Provincie Noord-Brabant

Bijlage 1: Beschrijving Opdracht ‘Netwerk PNB locaties’

Datum: 4 maart 2025

Casenummer: **C2348739**

Inhoudsopgave

1 Achtergrond en context

Provincie Noord-Brabant (hierna: PNB) is voornemens de dienstverlening voor het netwerkbeheer binnen de PNB locaties (het Provinciehuis en een vijftal zeer kleine locaties) uit te besteden. Deze *Bijlage 1 Beschrijving Opdracht 'Netwerk PNB locaties'* geeft deelnemers aan de aanbesteding inzicht in de gedachtegang van PNB en wat zij zoekt in de te leveren dienstverlening en de dienstverlener. Dit is opgedeeld in een korte beschrijving over PNB en de IT, een visie en beschrijving van de kavel, de doelstellingen en scope van deze opdracht en per scope-onderdeel een meer gedetailleerde beschrijving van welke kwaliteitseisen gesteld worden en welke kwaliteitswensen PNB heeft. Bijlage 2 Huidige situatie geeft een beschrijving van de huidige situatie.
Na de selectiefase zal een geüpdatet versie van deze Bijlage 1 (en van andere Bijlagen) deel uitmaken van de documentatie van de gunningsfase.

1.1 Provincie Noord-Brabant

PNB stáát voor Brabant en de Brabanders. In hun belang neemt de provinciale organisatie initiatieven om maatschappelijke vragen op te lossen. Die vragen liggen op het terrein van ruimte en wonen, natuur en milieu, water en bodem, veiligheid bestuur, economie, kennis en Talentontwikkeling, mobiliteit, energie, landbouw en voedsel, vrije tijd en erfgoed, economie, milieu, mobiliteit en vrije tijd.

Samen, slagvaardig en slim
SAMEN: PNB wil nadrukkelijker kijken of haar besluiten lokaal draagvlak hebben. Zij wil nauwer samenwerken met alle partijen in Provinciale Staten. Ze zoekt naar nieuwe manieren om ervoor te zorgen dat draagvlak onder de Brabantse bevolking nog meer de basis vormt voor haar besluiten, bijvoorbeeld via internetconsultaties en een correctief referendum.
SLAGVAARDIG: De focus ligt op doen. Als hier lokaal draagvlak voor is, versnelt PNB Noord-Brabant de realisatie van een aantal van onze belangrijke grote projecten.
SLIM: PNB zet in op technologische en sociale innovaties. Hierdoor ondersteunt zij niet alleen de Brabantse economie, zij stimuleert ook nieuwe oplossingen voor de maatschappelijke opgaven van vandaag en morgen.

Samenwerking
Dat doet PNB meestal niet alleen. Om haar ambities te halen wordt er veel samengewerkt met onder andere gemeenten, het Rijk, Europa en maatschappelijke instellingen.

Kennis en innovatie
Brabant is een Europese topregio op gebied van kennis en innovatie. Het bestuur van PNB investeert in Brabant om ook in de toekomst die toppositie te kunnen behouden. Want dankzij die toppositie is Brabant een prachtige provincie om in te wonen en te werken.

Kernwaarden
Onze kernwaarden vormen de basis van ons handelen en sturen ons dagelijks werk. Vanuit waarde werken we aan onze missie, visie en ambities en geven we ons samenspel met collega's vorm. De kernwaarden en de invulling ervan vormen een zogenaamde ambtelijke code, het is een afspraak die we met elkaar maken over onze manier van samenwerken. We voeren met collega's en leidinggevenden blijven het gesprek en maken met elkaar en in de teams afspraken over de betekenis van samenwerken vanuit de kernwaarden. Deze kernwaarden zijn:

- Werken vanuit vertrouwen
  Dit begint met elkaar leren kennen en oprechte ontmoetingen. Dit vraagt om zichtbaarheid en vindbaarheid van zowel onze medewerkers als managers: present leiderschap en presente professional.
- Werken vanuit verbinding
  Dit betekent dat we elkaar actief opzoeken, betrekken, samenwerken en elkaar ondersteunen. We investeren in inclusiviteit en creëren een cultuur waarin iedereen welkom is, zijn stem mag laten horen en zich belangrijk onderdeel van het team voelt.
- Werken vanuit verantwoordelijkheid
  Dit betekent dat we handelen met het provinciaal belang voor ogen en dat gezamenlijk uitdragen. We kunnen commitment geven, ook als er soms geen consensus is. We maken onze keuzes transparant en we leggen deze duidelijk uit aan elkaar en aan de Brabander.

Dit wil PNB bereiken door samen, slagvaardig en slim te werk te gaan.
Meer informatie over PNB is te vinden op www.brabant.nl.

1.2 PNB en IT

PNB is een organisatie die constant in beweging is. Deze beweging wordt gevoed vanuit haar visie en ambitie, gestuurd door markt- en maatschappelijke ontwikkelingen, beïnvloed door politieke besluiten en geholpen door technische vernieuwingen. Deze veranderingen hebben sterke invloed op de manier waarop PNB kijkt naar IT en hoe zij e.e.a. vertaalt naar doelstellingen, een bijpassende strategie en het organisatie- en governancemodel. PNB wil IT en het IT-landschap slagvaardiger, wendbaarder en veiliger maken voor al haar stakeholders.

Daarom richt PNB zich nu en de komende jaren met name op:

- Het naar de cloud brengen van het applicatie landschap.
- Data gedreven werken en het delen van data met externe samenwerkingspartners, zoals gemeenten, en burgers.
- Het verhogen van de cyberweerbaarheid met aandacht voor privacy door de sterke stijging van cybercriminaliteit.
- De toename van hybride werken: any time, any place, anywhere.
- Het verbeteren van de verduurzaming van technologie.
- Betalen naar gebruik (indien passend).

Het PNB-doel is om voor alle dienstengebieden een duidelijke roadmap te hebben waarin zowel Life Cycle Management als toekomstige technologische ontwikkelingen zijn vastgelegd zodat deze ook in de uitvoeringsagenda meegenomen worden. Samen met de IT-dienstverleners wil PNB deze roadmaps opstellen en/of verder ontwikkelen. Met het doel blijvend betrouwbare diensten te leveren.

PNB is ambitieus en er is zeker nog veel te doen. Vooral op het gebied van het ondersteunen van data integratie, inzet van AI en van de koppelingen naar de dienstverleners en externe gebruikers. Ook zal binnen de IT-organisatie een verdere professionalisering worden doorgevoerd waar het gaat om de project- en beheeraanpak.

Naast de interne en IT-marktontwikkelingen houdt PNB ook rekening met andere factoren, waarvan, voor IT, wellicht een van de belangrijkste is te vinden in de maatschappelijk ontwikkeling: tekort aan gekwalificeerd personeel. PNB werkt momenteel met een grote externe schil. Hierdoor heeft PNB juist de benodigde groep specialisten aan boord. PNB heeft de ambitie om, zodra duidelijk is welke rollen op de langere termijn nodig zijn, eigen specialisten in dienst te nemen.

Tegelijkertijd wil PNB zo veel als mogelijk haar standaard IT-dienstverlening uitbesteden aan gespecialiseerde marktpartijen. Partijen die bij uitstek geschikt zijn om diensten die voor PNB als gespecialiseerd worden gezien als standaard dienst te leveren. Dit maakt dat IT PNB zich kan richten op datgene waaraan ze werkelijk waarde toevoegt: “de business”. Dit zal het IT-landschap en daarmee PNB slagvaardiger, wendbaarder en veiliger maken voor al haar stakeholders.

1.3 Highlights IT-organisatie

De huidige IT-organisatie van PNB heeft de verantwoordelijkheid voor IT-regie gecombineerd met verantwoordelijkheden op operationeel gebied. PNB wil haar IT-organisatie nog beter gaan positioneren als partner voor de business en heeft daarop haar structuur aangepast.
In de nieuwe structuur staat de regierol en de daarmee samenhangende activiteiten op het gebied van supply en demand management centraal. Activiteiten die geen relatie hebben met regie worden óf elders in de organisatie belegd, óf (op termijn) ondergebracht bij dienstverleners zodat de juiste focus gerealiseerd wordt.

De nieuwe regieorganisatie bestaat uit een vijftal onderdelen met een duidelijke focus:

1. *I-advies* vormt een belangrijke schakel tussen bedrijfsvoering en IT;
2. *Project- en programmamanagement* richt zich op de realisatie van projecten voor vernieuwing of verbetering van de dienstverlening;

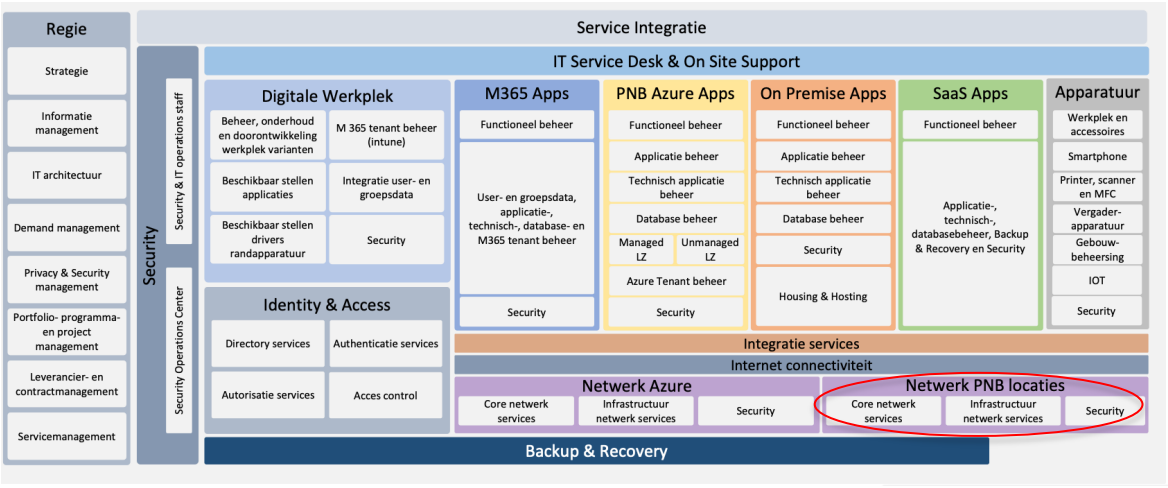
3. Het *serviceteam cloud en platformen* richt zich op de optimale inzet van cloud en platform én van de netwerkomgeving;
4. Het *serviceteam digitale werkplek* richt zich op de werkplek en de servicedesk;
5. *Service- en contractmanagement* richt zich op servicemanagement en contract- en leveranciers-management, evenals het licentiemanagement (SAM).

De invoering van de nieuwe structuur van de regieorganisatie is gestart in 2023 en het project loopt door tot 2025. De nieuwe structuur van de regieorganisatie zal operationeel zijn voor gunning van de kavel Netwerk.

1.4 IT-sourcing strategie

PNB heeft in 2023 haar IT-sourcing strategie herijkt. De belangrijkste doelstelling hierbij is dat PNB maximaal overzicht, inzicht, rust en grip heeft, en dat ze de “time-to-market” weet te verbeteren.
In de IT-sourcing strategie is, op basis van criteria, bepaald welke IT-werkzaamheden en diensten PNB zelf uitvoert en welke werkzaamheden en diensten bij specialistische dienstverleners belegd worden. Onderstaande afbeelding geeft aan welke onderdelen (kavels) PNB onderkent:

Deze aanbesteding betreft Kavel D (rood omcirkeld): deze bestaat uit de dienstverlening met betrekking tot het Netwerk op de PNB locaties.



2 Visie, doelstellingen en scope van de opdracht

2.1 Visie op het netwerk

PNB gaat het beheer van het lokale netwerk in het Provinciehuis in ’s-Hertogenbosch (en een vijftal kleine locaties in de provincie) inclusief een aantal diensten op dat netwerk heraanbesteden.
Hoewel bij PNB de beweging naar de cloud in volle gang is, ziet PNB ook dat een aantal diensten in eigen huis (dat wil zeggen: on premise, gehost op systemen in de MER in het Provinciehuis) zullen blijven bestaan. Sterker nog, gezien de ontwikkelingen in de buitenwereld zou het zo kunnen zijn dat de voorziene ‘beweging naar buiten’ in de toekomst beperkter zal blijken dan tot voor kort werd verwacht. In ieder geval zal een lokaal netwerk (LAN en WLAN in het gebouw) en een lokaal datacenter LAN te allen tijde blijven bestaan, waardoor de netwerkvoorzieningen eveneens te allen tijde betrouwbaar, beschikbaar en veilig moeten zijn. Dit geldt uiteraard ook voor de aan het lokale netwerk gekoppelde voorzieningen, zoals externe verbindingen, internet- en Azure-koppelingen en (ook IoT) devices. Het beheer van deze voorzieningen zelf valt buiten de scope van de aanbesteding maar het aanbieden, onderhouden en veilig houden van de koppelvlakken valt wél binnen scope.

Een aantal jaren geleden voorzag PNB de intrede van ‘connectivity as a service’, waarbij PNB niet langer zelf eigenaar van de apparatuur zou zijn. Hiervan is PNB teruggekomen. PNB is en blijft eigenaar van de bestaande en toekomstige netwerkapparatuur en van de (support-)licenties daarop. Aanschaf daarvan valt dan ook buiten de scope van de aanbesteding. Het dagelijks behéér van de apparatuur, de rapportages daarover, het verwerken van incidenten, problems en changes die gerelateerd zijn aan deze apparatuur valt wél binnen scope van de aanbesteding.

Hoewel het Provinciehuis uiteraard centraal staat in de dienstverlening zijn er een vijftal buitenlocaties waar een (zeer klein) lokaal netwerk bestaat. Gedurende de looptijd van het contract kunnen dat er meer of minder worden. Momenteel is het beheer hiervan nog een ‘grijs gebied’. In de visie van PNB valt het bieden van een beheerbare netwerkoplossing voor ‘kleine locaties’ binnen de scope van de aanbesteding, zodat ook buiten het Provinciehuis efficiënt en veilig gewerkt kan worden.

Overigens bevinden zich op het gebruikersnetwerk nauwelijks nog werkplekken (PC’s) in een intern VLAN: nagenoeg alle werkplekken zijn laptops of andere devices die via het untrusted (W)LAN connecteren met de buitenwereld (bijvoorbeeld naar M365 applicaties of naar W365/AVD werkplekken t.b.v. ‘interne’ connectiviteit). De resterende PC’s (enige tientallen) staan op de nominatie om uitgefaseerd te worden. In de visie van PNB verdwijnt het interne werkplek-VLAN op termijn nagenoeg volledig, op enkele ‘specials’ na. Inmiddels is er, conform PNB’s eerdere visie, binnen het LAN geen sprake meer van een lokale telefonie omgeving. Telefonie wordt volledig als clouddienst afgenomen en bestaat op het LAN slechts nog uit een VoIP-VLAN.

2.2 Doelstellingen van de opdracht

Met deze aanbesteding zoekt PNB een partner die:

1. Continuïteit garandeert: de partner heeft de schaal en expertise en de tooling om de dienstverlening stabiel, veilig en toekomstgericht over te nemen/in te richten en te beheren.
2. Innovatief en flexibel beheer biedt: door moderne technologieën en beheermethodieken toe te passen pro-actief kan beheren
3. Samenwerkt en regie invult: voor de netwerkgerelateerde zaken actief de samenwerking opzoekt met leveranciers in aanpalende kavels en/of met PNB.

2.3 Overall scope van de opdracht

Om bovenstaande doelstellingen te bereiken, is een scope gedefinieerd. Op het hoogste niveau bestaat deze uit:

1. Transitie: overname van het as-is beheer van de huidige leverancier, inclusief inrichting van eigen beheer-/monitoring tooling door de nieuwe leverancier
2. Beheer, onderhoud en monitoring: inclusief rapportages, optimalisatie en tijdige advisering over eventueel benodigde hardware-vernieuwing

De te beheren locaties die binnen de scope vallen zijn:

- het Provinciehuis in Den Bosch (95% van de aansluitingen);
- vijf zoutstrooidepots in de provincie en
- de locatie Waterstraat (Brabants Museum).

Ook het beheren van de verbindingen naar die locaties (níet het leveren van de verbinding zelf) valt binnen scope.

2.4 Onderdelen binnen de opdracht

PNB onderkent de volgende onderdelen binnen de kavel Netwerk PNB locaties:

1. Het beheer van het LAN;
2. Het beheer van de WLAN dienst;
3. Beheer en onderhoud netwerkapparatuur (software);
4. Fysiek beheer netwerkapparatuur (MER en SERs);
5. Beheer van beveiligingsinfrastructuur;
6. WAN koppelvlakken.

Onder beheer verstaat PNB beheer conform ITIL: de servicesupport processen, (tweedelijns) servicedesk en service delivery.

2.4.1 Het beheer van het LAN

Dit betreft de bekabelde LAN netwerkinfrastructuur op het Provinciehuis ten behoeve van de end-to-end connectiviteit voor de medewerkers, of juister gezegd: de connectiviteit van alle devices binnen het LAN. Denk hierbij ook aan de verbindingen naar: printers, scanners, narrowcasting, vergaderdisplays, IoT devices, etc. Centraal is het Provinciehuis uitgevoerd met dubbele core-switches in de MER en redundant daarop aangesloten access-switches in de SERs op alle etages. Werkzaamheden op hoofdlijnen:

- Verantwoordelijk voor de bekabelde netwerkinfrastructuur.
- Redundante core- en access-switches beheren en onderhouden.
- 24/7 monitoring en beheer.

2.4.2 Het beheer van de WLAN dienst

Dit betreft beheer van de WLAN netwerkinfrastructuur op locatie op basis van wireless accesspoints, internet router en de WLAN controller. De accesspoints zijn decentraal opgesteld en de WLAN controller staat centraal in de MER. Werkzaamheden op hoofdlijnen:

- Wireless access points en WLAN-controllers onderhouden, inclusief koppeling met Govroam functionaliteit.
- Netwerkprestaties monitoren en optimaliseren.
- Security en firmware-updates beheren.

2.4.3 Beheer en onderhoud van de netwerkapparatuur (software)

Opdrachtnemer is zelf verantwoordelijk voor het gebruik van de correcte softwareversies en tijdige patches/updates, nader vast te leggen in de (change)procedures. Hierbij dienen de (security) advisories gevolgd te worden van de fabrikant.
Upgrade en patching/updates volgen het changeproces. Werkzaamheden op hoofdlijnen:

- Up-to-date houden van netwerksoftware en firmware
- Controle op compliancy en licentiemanagement.
- Patches en updates volgens een gestandaardiseerd change-proces.

2.4.4 Fysiek beheer netwerkapparatuur (MER en SERs)

Plaatsing, aansluiten van fysieke hardware in de MER en SERs, inclusief het vervangen van onderdelen (bijv. een defecte voeding) vallen hieronder, alsmede het verrichten van alle fysieke (bekabelings)werkzaamheden van de LAN bekabeling. Voor de WAN connecties configureert de

opdrachtnemer de netwerkpoort. Het aansluiten van de betreffende (glas-)kabel gebeurt in afstemming met PNB.
Onsite werkzaamheden (zoals het bekabeld aansluiten van apparatuur op het netwerk) worden uitgevoerd door de servicedesk van PNB (OnsLoket). Zoals hierboven al deels aangegeven:

- alle fysieke werkzaamheden binnen de MER (het datacenter in Den Bosch) vallen, voor zover gerelateerd aan netwerkapparatuur, binnen scope van de aanbesteding.
- alle fysieke werkzaamheden binnen de SER (de patchruimtes op alle verdiepingen) die netwerkapparatuur betreffen (switches) vallen binnen scope van de aanbesteding.
- de kabels vanaf het patchpaneel naar de netwerkpoort op de switch in de SERs worden aangesloten door OnsLoket
- het aansluiten van 'end-user devices' (docking stations, desktops, telefoons, displays, dockingwerkplekken) binnen het Provinciehuis wordt uitgevoerd door OnsLoket
- het aansluiten van netwerkapparatuur op de verdiepingen (met name wifi access points) wordt uitgevoerd door de netwerkbeheerpartij. Bouwkundige werkzaamheden stemt de opdrachtnemer af met gebouwbeheer PNB.

Werkzaamheden op hoofdlijnen:

- Onderhouden en configureren van patchbekabeling.
- Vervangen van defecte hardwarecomponenten.

2.4.5 Beheer van beveiligingsinfrastructuur

Dit betreft op netwerkgebied firewalls (Juniper), loadbalancers, DMZ-componenten (F5 (reverse) proxy) en de IPAM/DHCP oplossing (Infoblox).
Werkzaamheden op hoofdlijnen:

- Firewalls, loadbalancers en DMZ-componenten beheren.
- Security monitoring en incidentbeheer.
- Operationele afstemming en samenwerking met SOC-SIEM dienstverlener.

2.4.6 Beheer van de WAN koppelvlakken

Beheer van de contracten van de internetverbindingen ligt bij PNB. In het geval van lijnverstoringen die netwerkbeheerder uit de monitoring constateert schakelt netwerkbeheerder rechtstreeks met WAN/ Internet leverancier. Het koppelvlak van de WAN/internetverbindingen (de configuratie van de netwerkpoort op de buitenzijde van de firewall) valt binnen scope.
Werkzaamheden op hoofdlijnen:

- Configureren en onderhouden van WAN-verbindingen.
- Directe samenwerking met internet- en netwerkleveranciers bij verstoringen.

2.5 Overzicht apparatuur

Zie Bijlage 3 voor een uitgebreid overzicht van de huidige situatie. Voor wat betreft de bestaande apparatuur is de status per februari 2025 als volgt:

Objectsoort Merk Type	Operationeel	Voorraad	Eindtotaal
Access Point	**154**	**30**	**184**
Cisco	**154**	**30**	**184**
C9120AXI	154	30	184
Core switch	**12**		**12**
Cisco	**12**		**12**
Catalyst C9200L	2		2
Nexus 9000	10		10
Edge switch	**95**	**23**	**118**
Cisco	**95**	**23**	**118**
C9200	2		2
Catalyst C2960L	18	6	24
Catalyst C3560CX	4	3	7
Catalyst C9200L	67	14	81
Catalyst C9300	4		4
Firewall	**2**		**2**
Juniper	**2**		**2**
SRX-4200	2		2
Internet verbinding	**3**		**3**
KPN	**3**		**3**
Internet1 - Servers/Trusted	1		1
Internet2 - Clients/Untrusted	1		1
Internet3 - VOIP	1		1
IPAM	**2**		**2**
Infoblox	**2**		**2**
IB-1415	2		2
Loadbalancer	**4**		**4**
F5	**4**		**4**
F5 Big-IP Virtual Edition	4		4
Proxy	**2**		**2**
Forcepoint	**2**		**2**
V5000 G5	2		2
WAN	**3**		**3**
(leeg)	**3**		**3**
Azure Express route 1	2		2
KPN EVPN	1		1
WLC	**1**		**1**
Cisco	**1**		**1**
Wireless Controller Virtual Cluster IP	1		1
Eindtotaal	**278**	**53**	**331**

2.6 Overzicht verantwoordelijkheden

De volgende tabel geeft een overzicht van de verdeling van verantwoordelijkheden tussen de provincie (PNB), de leverancier (LEV) en externe partijen (EXT).

Werkzaamheden	PNB	LEV	EXT
Opstellen High-level architectuur en securitybeleid LAN/WLAN	X		
Onderhoud architectuur en security LAN/WLAN		X	
Bestellen en overdragen van hardware/software	X		
Configuratie hardware/software		X	
Configuratie en beheer van het LAN/WLAN		X	
Performance monitoring en optimalisatie WLAN		X	
24/7 monitoring en incidentrespons		X	
Operationele afstemming en samenwerking met SOC-SIEM dienstverlener		X	
Patching en fysiek onderhoud MER/SERs		X	
Beheer firewalls en security-infrastructuur		X	
WAN-koppelingen en samenwerking externe partijen	X	X	X
Opstellen van richtlijnen voor patchbekabeling	X		
Bestellen en beheren van patchkabels	X		
Onderhoud patchbekabeling		X	
Aansluiten patchbekabeling	X	X	
Release- en changemanagement netwerkapparatuur		X	
Aanschaf netwerkhardware, inclusief onderhoudscontracten	X		
Namens PNB acteren op (onderhouds/support) contracten		X	
Operationeel en tactisch beheer netwerkhardware en acteren t.b.v. vervangen defecte hardware		X	
Beheer en onderhoud van IPAM, DHCP		X	
Configureren en onderhouden firewall-koppelingen		X	
Storingsbeheer en escalaties WAN-verbindingen	X	X	X

2.7 Buiten de scope van de opdracht

De volgende diensten vallen buiten de scope van de opdracht en worden uitgevoerd door de Provincie:

1. Het opstellen van de architectuur en het securitybeleid voor de LAN en WLAN-dienst;
2. Bestellen van de hardware en software voor de LAN en WLAN en uitvoeren van voorraadbeheer voor de LAN netwerkelementen en de WLAN accespoints;
3. Opstellen van richtlijnen voor patchbekabeling;
4. Bestellen van patchkabels en uitvoeren van voorraadbeheer voor werkplekaansluitingen;
5. Onderhouden en indien nodig configureren/aanpassen van de patchbekabeling van de wall outlet naar diverse end-user devices
6. Aansluiten van bekabeling (patchen) tussen patchpaneel en switchpoort in SERs
7. Beheer van de SAN fibre channel switch
8. Beheer telefonie (OnsLoket)
9. Toegangsbeheer MER (Service Delivery Management)
10. Beheer vergaderbordjes en narrow casting (wel PoE aansluiting leveren met VLAN)
11. Idem lockers (maar dan zonder PoE)
12. Idem parkeerinformatieborden

2.8 Mogelijk aanvullende opdrachten (optioneel in scope)

PNB heeft nog een on premise infrastructuur van beperkte omvang in haar eigen datacenter op het Provinciehuis, bestaande uit een zevental servers als virtualisatie hosts en een Storage Area Network (SAN). Deze on premise infrastructuur wordt naar verwachting de komende jaren grotendeels naar de Azure cloud gemigreerd. Hiervoor loopt inmiddels een migratietraject, waarbij het laatste deel vertraging heeft opgelopen. Het beheer van deze on premise infrastructuur heeft onder andere betrekking op het technisch beheer en onderhoud van servers en het SAN (in samenwerking met de dienstverlener) en het aansluiten van de hypervisor en het OS op bestaande backup voorziening. Dit kan onder andere aspecten omvatten zoals het beheer, onderhoud en monitoring van hardware- en virtualisatieplatformen tot en met het OS (aansturen hardware support contracten) en het geven van ondersteuning aan interne en externe applicatie leveranciers.

Het is op het moment van publiceren van deze aanbesteding nog niet duidelijk of het logischer is om het beheer van de on premise infrastructuur onder te brengen bij de netwerkkavel of bij de cloud platform kavel. Zodra duidelijk is wanneer en in welke vorm het migratietraject naar de cloud weer wordt opgestart, wordt duidelijk wat de exacte omvang en specificaties zijn van wat er on premise overblijft en welke specifieke dienstverlening daarop van toepassing is.

Indien die duidelijkheid leidt tot de keuze voor het onderbrengen van deze dienstverlening in de onderhavige opdracht kan de omvang van de overeenkomst worden verhoogd met een maximum bedrag van € 180.000,- per jaar. Deze extra opdracht heeft geen invloed op de uitvoeringsvoorwaarden, noch op de selectiecriteria en maakt evenmin deel uit van uw verzoek tot deelname en/of de beoordeling daarvan. De aard van de opdracht blijft daarmee hetzelfde. Deze optioneel in scope opgenomen extra dienst kan alleen op verzoek van de provincie worden opgestart. Gegadigden kunnen hier geen rechten aan ontlenen.

3 Visie, scope en verwachtingen Transitie

3.1 Visie

PNB ziet de transitie als de overname van de huidige dienstverlening en de bestaande inrichting van het netwerk en deze vervolgens overzetten naar diensten die conform de overeengekomen SLA worden geleverd. Onderdeel van de transitie is ook het inrichten van beheer- en monitoring-tooling, aangezien deze niet overgenomen kan worden. De overname van de dienstverlening van de huidige dienstverlener moet probleemloos en zonder noemenswaardige verstoringen verlopen.

De transitieperiode start met een kickoff waarin alle direct betrokkenen van de dienstverlener, PNB en derde partijen elkaar leren kennen. Hierin wordt tevens de aanpak voor de transitie geschetst zodat iedereen een duidelijk beeld heeft van de aanpak, planning en wat van hem of haar verwacht wordt.

Technische documentatie, kennis over specifieke toepassingen en inzicht in lopende problemen en (openstaande) verbeterpunten vormen vanuit de huidige partij(en)belangrijke input voor een succesvolle transitie. Van de dienstverlener verwacht PNB dat deze voorafgaand aan de transitie een gedegen verificatie doet van het bestaande netwerk en vervolgens tijdens de transitie de lead neemt in het ‘in control’ komen over de voor de netwerkdienstverlening relevante kennis en documentatie en deze waar nodig updatet. Tevens verwacht PNB dat de dienstverlener de acties neemt om (openstaande) verbeterpunten op te lossen en dienstverlening conform SLA te kunnen garanderen zodra de transitie is afgerond.
In de visie van PNB zal in overleg tussen PNB en de opdrachtnemer er in de eerste fase van de transitie gewerkt worden aan een z.s.m. overname van de as-is huidige dienstverlening. Tegelijkertijd zal een verbeterplan opgesteld worden met een brede scope (samenwerking, proces optimalisatie, verbeterde documentatie en besturingsafspraken, netwerkmonitoring, rapportage, e.d.). In een ‘roadmap verbeteringen en innovaties’ wordt beschreven wat er na afronding van de transitie uitgevoerd zal worden.

De transitie wordt aangepakt op basis van een vooraf vastgestelde methodiek (bijvoorbeeld Prince2) met beheersing van doorlooptijd, kwaliteit, budget en risico’s. Hierbij is de governance duidelijk en voor alle betrokkenen inzichtelijk wat van hen wanneer verwacht wordt.
Voor de start van de transitie is duidelijk wat de deliverables inclusief acceptatiecriteria per fase zijn. De deliverables bestaan o.a. uit projectmanagement-, technische- en samenwerkingsproducten, dienstverlening en goverance. De deliverables worden getest op basis van het testproces.
De samenwerking en het gereed zijn voor in beheername wordt in de praktijk, met alle betrokken partijen (latende en ontvangende partij en PNB) getest door middel van dry-runs met vooraf overeengekomen scripts en acceptatiecriteria. Pas als uit de dry-runs blijkt en alle partijen aangegeven hebben gereed te zijn voor de beheerfase vindt overdracht naar de beheerorganisatie plaats.
Decharge, en daarmee afronding van de transitie, vindt pas plaats na in beheername en overeenstemming van eventuele restpunten in de in te richten stuurgroep.

3.2 Scope

Tot de scope van de transitie behoort:

1. Uitvoeren due diligence.
2. As-is overname van het huidige beheer.
3. Inrichten van de gecontracteerde dienstverlening en verantwoordelijkheid van alle onderdelen in scope van het PNB uitgevraagde diensten.
4. Inrichten van het netwerkbeheer en de daaraan gerelateerde diensten.
5. Aansluiten bij de security monitoring en kwetsbaarheden management dienstverlening en het inrichten en uitvoeren van hier benodigde operationele activiteiten.
6. Inrichten en operationaliseren van de organisatie, goverance en samenwerking voor de beheer- en doorontwikkelfase.
7. Koppelen van ITSM-tooling, inclusief aansluiting op de ITIL processen.
8. Overnemen en actualiseren van beheer-, design- en inrichtingsdocumentatie, inclusief toegankelijk maken daarvan voor opdrachtgever.
9. Overnemen van de inzet in de lopende incidenten, problems, changes en projecten.
10. Inrichten en opleveren van netwerkrapportages conform standaarden en uitgangspunten PNB.

11. Opstellen van aansluitvoorwaarden voor derden die willen aansluiten op PNB netwerk.
12. Opstellen van het exit- of retransitieplan.
13. Opstellen van een document met verbetervoorstellen.
14. Oplevering aan de beheerorganisatie en aan PNB voor overgang naar FMO, op basis van ondertekende acceptatiedocumenten.
15. Oplevering van een exit-/retransitie-plan en geformaliseerde afspraken over het onderhoud daarvan.

3.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de transitie het volgende:

1. Gedegen aanpak

PNB verwacht een gedegen aanpak waarmee de dienstverlener invulling geeft aan:

a) De doelstellingen en scope en resultaten van het traject;
b) Een duidelijke aanpak met onderscheid in:
   - Fasen met bijbehorende tijdslijnen van het traject;
   - Transparante faseovergangen;
   - Dechargemomenten waarbij sprake is van een zorgvuldige voorbereiding van de inbedding en overgang;
   - Voldoende aandacht voor kennismaking van PNB en haar organisatieonderdelen;
   - Acceptatiecriteria en acceptatieproces;
   - Verificatie/validatie (inclusief afwijkingenproces van de aannames gedaan bij de inschrijving);
   - Vastgestelde deliverables met heldere en realistische acceptatiecriteria
c) De wijze waarop de bovenstaande scope onderdelen van de transitie worden gerealiseerd.
d) De wijze waarop dienstverlener zorgdraagt dat de kennis en ervaring die over PNB wordt opgedaan tijdens dit traject, gedurende de looptijd van het contract zowel binnen de organisatie (en de ingezette medewerkers) van de dienstverlener geborgd blijft.
e) Duidelijke en realistische randvoorwaarden, aannames en beperkingen waarbij dienstverlener een actieve rol neemt om samen met PNB en andere partijen invulling te geven aan een succesvolle transitie, inclusief het afwijkingenproces indien blijkt dat randvoorwaarden, aannames en beperkingen afwijken.
f) Een duidelijke governance in het plan van aanpak op operationeel, tactisch en strategisch niveau, met onder andere een stuurgroep.
g) Afhankelijkheden met andere lopende projecten en het retransitieplan van de huidige dienstverlener;
h) Belanrijkste risico's en mitigerende maatregelen inclusief een actief kwaliteits-, risico- en issuemanagementproces (voor zowel risico's die binnen als buiten de directe invloedsfeer van dienstverlener liggen).

2. Optimaliseren dienstverlening

PNB verwacht dat waar mogelijk quick-wins worden gerealiseerd tijdens de transitie, die worden meegenomen in de dienstverlening, zodat zo veel mogelijk wordt geautomatiseerd en standaard wijzigingen automatisch kunnen worden uitgevoerd conform SLA. 'Automatiseren' kan technisch zijn, maar kan ook bestaan uit bijvoorbeeld het versimpelen van change-processen, verbeteren afstemming met andere partijen, opschonen/ vereenvoudigen van switch-configuraties, opruimen ongebruikte poorten, etc.

PNB verwacht dat de leverancier een overzicht deelt van de minimaal te automatiseren activiteiten/processen in de transitie periode welke onderdeel zijn van het transitiebudget. De transitieperiode is zo kort als mogelijk met een beperkte freeze-periode, waarbij kwaliteit van procesinrichting en continuïteit van de dienstverlening centraal staan.

3. Intensieve samenwerking

De wijze waarop, conform de visie in hoofdstuk 5, tijdens dit traject intensief wordt samengewerkt met een duidelijke afbakening in rollen en verantwoordelijkheden van en tussen de dienstverlener, het PNB-team, de latende partij en andere betrokken dienstverleners. Dienstverlener maakt duidelijkheid wanneer welke en hoeveel inzet wordt verwacht van eenieder.

4 Visie, scope en verwachtingen Dienstverlening

4.1 Visie

Passend in de visie van PNB besteedt PNB de netwerkdienstverlening uit aan een opdrachtnemer die de schaalgrootte en expertise heeft om voor PNB de continuïteit van de dienstverlening te garanderen.

De opdrachtnemer biedt de netwerkdienstverlening binnen alle door PNB en de wetgeving gestelde kaders en richtlijnen, waaronder de BIO (hoofdstuk 6) en de architectuurkaders (hoofdstuk 8). PNB verwacht dat de Opdrachtnemer bescherming biedt tegen bedreigingen en hiervoor maatregelen implementeert op basis van een goede risicoanalyses en in nauwe samenwerking met opdrachtnemers van andere kavels, waaronder – maar niet uitsluitend – de partijen binnen de SOC-dienstverlening. Het netwerk van PNB is een veilige omgeving die te allen tijde voorzien is van een actueel beveiligingsniveau.

Hoewel het netwerk voor eindgebruikers vaak onzichtbaar is, is het de basis van álle functionaliteit binnen PNB: geen netwerk betekent geen werk voor nagenoeg alle medewerkers in het Provinciehuis! Maar ook verstoringen in het netwerk leiden al snel tot grootschalig productiviteitsverlies en kunnen het bestuurlijk besluitvormingsproces verstoren. PNB verwacht daarom van de opdrachtnemer dat deze zijn dienstverlening naast veilig, ook betrouwbaar en stabiel levert, conform best practices, óók (juist!) bij het uitvoeren van noodzakelijke wijzigingen en updates.
In het geval van een calamiteit (GRIP: Gecoördineerde Regionale Incidentbestrijdingsprocedure) kan het, afhankelijk van het niveau van de calamiteit, in uitzonderlijke gevallen nodig blijken netwerk-technische aanpassingen te doen. PNB verwacht dat in deze situatie de opdrachtnemer vanuit zijn expertise indien nodig acteert en hiervoor organisatorisch is ingericht en dat dit procesmatig is geborgd.
Een ‘hoog-over’ KPI, zoals ‘gebruikerstevredenheid’ vindt PNB van belang en hoewel het netwerk geen *voldoende* voorwaarde is voor die gebruikerstevredenheid, is het daarvoor wel een *noodzakelijke* voorwaarde. Bij een haperende gebruikerstevredenheid verwacht PNB dan ook van de opdrachtnemer dat deze alles in het werk stelt om in nauwe samenwerking met andere kavels (bijvoorbeeld werkplekbeheer of platformbeheer of de leveranciers van externe connectiviteit) de ‘root-cause’ zo snel mogelijk te vinden en snel en adequaat (mee) op te lossen. PNB verwacht zelfs van de opdrachtnemer dat deze zo pro-actief monitort dat PNB al geïnformeerd wordt over netwerkproblemen nog voor dat ze deze zelf heeft ervaren. In maandelijkse rapportages geeft de opdrachtnemer PNB transparant inzicht in wat er zich in die maand op het netwerk heeft voorgedaan, inclusief rapportage over performance en capaciteit. Daarnaast rapporteert opdrachtnemer over genomen stappen en/of verdere mogelijkheden tot optimalisatie van de dienst.

4.2 Scope

Tot de scope van de dienstverlening behoort:

1. Reactief en proactief beheer en onderhoud op een zo hoog mogelijke automatiseringsgraad, inclusief het uitvoeren van service requests en changes.
2. Incidentmanagement: snel identificeren van, reageren op en oplossen van incidenten om de bedrijfs-continuïteit te waarborgen en de impact op de bedrijfsvoering te minimaliseren (conform SLA).
3. Problemmanagement: identificeren, analyseren en oplossen van netwerkproblemen om de stabiliteit en betrouwbaarheid van het netwerk te waarborgen. Het omvat grondige analyses, implementatie van oplossingen, preventie van toekomstige problemen, documentatie, samenwerking met andere teams en continue verbetering.
4. Transparante en periodieke rapportages (bij voorkeur middels real time/near real time dashboards) over de dienstverlening gebaseerd op de SLA en KPI’s, performance en capaciteit inclusief verbetervoorstellen.
5. Deelnemen en actief bijdragen aan de verbetering van de governance zodat deze voldoet aan de randvoorwaarden voor beheer vanuit de dienstverlener en van PNB.
6. Aansturen van PNB en/of partners binnen PNB en samenwerken met PNB en/of partners buiten PNB zoals beschreven in hoofdstuk 5.
7. Opstellen, up-to-date houden en beschikbaar stellen van de documentatie, CMDB en architectuurdesigns (HLD / LLD) van alle onderdelen van het PNB netwerk op locatie, binnen het PNB on-premise datacenter en van de kleine locaties.

8. Configuratiemanagement: leverancier is verantwoordelijk voor het up-to-date houden van de CMDB voor de op zijn dienst van toepassing zijnde assets, ook al zijn deze eigendom van PNB.
9. Leverancier is verantwoordelijk voor backup en restore van de configuraties van de netwerkapparatuur.
10. Leverancier levert een (near) real-time koppeling met de ITSM tool van PNB voor incident-, change- en problemmanagement en configuratiemanagement.
11. Opstellen roadmap voor lifecycle management
12. Opstellen, up-to-date houden en beschikbaar stellen van het exit-/retransitieplan.
13. Implementeren en bewaken van de van toepassing zijnde security en compliancy eisen en voldoen aan eisen en aansluitvoorwaarden gesteld vanuit de SOC-dienstverlening, inclusief audit en rapportage.
14. Gezamenlijk met de dienstverlener van Kavel C (Cloud en Platform) bewaken van de demarcatie tussen beide kavels en waar nodig afstemmen en/of ingrijpen. Denk aan de raakvlakken tussen de lokale netwerkinfrastructuur en de configuratie daarvan en de netwerkinfrastructuur binnen de Azure cloud.

4.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de dienstverlener het volgende:

1. **Adequaat beheer en ondersteuning conform overeengekomen service levels (continuïteit)**
   Van de dienstverlener wordt verwacht zich te verdiepen in de bedrijfsprocessen van PNB. Hierdoor begrijpt hij wat de impact van verstoringen is op PNB, haar gebruikers, inwoners en externe partijen. De dienstverlening wordt afgestemd op de mate waarin de bedrijfsvoering missie-kritisch is en wat de operationele impact is van verstoringen op de PNB-bedrijfsvoering en op de omgeving. PNB verwacht dat de dienstverlener concrete en adequate servicelevels opstelt, conform levert en PNB wil hiervoor een Service Level Agreement (SLA) afsluiten. Daarbij eist PNB dat de dienstverlener minimaal invulling geeft aan de beschreven servicelevels zoals opgenomen in de eisen omtrent de dienstverlening.

   Naast dat de dienstverlener de continuïteit bewaakt is PNB ook op zoek naar een dienstverlener die aantoonbaar continu meedenkt en proactief is. Het zit zelfs in het DNA van de dienstverlener. PNB wil daarom afspraken maken die dit gedrag continu bevestigen en stimuleren in zowel de SLA als de DAP. Voorbeelden hiervan zijn (niet limitatief):
   a) Standaardiseren van verzoeken en wijzigingen:
      Dienstverlener heeft een gestandaardiseerd, in de regel geautomatiseerd, proces waarmee veel voorkomende verzoeken en wijzigingen worden uitgevoerd. Dienstverlener levert een uitputtend overzicht van deze gestandaardiseerde wijzigingen en verzoeken op. Ze zijn vast onderdeel van de inschrijfprijs c.q. het overeengekomen beheertarief en de lijst groeit continu.
   b) Verantwoordelijkheid:
      - De dienstverlener voelt zich verantwoordelijk en pakt ook de verantwoordelijkheid voor beheer en onderhoud.
      - Doet er alles aan om verstoringen te voorkomen.
      - Lost verstoringen zo spoedig mogelijk op basis van afgesproken service levels
      - Bewaakt continu de kwaliteit en veiligheid van het netwerk
      - Stelt zich, indien dit nodig wordt geacht, ook constructief kritisch op richting wijzigingsverzoeken.
   c) Parate kennis en ervaring:
      - PNB verwacht dat de opdrachtnemer acteert als ‘trusted advisor’ en meedenkt met de PNB beheerorganisatie bij functionele, technische en/of licentie- vraagstukken
      - Ondersteunt en adviseert bij incidenten, nieuwe verzoeken of wijzigingen adequaat vanuit aantoonbaar parate kennis en ervaring en acteert hierdoor snel.
   d) Technisch testen:
      - PNB verwacht dat de leverancier bij wijzigingen of bij het oplossen van incidenten en problems, altijd eerst zelf de benodigde technische testen succesvol heeft afgerond en de wijziging of oplossing vervolgens ter acceptatie aanbiedt aan een beperkte gebruikersgroep. Dit is in veel gevallen het PNB Testcentrum of de PNB beheerorganisatie.
      - PNB verwacht van de leverancier dat ze zelf en op eigen initiatief zorgdraagt voor de benodigde middelen om deze technische testen te kunnen uitvoeren.

   Naast bovenstaande punten staat PNB open voor aanvullingen van de dienstverlener op zowel de huidige levels als suggesties voor aanvullende afspraken.

2. **Proactief bewaken van kwaliteit**
   Voordat PNB (netwerk)storingen meldt zijn deze al in behandeling genomen door de dienstverlener. Het netwerk en de performance worden permanent gemonitord en waar nodig wordt op bevindingen en verstoringen direct geacteerd.

3. **Lifecyclemanagement**
   PNB verwacht van opdrachtnemer dat ze een gedetailleerd en passend concept Lifecyclemanagement-plan opstelt, wat in ieder geval, maar niet uitsluitend beschrijft:
   - Governance, inventarisatie, uitrol, probleemoplossing, controles, (preventief) onderhoud, updates/patches, upgrades, monitoring, beveiligingsmaatregelen, compliance, evaluatie, optimalisatie, innovatie, roadmap, vervangingen en einde levenscyclus.
   - Integratie en/of koppelingen met andere systemen in relatie tot lifecyclemanagement
   - Budgettering en resourceplanning

   PNB verwacht dat de opdrachtnemer evt benodigde ontbrekende informatie ophaalt bij PNB, het plan finaliseert in overeenstemming met PNB en daarna uitvoert. PNB verwacht verder dat opdrachtnemer het Lifecyclemanagementplan in afstemming met PNB blijvend onderhoudt, aanpast en uitvoert op basis van veranderende kennis, inzichten en afspraken.
   Nota bene: de aanschaf van hardware, inclusief licenties en onderhoudscontracten, doet PNB, op basis van het lifecyclemanagementplan en/of voortkomend uit de hiervoor beschreven governance, zelf.

5 Visie, scope en verwachtingen Regie en Samenwerking

5.1 Visie

In de IT-visie en de sourcing strategie heeft PNB haar doelen en ambitie op het gebied van IT-dienstverlening vastgelegd. De kern van de sourcing strategie is dat PNB zich focust op de overall regievoering over de kavels, samenwerking en het WAAROM en WAT van de dienstverlening. Wat betekent dat de niet-strategische IT-dienstverlening wordt uitbesteed en waar dit al het geval is, blijft dit zo. De IT-dienstverleners richten zich op de inhoud, het HOE en op een optimale samenwerking met PNB. Dit moet voor PNB leiden tot een beter overzicht, inzicht, rust en grip en tot een betere 'time to market' van nieuwe of gewijzigde diensten, het vergroten van het adaptief vermogen van PNB en tot het borgen van de continuïteit van de dienstverlening en expertise.

PNB wil een regiemodel en samenwerkingsmodel implementeren, geënt op het 9-vlaks model van Maes, ITIL en JAV waarin de onderstaande elementen centraal staan:

- *Efficiënte en doelgerichte regie en service integratie (SIAM)*
  Als onderdeel van de regievoering wil de PNB de service integratie rol invullen voor de verschillende dienstenketens. Wanneer PNB op termijn voldoende inzicht en ervaring op dit vakgebied heeft opgebouwd, wordt mogelijk ook de SI-rol uitbesteed.

- *PNB richt zich op het WAAROM en WAT, dienstverleners op het HOE*
  PNB richt zich op het ophalen van de vraag bij de business en de functionele formulering van deze vraag, het WAT en het WAAROM hierachter. De dienstverleners richten zich op de technische- en dienstinvulling van de functionele vraag en daarmee ook op de wijze waarop dit zal plaatsvinden, het HOE. In een enkel geval leggen interne spelregels, beleid of wettelijke kaders enige beperkingen op aan bovenstaande principe. In die gevallen wil of moet PNB zelfs meekijken "onder de motorkap" van de dienstverlener, meedenken over de oplossing. Dit geldt specifiek in de volgende situaties:
  1. Architectuur. PNB kent een aantal uitgangspunten en richtlijnen t.a.v. architectuur die ook raakvlakken hebben met het HOE. Bijvoorbeeld op het gebied van aansluitvoorwaarden en architectuurprincipes of de inzet van TOGAF. Daarnaast wordt een optimale architectuur-aansluiting verwacht tussen de functionele oplossing van de dienstverlener en de architectuur zoals gehanteerd door PNB. Denk hierbij bijvoorbeeld aan de enterprise of referentie architectuur. Dit maakt dat PNB graag meekijkt "onder de motorkap".
  2. Security. Dit is bij uitstek een element waarbij interne regelgeving, beleid en wettelijke voorschriften steeds vaker raakvlakken hebben met en in een enkel geval voorschrijvend zijn v.w.b. het HOE. Soms gaat het over het proces, soms over richtlijnen en soms over techniek.
  3. Regie. De regie over het IT-landschap en de onderliggende dienstverleners ligt bij PNB, waar de operationele regie binnen de keten van de kavel, inclusief de koppeling naar de aanpalende kavels, het werkgebied van de dienstverlener is. Op de koppelvlakken stemmen PNB en de dienstverlener met elkaar af hoe e.e.a. optimaal wordt geïmplementeerd. Gebruik van gezamenlijke (PNB) tooling voor o.a. ITIL is hierbij een belangrijk uitgangspunt.

- *Intensieve samenwerking met dienstverleners*
  PNB streeft naar een langdurige strategische samenwerking met dienstverleners, mogelijk tot wel 10 jaar bij gebleken succesvolle dienstverlening en samenwerking.
  Voor het invullen van dit 'partnership' wil PNB hieraan concreet invulling geven door toepassing van het Joint Added Value (JAV) model. Uitgangspunt hierbij is dat de PNB de dienstverlener 'op de winkel kan laten passen' zonder dat de kassa geteld moet worden.

  Het selecteren van de juiste partner is essentieel, waarbij PNB verwacht dat de dienstverlener verder kijkt dan alleen haar eigen belang, werkterrein of gecontracteerde dienstverlening en er een daadwerkelijk partnership gaat ontstaan. Het partnership leidt tot afgestemde belangen, innovatie en efficiëntere dienstverlening voor PNB én de dienstverlener. De samenwerking is gebaseerd op openheid, transparantie en vertrouwen en past in de visie van PNB als opgave gestuurde overheidsorganisatie.
  De essentie van JAV ligt in leveren van toegevoegde waarde en de vertrouwensrelatie die de juiste context creëert om het te laten ontstaan en gedijen. Hiertoe staan acht elementen centraal die in elke van de drie onderstaande te doorlopen fasen passend moeten worden ingevuld:

1. PNB geeft invulling door een gedegen voorbereiding van de aanbesteding en evaluatie en herinrichting van de eigen regie organisatie. Al in de aanbestedingsfase gaat PNB in gesprek met dienstverleners waarbij ook wordt gezocht naar een optimale cultural- en strategic fit. Dit is een belangrijke randvoorwaarde voor een goede samenwerking.
2. Partijen stemmen met elkaar een heldere, gedragen en duidelijke set afspraken af. Hiermee wil PNB ongecontroleerde escalaties vermijden en perspectief bieden om de vruchten te plukken van gedane investeringen. Heldere (financiële) kaders, dienstbeschrijvingen en servicelevels zijn opgesteld en er is een duidelijke gedragen rolverdeling. Openheid en transparantie ten opzichte van elkaar is essentieel.
3. Gedurende de looptijd van de overeenkomst wordt met geduld en respect gewerkt aan het op- en uitbouwen en onderhouden van een goede relatie. In deze fase wordt door partijen periodiek bij tactisch overleg geëvalueerd en successen worden gevierd.

Voor een beknopte uitleg van de acht elementen en hoe PNB deze vervolgens wil invullen, verwijzen we u naar *Bijlage 11 Samenwerking op basis van Joined Added Value*.

5.2 Scope

Tot de scope van de regie en samenwerking behoort:

1. Samenwerken gericht op continuïteit, stabiliteit, transparantie en betrouwbaarheid waarbij de werkwijze continu wordt geprofessionaliseerd.
2. Deelnemen en bijdragen aan de verschillende overleggen.
3. Transparantie in kosten en rapportages.

5.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de regie en samenwerking het volgende:

1. Bijdrage aan de samenwerking

PNB verwacht dat een dienstverlener verder kijkt dan alleen haar eigen belang, werkterrein of gecontracteerde dienstverlening en er een daadwerkelijk partnership gaat ontstaan. Het partnership leidt tot afgestemde belangen, innovatie en efficiëntere dienstverlening voor PNB én de dienstverlener. De samenwerking is gebaseerd op openheid, transparantie en vertrouwen en past in de visie van PNB als opgave gestuurde overheidsorganisatie. De communicatielijnen zijn op alle niveaus kort. Dienstverlener en PNB weten elkaar snel te vinden. Betrokkenen hebben voldoende mandaat om snel te besluiten waar nodig. PNB verwacht dat de dienstverlener actief bijdraagt aan de samenwerking en het JAV-model adopteert. In de samenwerking spelen houding en gedrag een belangrijke rol. PNB is van mening dat door deze samenwerking de diensten aan afnemers van de dienstverlening en uiteindelijk de PNB-collega's mede succesvol wordt doordat de dienstverlener:

a. In één keer goed en conform verwachting levert;
b. Samenwerking met partners binnen de regie organisatie van PNB opzoekt;
c. Een proactieve houding heeft en eigenaarschap toont om bij te dragen aan het oplossen van meldingen en afhandelen van (security) incidenten;
d. Het principe hanteert van resolve first, discuss later;
e. Proactief verbetervoorstellen doet over de actuele dienstverlenings- en kwaliteitsniveaus en de rapportages daarover;
f. Gevraagd en ongevraagd adviseert en uitdaagt over lopende ontwikkelingen en meedenkt over opvolging van latente behoeften en wensen;
g. Initiatieven realiseert, met een minimale administratieve last voor zowel PNB als dienstverlener zelf;
h. Werkt met standaarden, maar pragmatisch is waar het nodig;
i. Gebruik maakt van de kennis en ervaring van PNB op haar expertisegebieden (architectuur, PNB-organisatie, processen) en zich opstelt als stevige discussiepartner.
j. Indien door dienstverlener zelf of door PNB gewenst, of wanneer de situatie daarom vraagt, activiteiten op de PNB locatie uitvoert en door dienstverlener op PNB locatie deelneemt aan de diverse (strategische, tactische en operationele) overleggen op de PNB locatie in Den Bosch.

2. Operationele regie

PNB verwacht dat dienstverlener zorgdraagt voor de operationele regievoering over de diensten die hij levert en de aansluiting op aangrenzende diensten. Hierbij heeft de dienstverlener een duidelijk beeld van en ervaring met hoe de grensvlakken optimaal wordt ingevuld. De rolverdeling en verwachtingen over en weer zijn voor alle betrokken partijen helder en de communicatie- en escalatielijnen duidelijk. Daarnaast voldoet de dienstverlener aan de aansluitvoorwaarden van de SOC leverancier en informeert de dienstverlener de SOC-dienstverlener tijdig en volledig over de status van security incidenten op netwerkgebied.

3. Koppeling ITSM-tool

Voor een optimale samenwerking tussen opdrachtgever en dienstverlener is een snelle goed werkende koppeling tussen beide ITSM-tools van groot belang. De wijze van koppelen moet de regie en service integratie rol van PNB over alle kavels heen mogelijk maken. De PNB ITSM tool dient de single source of truth te zijn. Dit maakt tevens dat PNB-eigenaar kan zijn van een up to date CMDB. Het configuratie managementproces is naast incident, change en problem management, net als request fulfilment onderdeel van de koppeling. Een continu up to date ITSM tool vraagt een (near) realtime koppeling gebaseerd op API’s.
De dienstverlener verzorgt de API-koppeling vanuit zijn organisatie en onderhoudt deze koppeling tijdens de contractlooptijd. PNB verzorgt de API-koppeling aan zijn kant.

6 Visie op Informatiebeveiliging en Privacy

6.1 Visie

Informatiebeveiliging en de daarmee samenhangend cybersecurity hebben de laatste jaren een grote vlucht genomen. PNB onderkent dat in alle opzichten. Informatie moet voldoen aan de BIV eisen (Beschikbaarheid, Integriteit en Vertrouwelijkheid) en informatiesystemen moeten veilig kunnen worden gebruikt. Niet alleen door provinciale medewerkers, maar ook door samenwerkende overheden, dienstverleners, burgers en bedrijven participeren in de informatievoorzieningen van PNB. Door het toepassen van kaders, wet- en regelgeving zoals bijvoorbeeld de ISO- en BIO-normeringen bouwt PNB aan een veilige omgeving op basis van de onderstaande kernwaarden.

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen inzage, mutatie en verwijdering. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Deze kernwaarden gelden voor alle processen van PNB zodat de informatievoorziening gedurende de hele levenscyclus van informatiesystemen is geborgd. Dit ongeacht de vorm van de technologie en het karakter van de informatie. Informatiebeveiliging binnen PNB beperkt zich dus niet alleen tot de IT-omgeving. Het heeft betrekking op alle gebruikers van de provinciale informatie.

PNB is NEN-ISO27001 gecertificeerd. De organisatie voldoet daarbovenop ook aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een verplicht normenkader opgelegd vanuit de Rijksoverheid en geldt voor overheidsinstanties binnen Nederland zoals bijvoorbeeld rijk, provincies, waterschappen en gemeenten. Bovendien voldoet PNB aan de Europese NIS-richtlijn en is in voorbereiding op zijn opvolger NIS2. Bovengenoemde wet-, regelgeving en normenkaders dienen gezien te worden als de pijlers van de PNB-informatiebeveiliging. Daarnaast heeft PNB ook nog te maken met andere wetgevingen en normenkaders of uitvloeisels daarvan zoals bijvoorbeeld de Archiefwet, Wet Digitale Overheid en Forum Standaardisatie.

Gecertificeerde Dienstverlening

Informatiebeveiliging stopt niet bij de provinciale organisatie. Het maakt in de huidige tijd ook steeds meer deel uit van de bedrijfsvoering van dienstendienstverleners en ketenpartners van of voor PNB. Om deze reden stelt de PNB eisen aan de dienstverlener en de geleverde diensten die onderdeel uitmaken van de keten:

1. Dienstverleners en hun onderaannemers zijn NEN-ISO27001 gecertificeerd (of gelijkwaardig).
2. Alle dienstverlenende producten van de dienstverlener zijn NEN-ISO27001 gecertificeerd.
3. Onderaannemingen van de dienstverlener die bijdragen aan de diensten die worden verstrekt aan PNB zijn NEN-ISO27001 gecertificeerd.
4. De dienstverlener conformeert zich aan de Baseline Informatiebeveiliging Overheid (BIO) en afgeleide wetgeving en/of normenkaders over de volledige scope van geleverde dienstverlening. Na een verplichte audit worden geconstateerde afwijkingen in overleg met PNB binnen een overeengekomen periode ingevuld.
5. De dienstverlener conformeert zich vanaf de publicatie in de Staatscourant aan de toekomstige NIS2 wetgeving en de daaruit voortvloeiende cyberbeveiligingswet (CBW) voor de scope van geleverde dienstverlening.

Samenwerking met securitypartner

PNB heeft een complexe digitale omgeving en heeft daarom diverse gespecialiseerde dienstverleners gecontracteerd. Dit is ook het geval voor security en compliance. Deze dienstverlener levert naast het Security Operations Center (SOC) functioneel beheer op onderdelen zoals SIEM (Security Information and Event Management) en heeft een regievoerende rol ten aanzien van incidenten- en kwetsbaarhedenmanagement. De rol van de security dienstverlener gaat dus verder dan alleen het melden van incidenten en kwetsbaarheden. Hij fungeert als aanjager over incidenten en stelt eisen ten aanzien van security en compliance in de rol van regievoerder over de gehele IT-infrastructuur en de daarmee samenhangende dienstverleners.

Privacy
PNB is gegevensverwerker in de zin van de Algemene wet Verordening Gegevensbescherming (AVG). Dat betekent dat zij voor de uitvoering van haar taken als provincie en als werkgever persoonsgegevens verzamelt en verwerkt. Een adequate bescherming van deze persoonsgegevens is uitermate belangrijk. Burgers, personen uit samenwerkende organisaties en provinciale medewerkers hebben recht op een maximale bescherming van hun persoonsgegevens. PNB voldoet dan ook aan de actuele wetgeving en voorschriften zoals gesteld in de AVG. Dat betekent dat belanghebbenden van PNB mogen verwachten dat zij persoonsgegevens op een rechtmatige, behoorlijke en transparante manier, conform de AVG verwerkt. Dat geldt ook voor alle derde partijen die diensten leveren aan PNB waarbij zij persoonsgegevens verwerken en waarvoor ze verplicht een verwerkersovereenkomst hebben getekend.

6.2 Scope

Tot de scope van informatiebeveiliging en privacy behoort:

1. Het inrichten en onderhouden van de dienstverlening conform de geldende wet- en regelgeving en normenkaders op het gebied van informatiebeveiliging en privacy.
2. Het inrichten en onderhouden van de netwerkinfrastructuur conform de geldende wet- en regelgeving en normenkaders op het gebied van informatiebeveiliging en privacy en/of uitvloeisels van andere van toepassing zijnde wet- en regelgeving.
3. Het continu veilig houden van het PNB netwerk.
4. Inrichten en uitvoeren van de dienstverlening conform de AVG-richtlijnen.
5. Een integratie, dan wel een samenwerking, met andere provinciale dienstverleners op het gebied van security, met name de SIEM/SOC-dienstverlener.

6.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van informatiebeveiliging en privacy het volgende:

1. **Proactieve informatiebeveiliging**
   De dienstverlener is verantwoordelijk voor een adequate en passende inrichting en het actief onderhouden van alle netwerkcomponenten binnen de provinciale IT-infrastructuur. Van de dienstverlener wordt verwacht dat hij volledig transparant is ten aanzien van de beveiligingsstatus. Software is altijd voldoende up-to-date en ligt in lijn met het kwetsbaarhedenmanagement zoals dat wordt voorgeschreven door PNB en de verantwoordelijke dienstverlener. Security incidenten en externe dreigingen worden vroegtijdig ontdekt, gemeld en met passende maatregelen beantwoord, in nauwe samenwerking met de SOC dienstverlener. Dienstverlener hanteert vastgestelde procedures voor het afhandelen van security incidenten. Expertise, autonomie, snelheid en effectiviteit zijn hierin sleutelbegrippen in tegenstelling tot het verwijzen naar administratieve procedures of contractuele afspraken.
   Er wordt proactief onderzoek gedaan naar risico's en dreigingen binnen het verantwoordelijk domein van de dienstverlener. De dienstverlener mitigeert op basis van risico gebaseerde informatiebeveiliging. De dienstverlener beweegt (pro-)actief mee met de veranderende eisen vanuit PNB en/of wet- en regelgeving gedurende de looptijd van de overeenkomst. Daarnaast adviseert dienstverlener PNB proactief ten aanzien van risico's en nieuwe security en privacy gerelateerde oplossingen.

2. **Security als onderdeel binnen de dienstverlening**
   Van de dienstverlener wordt verwacht dat hij ten aanzien van security binnen zijn dienstverlening en de kavel zorgdraagt voor het beheer en het regulier onderhoud waarbij alle securityvoorzieningen en eisen in acht worden genomen. PNB is ervan overtuigd dat dit specifieke, passende en specialistische kennis en ervaring met zich meebrengt. Deze kennis is organisatorisch geborgd en komt tot uiting in functies en rollen bij de dienstverlener zoals CISO, ISO, ISM en/of operationeel security engineers. De provincie verwacht mede dat vanuit deze verschillende rollen op reguliere basis strategische en tactische overleggen plaatsvinden tussen de provincie en de dienstverlener. Ook moet dit specialisme bijdragen aan het adequaat opvolgen en van afhandelen security incidenten of het vertalen van maatregelen uit normenkaders en wet- en regelgeving naar functionele en/of technische oplossingen. De dienstverlener

hanteert standaardprocedures en/of draaiboeken in het geval van verschillende typen security incidenten of calamiteiten.
Operationele securitymedewerkers c.q. het securityteam en/of CIRT (Cyber Incident Response Team) opereert onafhankelijk van reguliere beheerteams waarbij altijd het belang van de klant centraal staat.

3. **Samenwerking met de security dienstverlener (SOC)**
PNB maakt gebruik van een gespecialiseerde securitypartner die is gecontracteerd voor een overkoepelend Security Operations Center (SOC) en het beheren van het Security Information and Event Management (SIEM). Dienstverlener is verantwoordelijk voor de operationele beveiliging binnen de eigen dienstverlening (bijvoorbeeld het doorvoeren van security patches en implementeren van mitigerende maatregelen) inclusief realtime ontsluiting van logbronnen richting het SOC. Ook informatie m.b.t. systeemarchitectuur en -configuratie wordt gedeeld. De aansluitvoorwaarden van de SOC dienstverlener zijn hierin leading.
Dienstverlener zorgt ervoor dat het SIEM voldoende rechten krijgt op de benodigde assets/componenten binnen beheerde infrastructuur. De behoefte van PNB is hierin leidend. Uit de SOC-dienstverlening ontstaan security incidenten die worden opgevolgd door de dienstverlener op basis van het reguliere incidentproces en zoals is overeengekomen met PNB en de security dienstverlener.

PNB is gebaat bij een goede samenwerking tussen de dienstverlener, de SOC dienstverlener en PNB. Dit vraagt om een gezamenlijk risicomanagement met daarin een duidelijke afbakening van het eigenaarschap van te treffen maatregelen. Van de samenwerkende partijen, en dus ook van de netwerkbeheer dienstverlener, wordt verwacht dat de dienstverlening ten aanzien van hoge prioriteit security incidenten 24x7x365 wordt ingevuld volgens de prioriteit P1 zoals vastgelegd in het SLA, inclusief bijbehorende servicelevels en afspraken, bijvoorbeeld ten aanzien van het informeren van PNB. Indien nodig werkt dienstverlener mee een te vormen Computer Security Incident Response Team (CSIRT).

4. **Security-verbeteringen in het netwerk**
De provincie is als overheidsorganisatie gebonden aan wet- en regelgeving waar het gaat om verwerking en opslag van informatie uit verschillende taken met bijbehorende processen binnen de ambtelijke organisatie. Voor informatiebeveiliging zijn de NEN-ISO27001, BIO, NIS2 en de AVG-normenkaders en wetgeving die de inrichting van de IT-infrastructuur direct raken. Maar ook uitvloeisels van deze normenkaders of wetgeving zoals het Forum Standaardisatie of de Wet Digitale Overheid of de Archiefwet drukken hun stempel op het IT-beleid en de technische inrichting. Van de dienstverlener wordt niet alleen verwacht bekend te zijn met de verschillende wet- en regelgeving, maar dat dit ook actief onderdeel is als het gaat om onderhoud, beheer, implementatietrajecten en/of wijzigingsprocedures binnen de ICT-infrastructuur. Dienstverlener verbetert dus de netwerk-infrastructuur op het gebied van securityonderdelen en vertaalt maatregelen vanuit normenkaders of high level designs naar functionele en technische oplossingen verwoord in zogenaamde low level designs.
Vanuit technologisch perspectief wordt gezocht naar een dienstverlener die handelt volgens security-by-design en security-by-default principes en die dergelijke principes ook kan implementeren binnen de aangeboden dienstverlening.

7 Eisen

PNB heeft de volgende overall kwaliteitseisen (knock-out criteria):

#	Eis Algemeen
1.	Dienstverlener verklaart expliciet dat hij voldoet aan alle in de selectieleidraad en daarbij behorende bijlage(n) genoemde voorwaarden en eisen die aan de opdracht zijn gesteld.
2.	Dienstverlener conformeert zich aan geldende en toekomstige van toepassing zijnde wet- en regelgeving.
3.	Dienstverlener conformeert zich aan het voor de scope van de opdracht relevante PNB-beleid.
4.	Dienstverlener conformeert zich aan de marktstandaarden en de standaarden voorgeschreven door het Forum voor Standaardisatie.
5.	Intellectual property t.a.v. data, processen en procedures, maatwerk scripting, designs, documenten, rapportages, logbronnen, IP-rechten, voor zover ze betrekking hebben op de aan opdrachtgever gecontracteerde dienstverlening, zijn en blijven eigendom van provincie Noord-Brabant.
#	Eis Inkoop en contract
1.	ARBIT-2022 voorwaarden zijn van toepassing.
2.	PNB betaalt slechts voor actieve en daadwerkelijke geleverde en door PNB geaccepteerde diensten.
3.	PNB kan marktconformiteit van prijzen en tarieven extern laten toetsen en vaststellen door middel van een benchmark. Dienstverlener verleent hieraan gevraagde bijdrage.
4.	Partijen zullen uitkomst van de benchmark bespreken en hieraan eventueel passende consequenties verbinden.
5.	Dienstverlener gaat akkoord met de Concept Overeenkomst.
6.	Dienstverlener gaat akkoord met de Verwerkersovereenkomst.
#	Eis Taal
1.	Dienstverlener garandeert dat gedurende de uitvoering van de opdracht door alle werknemers en ingezette derden die zorgdragen voor de uitvoering van de opdracht in de contacten met PNB, de Nederlandse taal in woord en geschrift zal worden gebruikt. Tevens verklaart dienstverlener dat bij de uitvoering van de opdracht alle documenten en rapportages in de Nederlandse taal zijn opgesteld. Een uitzondering hierop betreffen technische product handleidingen, die ook in het Engels mogen worden opgeleverd.
#	Eis Documentatie
1.	De dienstverlening dient in zijn geheel beschreven en voor PNB te allen tijde beschikbaar te zijn (voorbeelden, maar niet limitatief: handleidingen, beschrijvingen, designs).
2.	(Technische) documentatie is zo opgesteld dat de continuïteit van de dienstverlening is geborgd, PNB inzicht heeft en sturing kan geven op de geleverde diensten en dat PNB of een derde partij het beheer kan overnemen.
3.	PNB is eigenaar van alle beschrijvingen.
#	Eis prijzen en tarieven
1.	De door de inschrijver aangeboden prijzen en tarieven zijn in Euro (€), all-in, inclusief overige belastingen en/of heffingen, en exclusief BTW.
2.	Eventuele valutawijzigingen zijn voor rekening en risico van dienstverlener.
3.	De dienst wordt op een transparante manier gefactureerd, zodanig dat PNB de rekening begrijpt.
#	Eis architectuur
1.	Dienstverlener sluit haar dienstverlening aan de op architectuur van PNB en voldoet aan de door PNB gestelde aansluitvoorwaarden, architectuurprincipes en werkwijze.
2.	IPv6 en IPv4 moeten in combinatie (‘dual stack’) toegepast kunnen worden op communicatie tussen toepassingen in (een) netwerk(en).
3.	IPv6 moet kunnen worden toegepast op digitale diensten, zoals websites en e-mailservers. Aanvullend moeten apparaten van eindgebruikers in staat zijn om websites, applicaties en andere digitale diensten op het internet te bereiken via IPv6. Als het nodig is, is het toegestaan om aanvullend IPv4 toe te passen.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van de Transitie:

#	Kwaliteitseis
1.	De aangeboden transitie aanpak voldoet minimaal aan de in dit document beschreven beschrijving, uitgangspunten en scope.
2.	Decharge van het traject vindt plaats nadat projectwerkzaamheden zijn uitgevoerd, eventuele restpunten zijn benoemd, gepland en overeengekomen en er een formele overdracht is naar en acceptatie door de beheerorganisatie. Decharge vindt enkel plaats na akkoord PNB.
3.	De implementatie van de transitie wordt uitgevoerd tegen de door Inschrijver afgegeven vaste prijs.
4.	Binnen 3 maanden na de start van de transitie stelt dienstverlener een retransitie- of exitplan op conform de in de Overeenkomst gestelde eisen, waarin de wederzijdse verplichtingen uiteen worden gezet om een geruisloze overgang terug naar PNB of een opvolgende dienstverlener te faciliteren bij beëindiging van de overeenkomst. Het retransitieplan wordt gedurende de looptijd van de overeenkomst minimaal jaarlijks geactualiseerd en besproken met PNB.
5.	Om het gemeenschappelijk belang en de verantwoordelijkheden te benadrukken en het streven naar een effectieve samenwerking tussen PNB, verkrijgende dienstverlener en de latende dienstverlener te bekrachtigen, verklaren PNB en dienstverlener de Gedragscode Retransitie van 15 mei 2014 versie 1.2 van Sourcing Nederland van toepassing. Dienstverlener verklaart dat hij bij het beëindigen van de dienstverleningsovereenkomst 100% medewerking zal verlenen bij de overgang van de dan bestaande dienstverlening naar PNB en/of een derde partij. Dienstverlener borgt dat er geen blokkerende constructies in de diensten of dienstverlening worden gehanteerd die een succesvolle transitie en retransitie in de weg kunnen staan en dat data, informatie en middelen tussen de partijen vrij overdraagbaar is en gebruikt mag worden.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van dienstverlening:

#	Kwaliteitseis
1.	De aangeboden dienstverlening voldoet minimaal aan de in dit document beschreven beschrijving, uitgangspunten, service levels en scope.
2.	De aangeboden dienstverlening geeft volledige dekking aan de scope van de opdracht en de uitgevraagde dienstverlening .
3.	(Technische) documentatie is zo opgesteld dat de continuïteit van de dienstverlening is geborgd, PNB inzicht heeft en sturing kan geven op de geleverde diensten en dat PNB of een derde partij het beheer kan overnemen.
4.	Bij de Inschrijving overlegt dienstverlener een uitputtende lijst van de uitvoeringsprocessen zoals die tijdens de transitiefase en voor overgang naar SLA-gebaseerd beheer (FMO fase) zijn geimplementeerd.
5.	Dienstverlener heeft een vastgesteld continuïteitsplan waarin is opgenomen hoe, in geval van calamiteiten, de getroffen dienst en/of het getroffen informatiesysteem weer zo snel mogelijk operationeel gemaakt kan worden. Dit plan wordt minimaal jaarlijks beoordeeld door of namens PNB en getest.
6.	De opdrachtnemer levert maandelijks een gedetailleerde rapportage over de prestaties van de dienstverlening.
7.	Dienstverlener plant periodiek overleg in met PNB en derde partijen/oplosgroepen, zoals maandelijkse operationele overleggen en kwartaal overleggen op strategisch niveau. In deze overleggen worden de voortgang, prestaties en eventuele knelpunten besproken, evenals plannen voor verbetering van de dienstverlening. Dit overleg draagt bij aan een transparante en constructieve relatie met de opdrachtnemer.
8.	Dienstverlener heeft periodiek geteste procedures voor backup en recovery van informatie en configuratie voor herinrichting en foutherstel van verwerkingen. Dienstverlener conformeert zich aan de kaders en richtlijnen van de dienstverlener die verantwoordelijk is voor het uitvoeren van de reguliere backup and recovery dienstverlening voor de provincie.
9.	PNB is te allen tijden gerechtigd om een audit uit te voeren of uit te laten uitvoeren door een externe door PNB aan te wijzen auditor over de geleverde dienst. Bevindingen komende uit de audit worden door dienstverlener opgelost op zijn kosten.
10.	De dienstverlener draagt er zorg voor dat alle data wordt verwerkt en opgeslagen binnen de Europese Economische Regio (EER). Uitzonderingen hierop zijn alleen toegestaan met expliciete toestemming van de provincie Noord-Brabant.

11.	Alle informatiesystemen ten dienste van de dienstverlener beschikken over voorzieningen voor adequate en actuele bescherming tegen ongewenste invloeden.
12.	De toegekende toegangsrechten van alle voor of bij PNB in te zetten medewerkers en derden namens dienstverlener, worden bij de beëindiging van hun dienstverband, contract of overeenkomst direct verwijderd. Bij wijziging van de functie of rol worden de toegangsrechten direct aangepast.
13.	Voordat een account definitief wordt verwijderd dient dit te worden voorgelegd aan de PNB. Daarbij doet de dienstverlener een check op de bevoegdheden van het te verwijderen account. Mocht blijken dat er door het verwijderen van het betreffende account belangrijke content en/of beheerrechten komen te vervallen die niet (automatisch) worden overgezet naar een ander bestaand account, dan moet dit kenbaar worden gemaakt aan de PNB.
14.	Dienstverlener levert structureel en periodiek rapportages bij voorkeur in een Dashboard. Hij zal minimaal rapporteren over: • Aantal, prioriteit, soort melding (tenminste Incidenten, Problems, Service requests en wijzigingen) • Prestatieoverzichten van afhandeling meldingen (duur openstaande melding, reactietijd, hersteltijd, per categorie) inclusief percentage KPI realisatie • Wijzigingenbeheer: overzicht openstaande en uitgevoerde wijzigingen inclusief KPI realisatie • Trendanalyse over laatste 6 maanden van overeengekomen KPI afspraken • Verbetermaatregelen van service levels indien deze beneden het vereiste niveau zijn of dreigen te raken. • Overzicht van geautomatiseerde processen • Periodiek (minimaal jaarlijks) een technology roadmap • Indien nodig: deelname aan Design Authority (architectuurboard) van PNB • Houdt het HLD up to date
15.	Zie voor minimale service levels op gebied van incident management de onderstaande tabel. De meetperiode voor de opgestelde KPI's betreft één kalendermaand. Voor P1 verstoringen verwacht PNB 24x7 bereikbaarheid van de opdrachtnemer. Provincie Noord-Brabant **Prioriteitenmatrix** Urgentie: Zeer Hoog / Hoog / Medium / Laag Impact: Hoog (1 / 2 / 3 / 4); Medium (2 / 2 / 3 / 4); Laag (3 / 3 / 3 / 4) **Servicelevel**
16.	Dienstverlener garandeert onderstaande beschikbaarheid van de diensten:
17.	Wijzigingsbeheer moet ervoor zorg dragen dat gewenste aanpassingen aan geleverde oplossing (software, omgeving) / dienstverlening een gestructureerde, overzichtelijke en gecontroleerde manier een weg vinden naar het productiesysteem. Zie onderstaand de minimale eisen aan het change management:

Prioriteitcode/kleur	Omschrijving Prioriteit	Reactietijd (prestatieverplichting)	Oplossingstijd (inspanningsverplichting)
1	**Kritiek** - Bedrijfskritisch	< 15 min	< 4 uur
2	**Hoog** – (mogelijk) Bedrijfskritisch	< 30 min	< 8 uur
3	**Medium** - Niet bedrijfskritisch	< 4 uur	< 16 uur
4	**Laag** - Gedocumenteerde fout met workaround	< 8 uur	< 32 uur
5	**Zeer laag**	< 16 uur	5 werkdagen

Tijdvak	Beschikbaarheid	Meetperiode
Servicewindow	Minimale beschikbaarheid 99,5%	1 maand
Onderhoudswindows	Minimale beschikbaarheid 97%	1 maand

	<table><tr><th>Prioriteit</th><th>Norm</th><th>Tijdigheid</th><th>Juistheid</th><th>Volledigheid</th></tr><tr><td>Service request</td><td>Reactietijd: 1 Werkdag Doorlooptijd: 1 Werkdag</td><td></td><td>100% in één keer correct doorgevoerd.</td><td rowspan="3">• 90% binnen de norm afgesloten • 100% binnen 2 * de norm afgesloten</td></tr><tr><td>Standaard wijziging</td><td>Reactietijd: 1 Werkdag Doorlooptijd: 2 Werkdagen</td><td></td><td>100% in één keer correct doorgevoerd.</td></tr><tr><td>Niet standard wijziging</td><td>Reactietijd: 2 Werkdagen Doorlooptijd: 5 Werkdagen, na akkoord van CAB Indien van toepassing: een offerte binnen 5 Werkdagen*</td><td>minimaal 5 Werkdagen voor het beoogde Change-window aangekondigd bij het CAB</td><td>• in maximaal 2 keer goed-gekeurd door het CAB (tijdig, volledig, juist aangeleverd) • 90% in één keer correct doorgevoerd, in het geplande Change-window</td></tr></table>
18.	Dienstverlener koppelt alle relevante logbronnen aan het SIEM van PNB om een permanente stroom van benodigde events te leveren aan het overkoepelend Security Operations Center (SOC) en Security Information and Event Management (SIEM).
19.	Dienstverlener accepteert de aansluitvoorwaarden van de PNB SOC-dienstverlener en hij volgt de security events, gemeld door de SOC-dienstverlener, op conform die aansluitvoorwaarden.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van regie en samenwerking:

#	Kwaliteitseis
1.	De samenwerking geeft minimaal invulling aan de verwachtingen zoals beschreven in dit document.
2.	Dienstverlener realiseert een near realtime koppeling tussen zijn ITSM-tool en de PNB ITSM tool door middel van een API (t.b.v. incident, problem, change en config management en request fulfilment). Indien de ITSM-tool van PNB nog niet operationeel is op het moment van contracteren, realiseert dienstverlener een tijdelijke (email)koppeling tussen zijn ITSM-tool en de servicemanagement tool van PNB.
3.	Dienstverlener borgt gedurende de contractperiode dat er een bij de PNB verwachting passende (mix kennis en ervaring) contactpersoon is als vast aanspreekpunt voor de PNB architectuur board en t.b.v. roadmapgesprekken.
4.	Dienstverlener stelt voor de looptijd van de overeenkomst een vaste contactpersoon voor PNB aan voor escalatiebeheer, samenwerking en support planning.
5.	Dienstverlener is bereid projecten en complexere vraagstukken op locatie in gezamelijkheid op te pakken.
6.	Dienstverlener biedt ten behoeve van IT-meldingen en -vragen een deskundige servicedesk aan, dat wil zeggen 'een tweedelijnsondersteuning', die als aanspreekpunt rechtstreeks in contact staat met *OnsLoket* van de PNB.
7.	Afspraken m.b.t. samenwerking zijn minimaal vastgelegd in het DAP. Wijzigingen in het DAP worden onderling afgestemd en akkoord bevonden.
8.	In geval van calamiteiten of crisis is de directie van dienstverlener rechtstreeks toegankelijk voor het management van PNB.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van informatiebeveiliging en privacy:

#	Kwaliteitseis informatiebeveiliging
1.	PNB eist dat dienstverlener zich minimaal conformeert aan de onderstaande richtlijnen, normenkaders, wet- en regelgevingen of uitvloeisels daarvan die PNB hanteert voor beveiliging van IT-systemen: • BIO-overheid • NIS2 / CBW • Forum Standaardisatie • Provinciale richtlijnen • AVG

2.	Dienstverlener is NEN-ISO27001 gecertificeerd voor de volledige scope van de aangeboden dienstverlening.
3.	Bij gunning volgt een BIO-audit door een door PNB aangewezen onafhankelijk auditor. Dienstverlener werkt hier volledig aan mee zonder enige beperkende maatregelen vanuit de zijde van de dienstverlener.
4.	Dienstverlener voorziet in een security dienstverlening op organisatorisch niveau en heeft de afdoende kennis en expertise als het gaat om onderhoud en beheer op alle security-onderdelen binnen de infrastructuur in het on premise datacenter.
5.	Dienstverlener heeft de kennis- en expertise op het gebied van afhandeling van security incidenten (onderzoek, oplossing en rapportage).
6.	De dienstverlener conformeert zich aan het beleid van de door PNB gecontracteerde security dienstverlener bij de afhandeling van security incidenten inzake het verhelpen van kwetsbaarheden.
7.	Dienstverlener laat periodiek en minimaal eenmaal per jaar een penetratietest uitvoeren door een onafhankelijke partij. De provincie is betrokken bij de keuze van deze partij en ze krijgt inzage in de volledige rapportage. Bevindingen worden door de dienstverlener binnen een afgesproken tijd gemitigeerd of opgelost.
8.	Dienstverlener conformeert zich aan alle werkzaamheden voortvloeiend uit de maatregelen zoals die worden gesteld in de BIO-overheid en geeft daarnaast alle medewerking aan derde partijen die uit hoofde van PNB hiervoor werkzaamheden uitvoeren. Voorbeelden hiervan zijn penetratietesten, kwetsbaarhedenmanagement en auditing.
9.	De provincie behoudt het recht op (permanente) toegang/inzage op alle systeemonderdelen binnen de ICT-infrastructuur. Voorbeelden zijn systeemconfiguratie, logging en rapportage.
10.	Dienstverlener geeft volledige medewerking als het gaat om informatieverstrekking uit relevante logbronnen voor het Security Information and Event Management (SIEM) van PNB om een permanente stroom van benodigde eventlogging te leveren aan het overkoepelend Security Operations Center (SOC).
11.	Dienstverlener neemt in geval van een security incident of calamiteit deel aan een eventueel crisisteam.
12.	Dienstverlener stemt er in toe dat PNB haar invloed behoudt als het gaat om de toe te passen securityoplossingen en waarbij PNB altijd de laatste stem heeft.
13.	PNB bepaalt wie de eigenaar is of wordt van de securityoplossingen/-systemen.
14.	Alle informatiesystemen ten dienste van de dienstverlener beschikken over voorzieningen voor adequate en actuele bescherming tegen ongewenste invloeden.
15.	Ten aanzien van het uitoefenen van onderhoud en beheer conformeert de dienstverlener zich aan de BIO en provinciale richtlijnen waarbij beheertaken en beheerrollen worden gesegmenteerd, de toegang tot inhoudelijke data tot een minimum wordt beperkt alsook een beperking van maximale rechten per beheerrol. Dienstverlener gaat onverminderd akkoord met bijvoorbeeld realtime monitoring, verscherpte toegangsregels of andere maatregelen rondom de inzet en het gebruik van beheerrollen. Dit komt tot uiting in het toegangsbeleid van de dienstverlener t.a.v. beheertaken en beheerrollen.
16.	Er is een demarcatie tussen de bedrijfsvoering van de dienstverlener en die van de ambtelijke provinciale organisatie. Dienstverlener krijgt dan ook op geen enkele manier toegang tot inhoudelijke data van provinciale informatiesystemen als zijnde een ambtelijk medewerker van de provinciale organisatie. Met andere woorden is de dienstverlener geen onderdeel van de ambtelijke provinciale organisatie met daarin de overheidstaken van PNB en de daaruit voortvloeiende processen.
#	Kwaliteitseis informatiebeveiliging Privacy
1.	Dienstverlener conformeert zich aan en gaat akkoord met de provinciale verwerkersovereenkomst op grond van de AVG. Na gunning maken dienstverlener en aanbestedende dienst deze gezamenlijk op en deze wordt door beide partijen ondertekend.
2.	Dienstverlener handelt conform de Algemene wet Verordening Gegevensbescherming (AVG). Alle gegevens door PNB aan dienstverlener ter beschikking gesteld of door de onder de overeenkomst verrichte werkzaamheden aan dienstverlener bekend geworden, zullen anders dan op een door de Nederlandse Wet en regelgeving toegelaten wijze, niet aan derden worden verstrekt.
3.	Persoonsgegevens dienen standaard afgeschermd te zijn en mogen standaard niet openbaar zichtbaar zijn.

4.	Incidenten met betrekking tot privacy worden geregistreerd en conform de verwerkersovereenkomst gerapporteerd aan PNB. Afhankelijk van de grootte, aard en de impact van het incident wordt er een escalatiepad gevolgd waarin PNB tijdig en zo volledig als nodig wordt betrokken.
5.	Alle, en met name privacy gevoelige, data ten aanzien van de aangeboden dienstverlening wordt alleen binnen de Europese Unie (EU) verwerkt en/of opgeslagen. Taken waarbij er geen sprake is van het verwerken van privacy gevoelige data mogen buiten Europees grondgebied worden uitgevoerd, mits hiervoor expliciet toestemming is verleend door de Provincie Noord-Brabant.

8 BIJLAGE: Visie op architectuur

8.1 Architectuurniveaus

PNB onderscheidt verschillende architectuurniveaus, te weten:

- Enterprise architectuur
- Referentie architectuur
- Informatie architectuur
- Applicatie architectuur
- Solution architectuur
- Data architectuur
- Integratie architectuur
- Technische architectuur

Architectuur is een coherent geheel van principes, methoden, modellen en standaarden, die worden gebruikt voor het ontwerp en de realisatie van een bedrijfsorganisatiestructuur, business processen, informatiesystemen en infrastructuur. De organisatie-eigen Enterprise architectuur van PNB is sterk in ontwikkeling en zal de komende jaren verder worden verfijnd.

De voor dit document 2 belangrijkste architectuurniveaus zijn:

a. De referentiearchitectuur zien we als een basisset van principes, methoden, modellen en standaarden, die voor elke provincie uitgangspunt zijn bij gemeenschappelijke ontwikkelingen. Als referentiearchitectuur hanteert PNB de Nederlandse Overheid Referentie Architectuur (NORA) waarvan de PETRA (Provinciale EnTerprise Referentie Architectuur) op aansluit. De PNB Infrastructuur Referentie Architectuur (PICRA)[1] is de cloud en infrastructuur architectuur die concreter invulling geeft aan de technische architectuur vanuit NORA naar PETRA.

a. Solution architectuur zien we als beschrijving van de gewenste oplossing van een specifiek IT-probleem, of het eindresultaat van een IT-project. Een solution-architectuur komt tot stand op basis van de referentie architectuur. Een PSA (Project Startarchitectuur) gebaseerd op de bouwblokken van de referentie architectuur geeft richting en handvatten voor projecten. De PSA is hierdoor richtinggevend en kader stellend voor de totale solution architectuur. HLD(high level)-designs vormen een deeloplossing en gezamenlijk de concrete uitwerking van de totaaloplossing van de solution architectuur. De LLD-designs zijn vervolgens de specifieke invulling van de deeloplossingen afgeleid van de HLD-designs. Gezamenlijk vormen alle designs het geheel van bouwblokken van de totaaloplossing en daarmee de doelarchitectuur.

De overige architectuurniveaus worden verderop in het proces toegelicht in een bijlage.

8.2 PNB Referentie architectuur

IT-infrastructuur binnen PNB wordt geïmplementeerd op basis van de PICRA. De PICRA is een gelaagd model die van onder naar boven wordt doorlopen. De gelaagde vorm maakt het mogelijk om per laag een onderwerp af te bakenen. Elke volgende laag maakt gebruik van begrippen uit de onderliggende laag en dus in voorgaande teksten, wat tot een logische en gefundeerde opbouw leidt.
In de fase waarin low level designs (LLD) tot in detail worden uitgewerkt, wordt gebruik gemaakt van Bouwblokken om per onderdeel een low level design op te leveren.
Het bestaat uit de volgende lagen (layers) en bouwblokken:

- Datacenter layer: Housing
- Core Infra layer: Compute, Storage, Network
- Supporting Infra layer: Backup, Security, Operations Management, etc.
- Middleware layer, Dbases, Integration, etc.
- Applications services: Collaboration, Business applications, etc.
- Presentation services: Client-platform, Web-based, user experience, etc.

[1] De PNB Infrastructuur Cloud Referentie Architectuur (PICRA) is gelijk aan de C2RA, Cloud and Clear Referentie Architectuur en mag gebruikt en toegepast worden in afspraak met de auteur en eigenaar Cloud and Clear IT Consultancy.

- Compliance & Control layer: Confidentiality, Availability, Integrity, Scalability etc.
- Governance & Management layer: Architecture, ITSM, Project Management, etc.

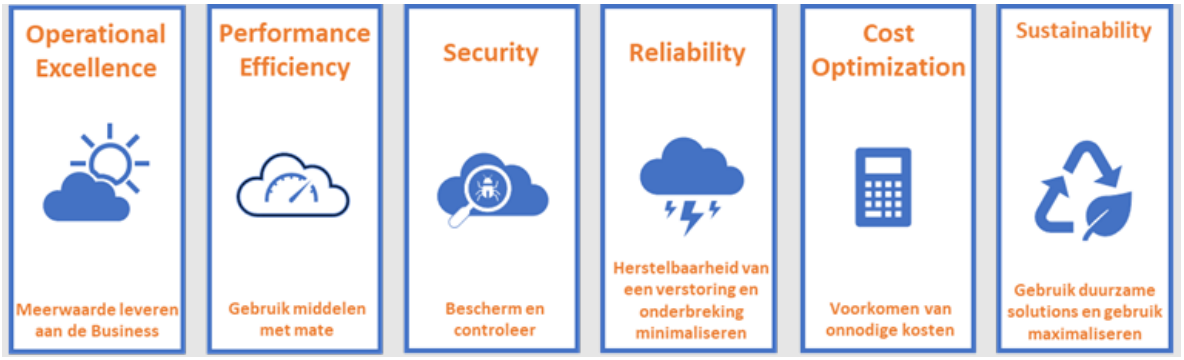
De Application en Presentation services bieden het merkbare en zichtbare: een desktop, applicaties, portals, e-mail, et cetera. Deze worden beheerd en bestuurd door de onderliggende “onzichtbare” infrastructuur, platform en datacenter services. Over alle lagen heen zijn de security en managementservices ingericht, die onder meer de betrouwbaarheid en integriteit bieden, en daarnaast de gereedschappen en voorwaarden leveren om de SLA’s waar te maken.
Met deze architectuur wordt voorzien in een volledig gelaagde, betrouwbare en veilige ICT-infrastructuur. Uitbreidingen op het gebied van applicatiediensten kunnen eenvoudig worden geïmplementeerd, omdat de onderliggende platformdiensten zorgdragen voor zaken als back-up, monitoring, patch management, et cetera.

PICRA heeft als uitgangspunt te werken met referentie architecturen van leveranciers om op basis hiervan de best bewezen oplossingen te implementeren. Hiermee worden onderstaande doelstellingen behaald:

- Snelheid, door sneller infrastructuur te bouwen en te implementeren
- Eenvoud, door de best practices als richtlijn te gebruiken voor het ontwerpen van oplossingen
- Efficiënt, door sneller time-to-value met een hoger ROI te creëren
- Optimalisatie, door uitvoerig geteste workload afstemming met applicaties en hypervisors

8.3 PICRA Framework pilaren

De onderstaande pijlers van PICRA-Framework begeleiden en zijn richtinggevend bij het ontwerpen volgens PICRA van Cloud en Infrastructuur vanuit zes verschillende perspectieven.



8.4 Architectuur principes

De belangrijkste architectuur principes van de PICRA zijn:

1. PNB werkt in de architectuuraanpak pragmatisch, niet bureaucratisch;
2. Architectuur wordt uitgedrukt in principes, modellen, standaarden en richtlijnen;
3. Architectuur zorgt voor kosten-efficiënte oplossingen, waarbij kwaliteit voorop staat;
4. Voorkom onnodig complexiteit en volg principe KISS (Keep It Smart Simple);
5. PNB-beleid geeft sturing aan de architectuur;
6. Er wordt gewerkt met houdbare en duurzame oplossingen en diensten, waarbij o.a. ook de volwassenheid en levensvatbaarheid van het product en de leveranciers worden beoordeeld;
7. Lean principes worden gevolgd: lever alles dat nodig is, lever niets wat niet gevraagd is;
8. Automate everything. Beperk handmatige acties in de run door bij het ontwerp zoveel mogelijk te scripten en automatiseren
9. Everything as Code. De IT-infrastructuur wordt in code configuraties vastgelegd en vanuit centrale repositories gedeployed.
10. Composable & Loosely coupled. Door functie en dienst te scheiden is het eenvoudig om deze los van elkaar aan te passen en te verbeteren.
11. Digital first & first time right. Door processen zo ver mogelijk te automatiseren vinden menselijke interventies alleen plaats waar deze hoge waarde in de keten leveren. Door processen en techniek goed in te richten is de privacy van gegevens geborgd en zijn DPIA's en informatieverzoeken uit te voeren.

12. Security and Privacy by design. Door processen en techniek goed in te richten en verantwoordelijkheden in rollen te borgen, is de gehele bedrijfsvoering robuust en wordt controleerbare kwaliteit geleverd.
13. Marktstandaarden. Gebaseerd op best practices en proven technology. De geboden oplossing en de daarin gebruikte componenten bestaat volledig uit industrie standaarden en bewezen technologieën.
14. Reliable design. Ontwerp met de gestelde kaders en eisen in het achterhoofd en toon aan dat het ontwerp hieraan voldoet.
15. Standaard gaat voor maatwerk. Maatwerk leidt tot inflexibiliteit van de IT-omgeving als geheel. Door maatwerk kunnen vernieuwingen niet eenvoudig worden doorgevoerd of zelfs worden tegengehouden.
16. Bewezen oplossingen. Kies een standaard bouwblok/oplossing (klant-, leverancier- of marktstandaard) in plaats van zelfbouw.
17. Just enough, just in time. Ontwikkel samen die architectuur-componenten waaraan nu behoefte is om verder de realisatie vorm te kunnen geven.
18. TOGAF. Dit model wordt gehanteerd bij het ontwikkelen van de architectuur.
19. Onze architectuur wordt vastgelegd in Blue Dolphin en onderhouden door de landschapseigenaren.