een beheer oogpunt moet de geleverde oplossing voldoen aan de volgende eisen.

Nr.	Omschrijving eis
BEH 1	Vanuit de grafische beheerinterface (GUI) van de storage appliances kunnen LUNs worden aangemaakt of worden gewijzigd.
BEH 2	Vanuit de grafische beheerinterface van de storage omgeving moeten LUNs kunnen toegewezen aan servers of deze toewijzingen worden gewijzigd (masking).
BEH 3	De masking van een LUN moet kunnen worden aangepast zonder dat het LUN offline gaat. (Bijvoorbeeld: vervanging HBA/server, toevoegen node aan bestaand cluster).
BEH 4	LUNs moeten kunnen worden vergroot zonder dat tijdens dat proces de beschikbaarheid wordt aangetast.
BEH 5	Vanuit de grafische beheerinterface van de storageomgeving moeten snapshots kunnen worden gemaakt.
BEH 6	De storage appliances moet nauw kunnen samenwerken met Microsoft Virtual Machine Manager versie 2019/2025. Derhalve moet e.e.a. Compliant zijn met SMI-S en Microsoft SMAPI.
BEH 7	Het moet mogelijk zijn om Microsoft VSS compliant snapshots te maken.

Nr.	Omschrijving eis
BEH 8	LUNs moeten THIN kunnen worden uitgegeven.
BEH 9	Het moet mogelijk zijn een snapshot van een disk te kunnen mounten.
BEH 10	Het systeem dient verwachte storingsen en storingsen per email te melden aan 1 of meerdere vooraf ingestelde mailadressen. Deze berichten worden verstuurd in clear-tekst en/of HTML format.
BEH 11	De switches en storage appliances zullen email berichten versturen gebruik makend van SMTP (of MS Graph API) bij voorkeur geauthentiseerd. Indien mogelijk middels Oauth.
BEH 12	Het systeem dient verwachte overschrijdingen of actuele overschrijdingen van drempelwaardes die betrekking hebben op de verbruikte capaciteit van LUNs, schijven, geheugen, processoren, netwerk, fibre channel en overige componenten te melden aan 1 of meerdere vooraf ingestelde emailadressen. Deze berichten worden verstuurd in clear-tekst en/of HTML-format.
BEH 13	De statussen zoals bijvoorbeeld die benoemd in BEH 12 moeten kunnen worden uitgevraagd middels SNMPv3 door gangbare monitoring software. De benodigde MIB's worden meegeleverd.
BEH 14	Er moeten (near)real-time rapportages gemaakt kunnen worden over de IOPS-behoefte van servers en/of LUNS.
BEH 15	Door middel van rapportages moeten op basis van historische gegevens extrapolaties mogelijk zijn om zodoende capaciteitsplanning te kunnen doen.
BEH 16	De systemen moeten voorzien zijn van een "phone home" functionaliteit die dagelijks metadata verstuurt aan de fabrikant en, in geval van een verstoring, deze meldt aan de fabrikant.
BEH 17	De storage appliances moeten hun logs centraal kunnen opslaan op een syslog server. Deze logs moeten echter ook lokaal beschikbaar blijven gedurende 3 maanden.

Beveiliging

Nr.	Omschrijving eis
BEV 1	Alle data die wordt opgeslagen zal worden versleuteld. Zie PS 43 en verder.
BEV 2	De beheerinterfaces van alle appliances en switches zullen authenticatie door een AAA server middels TACACS+ ondersteunen.

Nr.	Omschrijving eis
BEV 3	De permissies van een beheer account op de switches zullen worden bepaald door de AAA server middels TACACS+ .
BEV 4	Verschillende gebruikers zullen verschillende rechten krijgen op de appliances gebaseerd op de hun toegewezen rol (RBAC).
BEV 5	De voorziening voldoet aan de actuele vereisten gesteld in de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Daarbij gaat opdrachtgever op dit moment uit van TLS 1.2.
BEV 6	De gegevens die autonoom worden uitgewisseld met de fabrikant van de storage appliance zullen beperkt zijn tot technisch metadata.
BEV 7	De voor TLS gebruikte certificaten zullen zijn geratificeerd door het "Microsoft Trusted Root Certificate Program" en opgenomen zijn in de lijst http://aka.ms/trustcertpartners . <i>Deze eis vervalt indien het een certificaat voor lokaal intern TLS gebruik betreft, dan wordt deze gegenereerd door de vertrouwde PKI van de organisatie.</i>
BEV 8	Van de toegepaste FC switchpoorten moet het type connectie (port type locking) en de connectie zelf (port locking) kunnen worden ingesteld om tot een redelijk beveiligingsniveau te komen.
BEV 9	De gedaanten die een FC poort mag aannemen moet kunnen worden beperkt om te voorkomen dat iedere actieve poort een E_port kan worden.
BEV 10	FC poorten kunnen worden uitgeschakeld als ze niet in gebruik zijn (administrative shutdown).
BEV 11	Het FC netwerk zal een of meer van de volgende authenticatieprotocollen ondersteunen: FCAP, FCPAP, DH-CHAP. Een host of appliance kan zich middels deze protocollen authenticeren bij een FC Fabric.
BEV 12	FC verkeer dat het datacenter verlaat zal versleuteld zijn middels AES-256 (inflight encryption op intersite link).
BEV 13	Om zoveel mogelijk veiligheidsrisico's te elimineren zijn de onderstaande uitgangspunten van toepassing : a) De management omgeving is geïsoleerd en daarmee niet toegankelijk vanaf het internet; b) Alle diensten die niet gebruikt worden, staan uit.

Service levels

Nr.	Omschrijving eis
	Service desk
SLA 1	De Service desk van de leverancier neemt 24/7 storingen/incidenten aan, registreert deze, zet acties in gang om deze af te handelen en bewaakt de doorlooptijd van de afhandeling. De gemeente heeft de mogelijkheid om de status van het incident/de storing elektronisch te raadplegen.
SLA 2	De Service desk draagt zorg voor het relateren van incidenten aan reeds algemeen bekende problemen van de aangeboden producten.
SLA 3	<p>De Opdrachtnemer maakt voor de gemeente inzichtelijk wanneer een incident in behandeling is genomen en de status van het incident. Deze registratie bevat minimaal het volgende:</p> <ul style="list-style-type: none"> • Datum, het tijdstip van de eerste melding, de prioriteit en een uniek storingsnummer binnen de overeengekomen responsetijden; • Herstel met een planning en uitvoering van de herstelwerkzaamheden en eventuele maatregelen die genomen kunnen worden om de impact van de verstoring te minimaliseren; • Het documenteren van de storing en de eventueel doorgevoerde wijzigingen; • Melden van onvoorziene ontwikkelingen die zich voordoen bij het verhelpen van de storing; • Herstelbericht binnen 1 uur nadat de storing/het incident is verholpen.
SLA 4	De Opdrachtnemer is eindverantwoordelijk voor het beheren van gemelde incidenten.
	SLA
SLA 5	De opdrachtnemer stelt vóór implementatie, samen met de gemeente en de fabrikant(en) van de te leveren producten c.q. voorziening een onderhoud- en serviceovereenkomst (SLA) op.
SLA 6	De opdrachtnemer is verplicht support/onderhoudscontracten bij de fabrikant onder te brengen, maar voert zelf ten alle tijden de regie (en treedt op als contactpersoon) naar de gemeente.
SLA 7	Bij onverwachte calamiteiten, niet gerelateerd aan de opdracht (bijvoorbeeld natuurramp), levert de leverancier extra inzet op basis van nacalculatie. De extra inzet zal uitsluitend worden uitgevoerd na overleg en akkoord met de gemeente

Nr.	Omschrijving eis
	Beschikbaarheid
SLA 8	<p>De gegarandeerde beschikbaarheid van de totale voorziening is 24*7 minimaal 99,99% op jaarbasis, mits goed beheerd door de gemeente.</p> <p>A) Onderhoudswerkzaamheden van opdrachtnemer kunnen, indien de gemeente dit vereist, plaatsvinden na werktijden in de avonden, weekenden en op nationale feestdagen.</p> <p>B) Werkzaamheden door de opdrachtnemer worden altijd minimaal 14 werkdagen van tevoren gecommuniceerd.</p> <p>Een uitzondering op de 99,99% eis (inclusief A en B) zijn het oplossen van de incidenten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn, informatiebeveiligingsincidenten en rampen.</p>
	Health check
SLA 9	Om ervoor te zorgen dat de kwaliteit van de voorziening op peil blijft, dient Opdrachtnemer minimaal twee keer per jaar een health/security check op de totale voorziening uit te voeren.
	Beheer en onderhoud
SLA 10	Opdrachtnemer draagt zorg voor het onderhoud waaronder de firmware updates, software updates, begeleiding en implementatie changes en ondersteunt bij (beveiligings)incidentmanagement. De gemeente zal zelf het dagelijks beheer van de voorziening op zich nemen.
SLA 11	<p>Wijzigingen door de opdrachtnemer doorgevoerd in de oplossing welke van invloed kunnen zijn op de data integriteit, informatieveiligheid, privacywetgeving, beschikbaarheid, toegankelijkheid, functionele werking, koppelvlakken, etc. worden vooraf besproken en goedgekeurd door de gemeente. Wijzigingsprocedure met minimaal aandacht voor:</p> <ul style="list-style-type: none"> • Het administreren van significante wijzigingen (Release notes) • Impactanalyse van mogelijke gevolgen van de wijzigingen (Release notes) • Goedkeuringsprocedure voor wijzigingen
SLA 12	Alle wijzigingen worden door de opdrachtnemer altijd eerst getest voordat deze in productie worden genomen en worden via een wijzigingsprocedure doorgevoerd.
SLA 13	Relevante wijzigingen van de opdrachtnemer binnen de oplossing worden gelogd en zijn opvraagbaar door de gemeente.

Nr.	Omschrijving eis
SLA 14	De opdrachtnemer hanteert een degelijk patchschema om alle componenten (zoals firmware, operating systems, applicaties) van de oplossing actueel te houden om verbeteringen door te voeren en bekende fouten op te lossen.
SLA 15	De opdrachtnemer maakt gebruik van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen. Het realiseren hiervan leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillende is te misbruiken.
SLA 16	Medewerkers van opdrachtnemer bieden ondersteuning in de Nederlandse of Engelse taal in woord en geschrift.
SLA 17	Opdrachtnemer is verantwoordelijk voor het aanleveren en actueel houden van een contactenmatrix op functieniveau van alle betrokken medewerkers van zowel de opdrachtnemer als de gemeente.

SLA 18

Meldingen/Incidenten

De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de Oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA).

De gemeente bepaalt de prioriteit van incidenten.

De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de Oplossing. De Opdrachtnemer maakt voor de gemeente inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.

Ten aanzien van de reactie- en oplossingstijden wordt het volgende bepaald:

Categorie	Omschrijving	Reactietijd	Oplossingstijd
Prioriteit 1: Kritiek	Verstoring levert ernstige gevolgen op voor de dienstverlening op bedrijfskritische processen van de gemeente	Onmiddellijk (24/7)	Oplossingsrichting binnen 1 uur na aanmelding Oplossing binnen 4 uur na aanmelding
Prioriteit 2: Hoog	Verstoring levert ernstige gevolgen op voor redundantie of voor de dienstverlening op niet bedrijfskritische processen van de gemeente.	1 uur (24/7)	Oplossingsrichting binnen 4 uur na aanmelding Oplossing binnen 8 uur na aanmelding
Prioriteit 3: Middel	Verstoring levert gevolgen op voor de dienstverlening op niet bedrijfskritische processen van de gemeente maar een alternatief is beschikbaar.	4 uur (24/7)	Oplossingsrichting binnen 1 dag na aanmelding Oplossing binnen 2 dagen na aanmelding

Nr.	Omschrijving eis
	Prioriteit 4: Klein Gebruikersvragen 24 uur (op werkdagen tussen 08.00 en 17.00 Antwoord binnen 1 week uur) na aanmelding
	Beveiligingsincidenten
SLA 19	De gemeente heeft informatiebeveiliging hoog in het vaandel staan en verwacht dat opdrachtnemer hoge prioriteit geeft aan het snel installeren van de laatste beveiligingspatches. Een beveiligingsincident is een enkele of een serie van ongewenste of onverwachte gebeurtenissen die een kans hebben op het veroorzaken van een ramp, het compromitteren van bedrijfsprocessen en een bedreiging vormen ten aanzien van de beveiliging. Iedere inbreuk op de beveiliging, waarbij de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie in gevaar is of kan komen wordt hieronder verstaan.
SLA 20	Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig zijn, worden onmiddellijk gemeld aan en besproken met de gemeente.

Nr.	Omschrijving eis															
SLA 21	<p data-bbox="352 499 1374 568">Een kwetsbaarheid wordt geclassificeerd en afgehandeld binnen de hersteltijd zoals hieronder geschetst.</p> <table border="1" data-bbox="352 645 1374 1592"> <thead> <tr> <th data-bbox="352 645 839 705">Categorie</th> <th data-bbox="839 645 1102 705">Reactietijd</th> <th data-bbox="1102 645 1374 705">Hersteltijd</th> </tr> </thead> <tbody> <tr> <td data-bbox="352 705 839 936"> Extreem Extreem hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke catastrofale gevolgen op het gebied van financiën, reputatie etc. </td> <td data-bbox="839 705 1102 936">Onmiddellijk (24/7)</td> <td data-bbox="1102 705 1374 936">Binnen 4 uur na aanmelding</td> </tr> <tr> <td data-bbox="352 936 839 1167"> Hoog Hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke (significante) financieel, reputatie etc. gevolgen </td> <td data-bbox="839 936 1102 1167">1 uur (24/7)</td> <td data-bbox="1102 936 1374 1167">Binnen 8 uur na aanmelding</td> </tr> <tr> <td data-bbox="352 1167 839 1397"> Middel Middelmatig risico op gecompromitteerde beveiligingsinrichting met minimale financieel, reputatie etc. gevolgen </td> <td data-bbox="839 1167 1102 1397">4 uur (24/7)</td> <td data-bbox="1102 1167 1374 1397">Binnen 1 week na aanmelding</td> </tr> <tr> <td data-bbox="352 1397 839 1592"> Laag Laag risico op gecompromitteerde beveiligingsinrichting met meetbare negatieve impact als resultaat </td> <td data-bbox="839 1397 1102 1592">24 uur (24/7)</td> <td data-bbox="1102 1397 1374 1592">Antwoord matrix met voorgestelde oplossingsrichting binnen 1 week na aanmelding</td> </tr> </tbody> </table>	Categorie	Reactietijd	Hersteltijd	Extreem Extreem hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke catastrofale gevolgen op het gebied van financiën, reputatie etc.	Onmiddellijk (24/7)	Binnen 4 uur na aanmelding	Hoog Hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke (significante) financieel, reputatie etc. gevolgen	1 uur (24/7)	Binnen 8 uur na aanmelding	Middel Middelmatig risico op gecompromitteerde beveiligingsinrichting met minimale financieel, reputatie etc. gevolgen	4 uur (24/7)	Binnen 1 week na aanmelding	Laag Laag risico op gecompromitteerde beveiligingsinrichting met meetbare negatieve impact als resultaat	24 uur (24/7)	Antwoord matrix met voorgestelde oplossingsrichting binnen 1 week na aanmelding
Categorie	Reactietijd	Hersteltijd														
Extreem Extreem hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke catastrofale gevolgen op het gebied van financiën, reputatie etc.	Onmiddellijk (24/7)	Binnen 4 uur na aanmelding														
Hoog Hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke (significante) financieel, reputatie etc. gevolgen	1 uur (24/7)	Binnen 8 uur na aanmelding														
Middel Middelmatig risico op gecompromitteerde beveiligingsinrichting met minimale financieel, reputatie etc. gevolgen	4 uur (24/7)	Binnen 1 week na aanmelding														
Laag Laag risico op gecompromitteerde beveiligingsinrichting met meetbare negatieve impact als resultaat	24 uur (24/7)	Antwoord matrix met voorgestelde oplossingsrichting binnen 1 week na aanmelding														

Communicatie

Nr.	Omschrijving eis
COM 1	Opdrachtnemer wijst gedurende de looptijd van de overeenkomst één vast contactpersoon (en een vaste vervanger) aan op operationeel, tactisch en strategisch niveau.
COM 2	De gemeente wijst gedurende de looptijd van de overeenkomst één vast contactpersoon (en een vaste vervanger) aan op operationeel, tactisch/strategisch niveau.

Nr.	Omschrijving eis																
COM 3	<p>Onderstaand schema is een beknopte weergave van de onderwerpen voor de communicatie tussen beide partijen. Communicatie op de genoemde niveaus vindt alleen met de daarvoor geautoriseerde personen plaats. Rapportages worden door de Opdrachtnemer tijdig ter beschikking gesteld. De communicatie vindt plaats op de volgende niveaus:</p> <table border="1" data-bbox="368 712 1393 2013"> <thead> <tr> <th data-bbox="368 712 523 772">Wat</th> <th data-bbox="523 712 778 772">Wie</th> <th data-bbox="778 712 986 772">Frequentie</th> <th data-bbox="986 712 1393 772">Bespreekpunten</th> </tr> </thead> <tbody> <tr> <td data-bbox="368 772 523 1265">Operationeel overleg</td> <td data-bbox="523 772 778 1265">Opdrachtnemer De gemeente: Systeembeheer</td> <td data-bbox="778 772 986 1265">In overleg, afhankelijk van de voortgang/ werkzaamheden</td> <td data-bbox="986 772 1393 1265">Samenwerking Voortgang werkzaamheden Klachtenafhandeling Openstaande offertes Planningen Calamiteiten Facturatie Verbetervoorstellen</td> </tr> <tr> <td data-bbox="368 1265 523 1615">Tactisch overleg</td> <td data-bbox="523 1265 778 1615">Opdrachtnemer De gemeente: Contractmanager Teammanager ICT Systeembeheer</td> <td data-bbox="778 1265 986 1615">2 x per jaar</td> <td data-bbox="986 1265 1393 1615">Evaluatie samenwerking/ projecten Verbetervoorstellen Calamiteiten Financieel Beoordeling SLA</td> </tr> <tr> <td data-bbox="368 1615 523 2013">Strategisch overleg</td> <td data-bbox="523 1615 778 2013">Opdrachtnemer De gemeente: Contractmanager Teammanager ICT Systeembeheer CISO</td> <td data-bbox="778 1615 986 2013">1 x per jaar</td> <td data-bbox="986 1615 1393 2013">Contractafspraken Ontwikkelingen bij de gemeente/Opdrachtnemer Calamiteiten Marktontwikkelingen Meerjarenvisie Verbetervoorstellen</td> </tr> </tbody> </table>	Wat	Wie	Frequentie	Bespreekpunten	Operationeel overleg	Opdrachtnemer De gemeente: Systeembeheer	In overleg, afhankelijk van de voortgang/ werkzaamheden	Samenwerking Voortgang werkzaamheden Klachtenafhandeling Openstaande offertes Planningen Calamiteiten Facturatie Verbetervoorstellen	Tactisch overleg	Opdrachtnemer De gemeente: Contractmanager Teammanager ICT Systeembeheer	2 x per jaar	Evaluatie samenwerking/ projecten Verbetervoorstellen Calamiteiten Financieel Beoordeling SLA	Strategisch overleg	Opdrachtnemer De gemeente: Contractmanager Teammanager ICT Systeembeheer CISO	1 x per jaar	Contractafspraken Ontwikkelingen bij de gemeente/Opdrachtnemer Calamiteiten Marktontwikkelingen Meerjarenvisie Verbetervoorstellen
Wat	Wie	Frequentie	Bespreekpunten														
Operationeel overleg	Opdrachtnemer De gemeente: Systeembeheer	In overleg, afhankelijk van de voortgang/ werkzaamheden	Samenwerking Voortgang werkzaamheden Klachtenafhandeling Openstaande offertes Planningen Calamiteiten Facturatie Verbetervoorstellen														
Tactisch overleg	Opdrachtnemer De gemeente: Contractmanager Teammanager ICT Systeembeheer	2 x per jaar	Evaluatie samenwerking/ projecten Verbetervoorstellen Calamiteiten Financieel Beoordeling SLA														
Strategisch overleg	Opdrachtnemer De gemeente: Contractmanager Teammanager ICT Systeembeheer CISO	1 x per jaar	Contractafspraken Ontwikkelingen bij de gemeente/Opdrachtnemer Calamiteiten Marktontwikkelingen Meerjarenvisie Verbetervoorstellen														

Nr.	Omschrijving eis
COM 4	De Opdrachtnemer draagt zorg voor schriftelijke verslaglegging van alle overlegvormen en levert dit binnen 5 werkdagen op aan de gemeente. De Opdrachtnemer is initiatiefnemer met betrekking tot de organisatie van de overleggen, de agenda en de schriftelijke verslaglegging.

Projectmanagement

Nr.	Omschrijving eis
PM 1	In geval van een project neemt Opdrachtnemer de gehele projectleiding op zich, dit betekent dat de Opdrachtnemer verantwoordelijk is voor alles wat nodig is om het project goed te laten verlopen.
PM 2	Opdrachtnemer stelt een projectleider aan die gedurende het gehele project fungeert als aanspreekpunt voor de gemeente. Deze projectleider beheerst de Nederlandse taal in woord en geschrift. De projectleider is bij alle overleggen verplicht aanwezig. Wanneer het nodig is voor de werkzaamheden is de projectleider ook aanwezig op locatie van de gemeente.
PM 3	Opdrachtnemer werkt volgens een planmatig projectaanpak en stelt een projectteam samen met daarin medewerkers van Opdrachtnemer en de gemeente.
PM 4	<p>Elk project start met een startoverleg georganiseerd door Opdrachtnemer. Hierin wordt minimaal het volgende besproken:</p> <ul style="list-style-type: none"> • Details van de werkzaamheden • Planning • Welke onderdelen worden op welk moment door Opdrachtnemer uitgevoerd • Welke taken zijn voor de gemeente <p>Opdrachtnemer stelt vooraf een agenda op welke minsten 1 week van tevoren met de gemeente wordt gedeeld.</p> <p>Opdrachtnemer vraagt van tevoren welke personen vanuit de gemeente aanwezig zullen zijn.</p>
PM 5	De projectleider van Opdrachtnemer voert de coördinatie over alle werkzaamheden in het kader van het project, bewaakt de voortgang en is eindverantwoordelijk voor het behalen van de afgesproken planning.
PM 6	De projectleider van de Opdrachtnemer bewaakt het afgesproken budget en signaleert tijdig wanneer het lijkt dat deze overschreden gaat worden.

Nr.	Omschrijving eis
PM 7	Elke 4 weken vindt er een project/voortgangsoverleg plaats, tenzij er problemen in de planning of uitvoering ontstaan. In dat geval kan de gemeente van Opdrachtnemer eisen dat er binnen 5 dagen na verzoek van de gemeente een extra projectoverleg plaatsvindt. Project- en voortgang overleggen worden niet in rekening gebracht.
PM 8	Projectleider van Opdrachtnemer leidt de project- en voortgang overleggen en is tevens verantwoordelijk voor administratie, besluitlijsten, agenda's en voorbereiding van de benodigde besluitvorming.
PM 9	Opdrachtnemer zorgt voor een vaste vervanger van de projectleider.
PM 10	Voordat gestart wordt met een nieuw project vraagt de gemeente een nadere offerte aan. Zie hiervoor de procedure rondom een nadere offerte.
PM 11	Alle ontwerpen, plannings en overige documentatie met betrekking tot de te implementeren oplossing of eventuele vervolgprojecten worden pas geaccepteerd na goedkeuring door de stuurgroep of een gedelegeerde.

Nadere offertes bij projecten en/of meerwerk

Nr.	Omschrijving eis
OFF 1	<p>Daar waar sprake is van projecten binnen de overeenkomst vraagt de gemeente een nadere offerte aan. Deze nadere offertes voldoen aan:</p> <ul style="list-style-type: none"> • Al het gestelde in dit PvE • Alle werkzaamheden en vereisten uit de aanbestedingsleidraad en bijlagen • Tarieven uit het door Opdrachtnemer ingediende prijzenblad <p>Wanneer dit niet het geval is, Opdrachtnemer kan niet aan de vereisten voldoen, dn heeft de gemeente de mogelijkheid het project buiten deze overeenkomst uit te laten voeren.</p>
OFF 2	Nadere Offertes worden binnen 10 werkdagen na aanvraag opgeleverd en besproken, tenzij partijen anders overeenkomen. Pas na schriftelijk akkoord van de gemeente op de nadere offerteaanvraag mag de nadere opdracht worden uitgevoerd.
OFF 3	Er mogen geen kosten in rekening gebracht worden voor het maken van een nadere offerte en eventueel het plan van aanpak.

Nr.	Omschrijving eis
OFF 4	De nadere offerte moet vergezeld zijn van een open begroting die de tarieven zoals door Opdrachtnemer ingediend bij inschrijving niet overschrijdt (behalve in geval van indexering).
OFF 5	In iedere nadere offerte zal een gestandsdoeningstermijn worden aangegeven. Bij gebrek daaraan geldt een gestanddoeningstermijn van 60 dagen.
OFF 6	Indien blijkt dat tijdens de uitvoering meerwerk wordt geconstateerd doet Opdrachtnemer hiervoor een prijsopgave. Alleen na schriftelijke goedkeuring van de gemeente mag dit meerwerk worden uitgevoerd.

Facturatie

Nr.	Omschrijving eis
FAC 1	<p>Facturatie levering hardware en implementatie/migratiefase</p> <p>De facturatie van de leveringen, implementatie en migratie kosten vindt plaats volgens onderstaande termijnen:</p> <p>Facturatie storage- en storagenetwerkapparatuur:</p> <ul style="list-style-type: none"> • 50% na levering hard -en software • 25% na oplevering • 25% na acceptatie <p>Facturatie van de laatste termijn vindt alleen plaats na afronding en goedkeuring van de gemeente van de werkzaamheden en oplevering van rapporten, garantiecertificaten etc.</p>
FAC 2	<p>Facturatie bij jaarlijkse kosten</p> <p>Jaarlijkse licentie en onderhoudskosten worden 1 keer per jaar vooraf gefactureerd.</p>

Nr.	Omschrijving eis
FAC 3	<p>Facturen worden digitaal in een readable Pdf-document verstuurd naar purmerend@factuurportal.eu</p> <p>De facturen dienen de volgende informatie te bevatten:</p> <ul style="list-style-type: none"> • Factuurdatum • Factuurnummer • Kostenplaatsnummer gemeente • Contactpersoon gemeente • Totaalbedrag exclusief en inclusief btw • Specificatie van de gefactureerde werkzaamheden • Contractnummer <p>Eventueel verdere eisen ten aanzien van facturatie wordt tijdens de implementatieperiode met elkaar afgestemd.</p> <p>Facturen die niet voldoen aan de in deze eis vermelde gegevens worden geretourneerd.</p>
FAC 4	Er worden geen andere bedragen gefactureerd dan datgene wat is geoffreerd en goedgekeurd door Gemeente Purmerend.
FAC 5	Facturen worden digitaal verstrekt binnen 30 dagen na afronding van een fase of opdracht.
FAC 6	De gehanteerde tarieven in de factuur dienen in overeenstemming te zijn met de door de Opdrachtnemer aangeleverde tarieven zoals vermeld in het prijzenblad (bijlage 3) of de nadere offerte, tenzij met de gemeente anders is overeengekomen.

Beëindiging contract/ Retransitie

Nr.	Omschrijving eis
EXI 1	Opdrachtnemer is verplicht mee te werken aan de Exit-werkzaamheden bij het overbrengen van de voorziening naar de door de gemeente geselecteerde nieuwe leverancier. Zo soepel als de migratie naar Opdrachtnemer wordt gewenst, zo soepel wordt dit ook verwacht bij beëindiging van het contract.
EXI 2	<p>Opdrachtnemer waarborgt de continuïteit van haar dienstverlening tijdens de Retransitieperiode. Hierbij dient de Opdrachtnemer te voldoen aan de volgende voorwaarden:</p> <ul style="list-style-type: none">A) Opdrachtnemer draagt de kennis en de middelen van de gemeente over aan de door de gemeente geselecteerde partij, behalve van die zaken waarvan van tevoren expliciet is aangegeven dat deze intellectueel eigendom zijn van Opdrachtnemer;B) Opdrachtnemer stelt in overleg met de gemeente een exitplan op;C) Opdrachtnemer stelt tijdens de exitperiode een projectmanager aan die vanuit Opdrachtnemer verantwoordelijk is voor de Transitie en die voor de gemeente beschikbaar is voor escalaties, klachten en vragen;D) Opdrachtnemer draagt alle door de gemeente of Opdrachtnemer namens de gemeente aangeschafte licenties en data van de gemeente over aan de gemeente op een gestructureerde en gangbare wijze;E) De gemeente blijft eigenaar van al zijn door de gemeente of Opdrachtnemer namens de gemeente aangeschafte hardware, data en licenties;F) Opdrachtnemer zorgt tevens voor een up to date documentatie die nodig is voor installatie en overdracht zodat een goede werking van de voorziening bewerkstelligd kan worden door de nieuwe leverancier;G) Bij beëindiging van de overeenkomst worden alle gegevens, naar keuze van de gemeente, vernietigd of gewist. Hiervan wordt een bewijs van vernietiging door opdrachtnemer aangeleverd.
EXI 3	Uiterlijk 31 maart 2026 stelt Opdrachtnemer een concept Exitplan op. Deze wordt daarna in overleg met de gemeente verder afgestemd en goedgekeurd.