

Beschrijvend document PNB Moderne Werkplek

Datum: 27 maart 2025
Casenummer: C2347381

EIGENDOM EN VERTROUWELIJKHEID

De informatie in dit document is juridisch eigendom van en vertrouwelijk binnen Provincie Noord-Brabant. Het is niet toegestaan dit document te reproduceren, in welke vorm dan ook, mechanische of elektronisch, inclusief elektronische archiefsystemen, geheel of gedeeltelijk te uploaden en/of, al dan niet geautomatiseerd, te verwerken in of door middel van AI-tools, ongeacht het doel hiervan, zonder de schriftelijke goedkeuring van de Provincie Noord-Brabant.

Inhoudsopgave

Inhoudsopgave	2
1 Achtergrond en context.....	4
1.1 Provincie Noord-Brabant	4
1.2 PNB en IT	5
1.3 Highlights IT-organisatie.....	6
1.4 Highlights IT-sourcing strategie	6
2 Scope en doelstellingen.....	7
2.1 Scope	7
2.2 Doelstellingen	7
2.3 Buiten de scope van de opdracht	7
2.4 Mogelijk aanvullende opdrachten (optioneel in scope).....	7
3 De moderne werkplek	9
3.1 Inleiding	9
3.2 Moderne werkplek	9
3.3 Applicaties	9
4 Transitie	11
4.1 Inleiding	11
4.2 Scope	12
4.3 Verwachtingen Transitie.....	12
5 Dienstverlening en doorontwikkeling.....	14
5.1 Inleiding	14
5.2 Scope van de dienstverlening.....	15
5.2.1 Moderne werkplek dienstverlening	15
5.2.2 Applicatie dienstverlening.....	15
5.2.3 Detailbeschrijving scope	15
5.3 Verwachtingen t.a.v. de dienstverlener en de dienstverlening	17
6 Regie en samenwerking.....	19
6.1 Inleiding	19
6.2 Scope	20
6.3 Verwachtingen	20
7 Informatiebeveiliging en privacy	22
7.1 Inleiding	22
7.2 Scope	23
7.3 Verwachtingen	23
8 Eisen.....	25

BIJLAGE: Architectuur bij PNB 30

1 Achtergrond en context

Provincie Noord-Brabant (hierna: PNB) is voornemens de dienstverlening voor de Moderne werkplek dienstverlening uit te besteden. Dit beschrijvend document 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, de visie en beschrijving van de kavel, de doelstellingen en scope van deze opdracht en vervolgens per scope-onderdeel een meer gedetailleerde beschrijving van welke kwaliteitseisen gesteld worden en welke kwaliteitswensen (verwachtingen) PNB heeft. Bijlage 2 Huidige situatie geeft een uitgebreide beschrijving van de huidige situatie.

1.1 Provincie Noord-Brabant

PNB staat 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.

Ambities voor de organisatie

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 topospositie te kunnen behouden. Want dankzij die topospositie 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 governance-model. 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.
- “Alles as-a-Service” inclusief “betalen naar gebruik”.

PNB heeft de afgelopen jaren een snelle ontwikkeling doorgemaakt. Zo is onder andere werken onder architectuur geïnitieerd, ondersteund door de implementatie van Blue Dolphin met het doel inzicht te bewaren en snel te kunnen schakelen bij nieuwe projecten. Voor de belangrijkste dienstgebieden zijn visie en beleidsdocumenten opgesteld. Denk hierbij aan de *Cloud Visie* en *Cloud Governance*, inclusief *Financial Governance*, een *Werkplek Visie* en het backup beleid dat inmiddels grotendeels geïmplementeerd is. Daarnaast heeft PNB veel aandacht voor de inrichting van maatregelen rondom informatiebeveiliging, waar met inzet van nieuwe tooling de belangrijkste bedreigingen inmiddels worden afgedekt. Momenteel wordt hard gewerkt aan het verder vormgeven van het vervolgonderzoek, de analyse en, waar nodig, de opvolging van hieruit voortvloeiende acties.

Om klanten nog sneller te kunnen ondersteunen in hun wensen met migratie naar de cloud, is PNB gestart met een *Competence Center (CC)* wat onboarding ondersteunt en consultancy biedt.

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 streeft ernaar om een aantrekkelijke werkgever te zijn. Op het gebied van IT zien we dat de zeer ervaren IT-specialisten de voorkeur geven aan werkgevers met continu sterk vernieuwende projecten. En hoewel PNB die ook heeft, gaat ook veel aandacht uit naar het borgen van de veiligheid en continuïteit van het IT-landschap. PNB werkt hierbij momenteel met een grote externe schil. Hierdoor hebben we 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.

De snelle ontwikkelingen, het tekort aan interne specialisten, de overgang naar cloud, SaaS en overige as-a-service diensten en de groei van outsourcing van IT-diensten heeft PNB overtuigd om de transitie naar een regieorganisatie door te zetten. En gelijktijdig zo veel als mogelijk haar standaard IT-dienstverlening uit te besteden 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”.

En het 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 de cloud- en Platform en netwerkomgeving en voorziet in roadmap en architectuurprocessen voor de werkplek;
4. Het *serviceteam digitale werkplek* richt zich op de werkplek en de M365 apps;
5. *Service- en contractmanagement* richt zich op servicemanagement en contract- en leveranciersmanagement evenals het licentiemanagement (SAM).

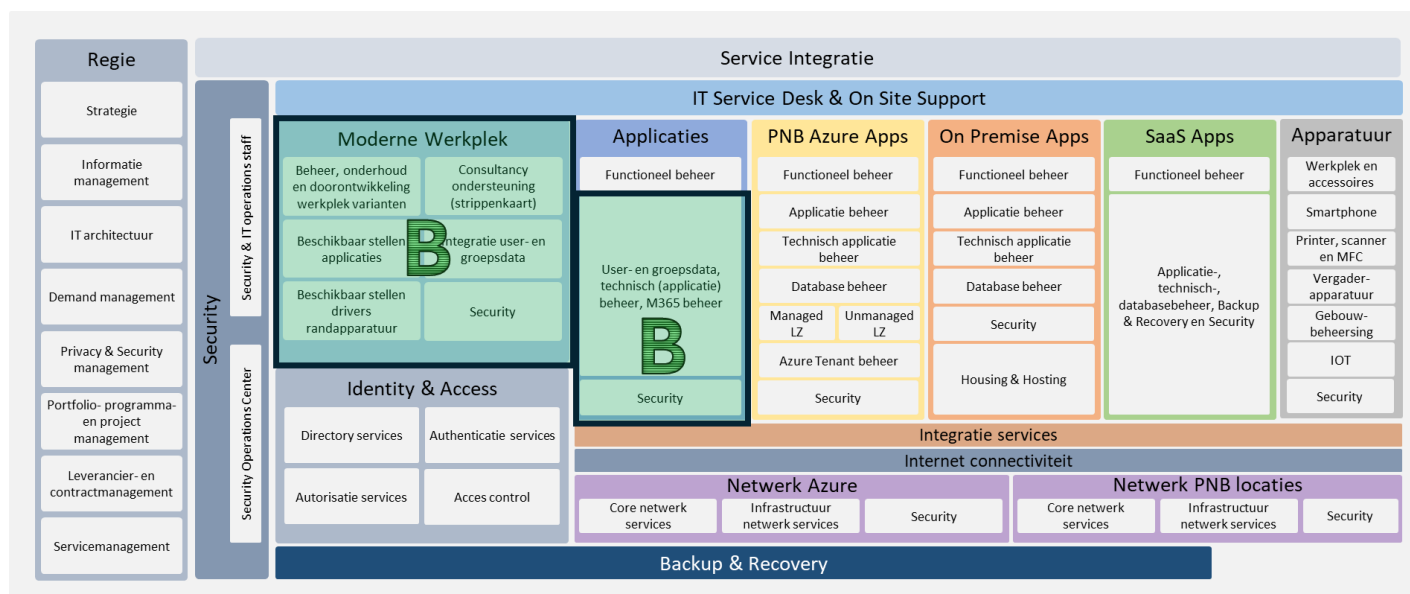
De invoering van de nieuwe structuur van de regieorganisatie is gestart in 2023 en het project loopt door tot medio 2025. Het project loopt parallel door aan deze aanbesteding en de transitie.

Om de bedrijfsvoering van PNB optimaal te ondersteunen is goede samenwerking cruciaal. De regieorganisatie is de verbindende schakel tussen de vraag uit de business en de diensten die door de dienstverleners geleverd worden. Over de regievoering en samenwerking geeft hoofdstuk 4 een nadere toelichting.

1.4 Highlights 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 ze weet de “time-to-market” 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.



Deze aanbesteding betreft kavel B, dat bestaat uit de dienstverlening rondom de moderne werkplek en M365 Apps.

2 Scope en doelstellingen

2.1 Scope

De scope bestaat uit drie hoofdonderdelen:

1. De transitie van de moderne werkplek-dienstverlening inclusief overname huidige dienstverlening.
2. Het beheren, onderhouden en continu verbeteren van de moderne werkplek.
3. Doorontwikkeling gericht op het samen, op basis van mogelijke nieuwe functionaliteit en nieuwe applicaties, verder ontwikkelen van het werkplek landschap.

2.2 Doelstellingen

Met deze aanbesteding wil PNB het volgende bereiken:

1. Een soepele transitie van de (moderne) werkplek- en M365-dienstverlening naar de nieuwe dienstverlener. Het ontwerpen, voorbereiden en realiseren van een uitstekend geplande en beheersbare transitie van de bestaande dienstverlening naar de nieuwe dienstverlener, met minimale verstoring van de dagelijkse werkzaamheden.
2. Het door de dienstverlener inrichten en uitvoeren van de moderne werkplek dienstverlening op basis van een duidelijke regiestructuur tussen PNB en dienstverlener, aansluitend op de wensen van PNB en conform de overeengekomen processen en serviceniveaus.
3. Een werkplek dienstverlening waarbij dienstverlener verantwoordelijk is voor het beheer en de continue doorontwikkeling van de moderne werkplek. Dit omvat het borgen van de beschikbaarheid, veiligheid en continuïteit van de werkplekken en applicaties. En het invulling geven aan de operationele processen zoals incidentafhandeling, regulier onderhoud en monitoring van en sturen op resources en (verbetering van) gebruikerstevredenheid.
4. Het realiseren van een samenwerkingsverband tussen dienstverlener en PNB waarin wederzijds waarde wordt gecreëerd door het continu werken aan veiligheid, kwaliteit, continue verbeteringen en innovatie (doorontwikkeling). Transparantie is het uitgangspunt van de samenwerking.

De scope en doelstellingen worden verder uitgewerkt in de volgende hoofdstukken. Beschreven doelstellingen en scope zijn verder van toepassing op de werkplek verschijningsvormen en applicaties voor zowel de Provincie als de Provinciale Staten (PS) omgeving. Dit zijn beide separaat beheerde omgevingen met eigen Azure en en M365 tenants en volledig van elkaar gescheiden omgevingen i.v.m. wettelijke regelgeving over dualisme.

2.3 Buiten de scope van de opdracht

De volgende diensten vallen buiten de scope van de opdracht:

1. Licenties en hardware
2. IAM
3. 1^e lijn helpdesk of onsite support
4. Adoptieproject
5. Microsoft licenties en spend
6. Microsoft contract: er zal gebruik gemaakt worden van de interprovinciale PNB Enterprise Agreement

2.4 Mogelijk aanvullende opdrachten (optioneel in scope)

Binnen de looptijd van de overeenkomst wil PNB mogelijk een aantal extra diensten afnemen bij de moderne werkplek dienstverlener. Optioneel in scope betekent dat deze aanvullende opdrachten, indien de optie wordt gelicht én PNB en de moderne werkplek dienstverlener tot overeenstemming komen, niet opnieuw aanbesteed hoeven te worden. Het houdt geen verplichting in zich dat PNB deze opdrachten bij de moderne werkplek dienstverlener moet onderbrengen, noch dat de dienstverlener verplicht is die diensten te leveren. Ze maken dan ook geen deel uit van uw verzoek tot deelname en/of de beoordeling daarvan.

1. 1^e Lijns helpdesk/onsite support
PNB beschikt over een 1^e lijns IT helpdesk met on site support, *OnsLoket*. De rol van eerstelijns support is eerste aanspreekpunt voor gebruikersvragen, incidenten, serviceverzoeken en het uitvoeren van enkele taken op het gebied van werkplekbeheer en gebruikersbeheer. De eerstelijns support is verantwoordelijk voor het registreren, categoriseren en waar mogelijk oplossen van incidenten net als voor het doorverwijzen en escaleren van complexe zaken naar de tweede of derdelijns support.

In aanvulling op bovenstaande taken ligt ook de operationele service integratie bij de *OnsLoket*.

Deze taak wordt snel belangrijker en veeleisender dan op dit moment het geval is. Met name omdat de komende 2 jaren meerdere IT kavelen worden uitbesteed. PNB voorziet dat na afloop van alle transitieën en de overgang naar de FMO (Future Mode of Operations) op die kavelen (vermoedelijk 2027) duidelijk wordt of PNB nog voldoende in staat is deze dienst zelf schaalbaar, flexibel, met voldoende kwaliteit en 24x7 te leveren. Is dat niet het geval, zal een besluit worden genomen of de 1^e lijns IT helpdesk inclusief on site support wordt uitbesteed.

Indien de optie wordt gelicht leidt dat tot het onderbrengen van deze dienst in de onderhavige opdracht en kan de omvang van de overeenkomst worden verhoogd met maximaal € 900.000,- per jaar. Deze extra opdracht heeft geen invloed op de overige uitvoeringsvoorwaarden die daarmee gelijk blijven aan hetgeen in deze procedure is vastgesteld. De aard van de opdracht blijft daarmee hetzelfde.

2. Innovatie

PNB heeft een sterke behoefte aan een moderne werkplek dienstverlening waarop continu wordt geïnnoveerd en doorontwikkeld door de dienstverlener. Standaard wijzigingen in de dienst van de dienstverlener en standaard wijzigingen zoals die door Microsoft worden doorgevoerd (ook wel “update” genoemd) vallen in de reguliere dienstverlening en daarmee in het standaard beheertarief (net als grote of complexe changes n.a.v. storingen, correcties of fouten aan de kant van dienstverlener). Daar staat tegenover dat de grote impactvolle functionele wijzigingen die een projectmatige aanpak vereisen optioneel in scope zijn en worden gefinancierd vanuit het daarvoor geoormerkte Innovatie-budget. Onder impactvolle functionele wijzigingen wordt verstaan: nieuwe diensten die nog die nog niet op de PNB-werkplek zijn geïmplementeerd op het moment van contracteren, zoals bijvoorbeeld LLM (Large Language Module)-diensten.

Op voorhand is voor PNB niet te voorzien welke grote functionele wijzigingen door met name Microsoft zullen worden geannonceerd, of die überhaupt relevant en interessant zijn voor PNB, of er voldoende resources beschikbaar zijn om de innovatieprojecten uit te voeren en of er nog voldoende innovatie-budget in het betreffende jaar beschikbaar is. Gedurende de looptijd van het contract zal dienstverlener PNB informeren over potentiële innovatieprojecten en de toegevoegde waarde voor PNB. Aan de hand hiervan zal PNB besluiten of: a) het potentiële project relevant is dan wel voldoende waarde toevoegt, b) er voldoende resources zijn om het project succesvol uit te kunnen voeren, c) er voldoende budget resteert en d) er een bij de verwachtingen van PNB passend voorstel tot implementatie en uitvoering is uitgebracht.

Is aan al deze voorwaarden voldaan kan de omvang van de overeenkomst worden verhoogd door het in opdracht geven van één of meer van deze projecten voor maximaal € 350.000,- per jaar voor contractjaren 1 en 2 en voor maximaal € 100.000,- voor de daaropvolgende contractjaren gedurende de initiële contractlooptijd. Deze extra opdracht heeft geen invloed op de overige uitvoeringsvoorwaarden die daarmee gelijk blijven aan hetgeen in deze procedure is vastgesteld. De aard van de opdracht blijft daarmee hetzelfde.

3 De moderne werkplek

3.1 Inleiding

Snel veranderende behoeften binnen PNB en in de markt, m.b.t. de regelgeving rond beveiligingseisen en de technologische veranderingen hebben hun effect op de moderne werkplek van PNB. Om hier adequaat en tijdig in te kunnen voorzien en op te ontwikkelen is de moderne werkplek van PNB gebaseerd op cloud georiënteerde Microsoft technologie (Microsoft first, cloud first). De nadruk van de moderne werkplek ligt hierbij op het makkelijk, productief en veilig samenwerken door en met gebruikers van de PNB en Provinciale Staten. De moderne werkplek in welke verschijningsvorm dan ook, voldoet altijd aantoonbaar aan informatiebeveiligings- en privacy beleid o.b.v. NIS2, CwB, BIO. Hierbij ook rekening houdend met de richtlijnen naar de open standaarden van Forum Standaardisatie. Dit op basis van het Zero-Trust principe.

3.2 Moderne werkplek

De moderne werkplek van PNB is gebaseerd op moderne cloud georiënteerde Microsoft technologie. Het is een integraal toegangspunt waarmee gebruikers van PNB veilig en eenvoudig snel toegang tot applicaties en data hebben. Afhankelijk van de werkplek verschijningsvorm krijgen gebruikers volledig of beperkte toegang tot applicaties en data. De reden hiervan is dat het beveiligingsniveau geconfigureerd, gemonitord en gerapporteerd kan worden op beheerde apparaten. Daarmee is het controleerbaar, beheersbaar en voldoet aan PNB informatiebeveiligings- en privacy beleid. Om aan de behoeften van gebruikers te voldoen en (deels) toegang te bieden tot applicaties en data van PNB, onderkent PNB de volgende werkplek verschijningsvormen:

- Choose Your Own Device (CYOD); apparaten verstrekt door de provincie.
- Bring Your Own Device (BYOD); eigen apparaten van (externe) medewerkers of dienstverleners.
- Azure Virtuele Desktop (AVD); een virtuele desktop vanuit de Microsoft Azure Cloud.
- Specials
- Smartphones

De belangrijkste van de vijf verschijningsvormen binnen PNB is CYOD, waarbij de laptop het standaard onderliggende device is. Andere varianten zijn o.a. een virtuele werkplek, smartphone, tablet of desktop, waarbij de desktop meestal een special is. In het meest ideale geval is de verschijningsvorm passend bij de specifieke (5) persona's en de gebruikersrol, waarbij voor elke rol een gepersonaliseerde set van apparaten, applicaties, functionaliteiten en dienstverlening beschikbaar wordt gesteld. De moderne werkplek integreert naadloos en gemakkelijk met randapparatuur, zoals vergadersystemen, audiovisuele apparatuur en andere relevante technologische voorzieningen. De moderne werkplek biedt de gebruiker een intuïtieve en consistente gebruikerservaring waarbij applicaties op eenvoudige manier aan de gebruiker ter beschikking worden gesteld. De werkplek voelt voor elke gebruikersgroep natuurlijk aan.

Het managen van de werkplekken wordt voornamelijk gedaan op basis van moderne cloud georiënteerde Microsoft technologie. Dit met als doel snel, veilig en efficiënt applicaties uit te rollen, te updaten of te kunnen verwijderen. Met het voorgaande wordt een veilige moderne werkplek gefaciliteerd die toegang geeft tot PNB data om efficiënt en effectief samen te werken.

Voor de gebruiker doet de moderne werkplek het altijd en overal binnen de kaders van (wettelijke) informatie- beveiligingseisen. Van de moderne werkplek wordt verwacht dat hij een uitstekende en positieve (dus meetbaar en performant, consistent, veilig) gebruikerservaring biedt. Dit ondersteund door tijdige en juiste rapportages en gebruikerstevredenheidsscores.

3.3 Applicaties

In de moderne werkplek van PNB staan samenwerking en productiviteit via en door middel van de juiste set applicaties centraal. PNB biedt op de werkplek een vaste set aan toepassingen. Hierin ziet PNB vanuit beheerperspectief drie clusters terug: standaard applicaties, SaaS en overige applicaties.

1. Standaard applicaties.
PNB heeft een standaard applicatieset. De applicaties (inclusief plug-ins) uit deze set dienen beschikbaar te zijn op alle werkplek verschijningsvormen.

Binnen deze applicatieset speelt M365 een centrale rol bij het beheer van ongestructureerde data binnen PNB, vooral voor wat betreft de werkdOCUMENTEN en samenwerking met interne en externe gebruikers.

PNB streeft ernaar om M365 en de andere applicaties uit de basis applicatieset zo volledig mogelijk uit te nutten m.b.t. de voor de gebruikers relevante functionaliteiten en toepassingen. Dit uitnutten werkt echter pas echt goed indien er voldoende aandacht is voor adoptie van die functionaliteiten. Adoptie op de werkvloer, vanuit de daarvoor aangewezen personen binnen PNB en vanuit de dienstverleners. En adoptie gestimuleerd door de inzet van duidelijke handleidingen, instructies, tips, video, QRG/A en trainingen.

Nieuw voor gebruikers is de toepassing van Copilot in M365, de digitale assistent, die helpt bij het vinden van informatie en die de gebruiker ondersteunt bij vereenvoudigen en efficiënter uitvoeren van gebruikerstaken. PNB onderzoekt momenteel de waarde van AI voor de organisatie en de gebruikers net als de consequenties daarvan voor veiligheid en privacy. Vooral dat laatste maakt dat PNB er rekening mee houdt dat de Microsoft backend en frontend steeds meer met elkaar verweven raken, wat zowel voordelen als risico's en aandachtspunten met zich mee brengt. Van de dienstverlener wordt verwacht op zowel operationeel als tactisch en strategisch niveau PNB te adviseren over inzet en gebruik van Copilot net als over het beveiligings- en privacy-perspectief daarvan. De beheerdienst is vooral gericht op het maken en beheren van het package, het beschikbaar stellen, updaten en verwijderen van (de toegang tot) de applicatie (op het moment van publicatie van deze aanbesteding nog in de pilotfase).

2. SaaS-toepassingen.
Het aantal SaaS-applicaties neemt gestaag toe binnen PNB. Dat zal de komende jaren verder stijgen. De beheerdienst spitst zich hier met name toe op het veilig beschikbaar stellen van de applicatie.
3. Overige applicaties.
PNB beschikt over enkele honderden business- en productiviteitsapplicaties die of vanuit het on-premise datacenter of vanuit Azure aan de gebruikers worden aangeboden. De beheerdienst is vooral gericht op het beschikbaar stellen, updaten en verwijderen van (de toegang tot) de applicatie.

De volgende elementen zijn, op hoofdlijnen, dan ook onderdeel van de standaard werkplek beheerdienst:

Beheeronderdelen	Standaard applicaties (incl M365)	SaaS	Overige applicaties
Creëren, beheer package en beschikbaar stellen	X		
Beschikbaar stellen (inclusief snelkoppeling)	X	X	X
Updaten	X	X	
Verwijderen	X	X	X

Het creëren en beheren van de packages en het beschikbaar stellen van de overige applicaties is geen onderdeel van de standaard werkplek dienstverlening, maar zal op verzoek van PNB case by case worden beoordeeld en eventueel in opdracht worden gegeven. Het verwijderen van de overige applicaties is wel onderdeel van de standaard dienst.

Het creëren van packages door de dienstverlener vindt plaats op een voorspelbare, kosten efficiënte en logische manier. De aanpak van de dienstverlener moet leiden tot een indeling van categorieën (bijvoorbeeld hoog, middel en laag) die aangeeft hoeveel tijd en wat de moeilijkheid is om de packages te creëren.

Voor meer informatie over de huidige applicaties verwijzen we u naar bijlage 2 Huidige situatie.

4 Transitie

4.1 Inleiding

De transitie is voor PNB een belangrijk proces, immers continuïteit van de dienstverlening valt of staat bij een succesvolle as-is overgang van de huidige werkplekdienstverlening van én werkplekinrichting door de huidige dienstverlener naar de nieuwe dienstverlener. Waarbij een storing of onderbreking van de dienstverlening t.a.v. de werkplek of productiviteitsapplicaties als eerste wordt opgemerkt door de gebruikers. De overgang naar de nieuwe dienstverlener verloopt dan ook bij voorkeur zonder (noemenswaardige) verstoringen, in ieder geval voor wat betreft de gebruikers.

PNB verwacht een overgang met een zo kort mogelijk doorlooptijd, waarbij de dienstverlener geleidelijk meer verantwoordelijkheden overneemt tot het moment dat wordt overgegaan naar SLA-gebaseerd beheer (FMO fase). De transitie verloopt op basis van een fasegewijze, bewezen en gestructureerde aanpak volgens een algemeen erkende methode. Dienstverlener heeft ruime ervaring (meer dan 5 keer succesvol en naar tevredenheid opdrachtgever uitgevoerd) in vergelijkbare transitie van vergelijkbare trajecten. En die as-is situatie is in grote lijnen de volgende: door de bestaande dienstverlener is in 2024 een nieuwe Microsoft gebaseerde werkplek omgeving ingericht. Citrix is uitgefaseerd en einde 2024 hebben veel werknemers een nieuwe laptop ontvangen. PNB heeft twee personen die de adoptie hebben gedaan. De werkplek omgeving en dienstverlening is op dit moment stabiel. Dit is de omgeving die in beheer genomen dient te worden door de nieuwe dienstverlener.

PNB ziet deze transitie met name als een ‘brownfield’ transitie waarbij zo veel als mogelijk de huidige werkplek en apps inclusief onderliggende dienstverlening wordt gecontinueerd (en verbeterd). Er is, tenminste bij aanvang van de overeenkomst, geen sprake van een vervanging van de huidige werkplek in een standaard werkplekconcept van de dienstverlener. Niet is uit te sluiten dat PNB alsnog op later termijn gebruik maakt van het werkplek concept van dienstverlener.

Onderdeel van de transitie is de due diligence, waarin dienstverlener in maximaal 6 weken na contractering onderzoekt welke afwijkingen hij constateert tussen hetgeen door PNB in de aanbestedingsstukken en NvI's als uitgangspunten zijn opgegeven en de gerapporteerde “werkelijkheid” op het moment van onderzoek. Deze verschillen worden besproken tussen opdrachtgever en dienstverlener en, daar waar dit opportuun is, worden hierover verdere afspraken gemaakt. Eventuele verschillen geconstateerd na de due diligenceperiode van 6 weken zijn voor rekening van dienstverlener.

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 ‘moderne werkplek-landschap’. Waarna hij tijdens de transitie de lead neemt in het ‘in control’ komt over de, voor de dienstverlening 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 als de transitie wordt afgerond.

Nadat overdracht van de dienstverlening heeft plaatsgevonden zal dienstverlener de noodzakelijke aanpassingen doorvoeren om te komen tot een SLA-gebaseerde dienstverlening. Hierbij is samenwerking tussen alle betrokken partijen voorwaardelijk voor succes. PNB verwacht dat dienstverlener in staat is op de juiste manier met de latende partij (en andere kaveleigenaren) samen te werken en dat de bemoeienis van PNB in de transitie, in ieder geval v.w.b. overdracht, tot een minimum blijft beperkt.

Het transitieproces omvat meer dan een technische overdracht; het legt een stabiele basis voor toekomstige samenwerking en continuïteit van dienstverlening. De dienstverlener neemt direct vanaf dag één het initiatief. Hij is zelfredzaam, pragmatisch en denkt mee en is zich heel goed bewust van de behoefte van de PNB-gebruikers. Met als belangrijkste doel met alle betrokkenen te komen tot een snelle succesvolle en tegelijkertijd betrekkelijk impact loze transitie. De gebruiker ervaart geen onderbreking van dienstverlening en dienstverlener leert ook de PNB-organisatie en de belangrijkste stakeholders en samenwerkingspartners snel kennen.

Grote wijzigingen in werkplekverschijningsvormen en in gebruik zijnde applicaties worden voorlopig niet verwacht (maar zijn niet uitgesloten). Dienstverlener dient er, samen met de backup/restore dienstverlener, zorg te dragen voor een juist ingevuld backup en restore proces. Dat geldt tevens voor het proces rondom en het afhandelen van security meldingen waarvoor u samen met de de SOC-dienstverlener een proces inricht waarbij alle logdata wordt gedeeld, een escalatieproces wordt overeengekomen en aan de aansluitvoorwaarden van de SOC dienstverlener wordt voldaan.

De dienstverlener geeft, by design, extra aandacht aan positieve gebruikerservaringen onder ander via een duidelijke communicatie en een snelle en adequate ondersteuning tijdens de transitie. PNB hecht waarde aan een respectvolle, constructieve samenwerking, waarin alle partijen zich professioneel opstellen en gezamenlijke verantwoordelijkheid nemen voor een succesvol verloop. Het is belangrijk om vroeg in het proces duidelijke afspraken te maken met, en verwachtingen te delen tussen, alle betrokken partijen. Communicatie naar de gebruikers over de status van de overgang en de (mogelijke) tijdelijke impact voor gebruikers heeft de hoogste prioriteit. Het initiatief hiervoor ligt bij de dienstverlener, waarbij uiteraard gebruik gemaakt wordt van het transitieteam van PNB voor de uiteindelijke communicatie.

De samenwerking en het gereed zijn voor inbeheername wordt in de praktijk, met alle betrokken partijen (latende, ontvangende 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 vindt plaats na in beheer name en overeenstemming van eventuele restpunten in de in te richten stuurgroep.

4.2 Scope

Tot de scope van de transitie behoort:

1. Uitvoeren due diligence.
2. Opstellen van een door PNB geaccordeerd transitieplan, inclusief afstemming met latende partij.
3. Overnemen van de bestaande werkplek dienstverlening.
4. Het doorvoeren van noodzakelijke optimalisaties om te komen tot SLA-gebaseerde dienstverlening.
5. Inrichten en operationaliseren van de organisatie, governance en samenwerking voor de beheer- en doorontwikkelfase.
6. Inrichten van het beheer van de moderne werkplek en de daaraan gerelateerde diensten.
7. Inrichten van en aansluiten op het backup- (en restore-) proces in samenwerking met de backup en restore dienstverlener.
8. Aansluiten bij de security monitoring (SOC-dienstverlener) en kwetsbaarheden management dienstverlening en het inrichten en uitvoeren van hier benodigde operationele activiteiten.
9. Het inventariseren, implementeren en testen van de near realtime API-koppeling tussen ITSM-tooling van opdrachtnemer en opdrachtgever inclusief aansluiten op de ITIL-processen: incident mngt, change mngt, config mngt, problem mngt en request fulfilment.
10. Overnemen, actualiseren en opstellen van beheer, design- en inrichtingsdocumentatie en werkinstructies.
11. Overnemen en afronden van de lopende incidenten, problems, changes en projecten.
12. Oplevering en overdracht naar beheerorganisatie en aan PNB.
13. Opstellen en voor akkoord overleggen aan PNB van het exit- of retransitieplan inclusief kosteninschatting.

4.3 Verwachtingen Transitie

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

1. Gedegen aanpak

PNB verwacht een stapsgewijze, gedegen en bewezen 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 en op realiteit gebaseerde 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 nog op te stellen retransitieplan van de huidige dienstverlener;
- h) Belangrijkste risico's en mitigerende maatregelen inclusief een actief kwaliteits-, risico- en issue managementproces (voor zowel risico's die binnen als buiten de directe invloedssfeer van dienstverlener liggen).

2. Optimaliseren dienstverlening

PNB verwacht dat de huidige dienstverlening wordt geoptimaliseerd alvorens over te gaan naar FMO, zodat zo veel mogelijk is geautomatiseerd en standaard wijzigingen automatisch kunnen worden uitgevoerd conform SLA.

PNB verwacht dat de dienstverlener een overzicht deelt van de minimaal te automatiseren activiteiten/processen in de transitieperiode 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 en pro-actieve samenwerking

Van de dienstverlener wordt verwacht dat hij de lead neemt om een uitstekende samenwerking tussen alle betrokken partijen te bewerkstelligen. En hij neemt de lead bij het initiëren, onderhouden en uitbreiden van een intensieve samenwerking om de transitie tot succes te maken. De dienstverlener werkt constructief en rechtstreeks samen met de partij(en), zowel binnen als buiten PNB, waarmee afgestemd moet worden. Er is sprake van een duidelijke afbakening van rollen en verantwoordelijkheden van en tussen de dienstverlener, het PNB-team, de latende partij en andere betrokken dienstverleners. Dienstverlener maakt duidelijk wanneer, welke en hoeveel inzet wordt verwacht van eenieder en wat het gewenste resultaat is.

Van dienstverlener wordt verwacht dat hij proactief PNB en betrokken kaveleigenaren meenemeent in het transitieproces, dat hij structureel en regelmatig duidelijk rapporteert over minimaal de voortgang, indepiments, risico's en voorgestelde oplossingen, waarvoor zowel op commercieel gebied, als voor service management en transitie management een vaste contactpersoon wordt ingezet gedurende de hele transitieperiode.

5 Dienstverlening en doorontwikkeling

5.1 Inleiding

PNB streeft naar een wendbare, veilige en betrouwbare moderne werkplek voor de gebruikers. Productiviteitsverbeteringen, innoveren, het voldoen aan de veiligheidsnormen en heldere en duidelijke afspraken over producten, diensten en kwaliteitsniveaus ziet PNB hiervoor als essentieel.

De dienstverlening die hierbij nodig is, is snel, stabiel en betrouwbaar en altijd en overal beschikbaar. Tevens is ze logisch van opzet en eenvoudig te doorgronden voor PNB, waardoor meldingen en aanvragen voor nieuwe producten of diensten eenvoudig en snel worden opgepakt en afgehandeld. Er is sprake van een heldere set van afspraken over producten, diensten, kwaliteitsniveaus en van resources. Op het gebied van de moderne werkplek als ook op het gebied van productiviteits applicaties vinden er continu veel ontwikkelingen plaats. De ene wat relevanter voor PNB dan de ander. De dienstverlener heeft een ruime focus op het continu verbeteren van de werkplek en de gebruikerservaring en op innovatie, zodat de moderne werkplek toekomstbestendig blijft en aan blijft sluiten bij de behoeften van gebruikers en strategische doelen van PNB. Hierbij is de dienstverlener kritisch in het samen met PNB beoordelen welke innovaties echt voldoende meerwaarde bieden.

PNB maakt een duidelijk onderscheidt tussen innovatie (revolutie) en doorontwikkelen (evolutie). De eerste categorie betreft nieuwe, vaak belangrijke en grote ontwikkelingen die leiden tot impactvolle functionele wijzigingen voor de PNB gebruiker en waarbij de implementatie een projectmatige aanpak vereist, al dan niet ondersteund met een adoptietraject. Deze grote innovatieve werkzaamheden, complexere projecten of grote veranderingen voor de moderne werkplek en applicaties zijn **geen** onderdeel van de scope en standaard dienstprijs van de dienstverlener (zie hoofdstuk 2.4). Werkzaamheden worden vooraf v.w.b. scope en omvang tussen PNB en de dienstverlener afgestemd en op basis van een offerte voor de uit te voeren werkzaamheden (eventueel aangevuld met de mogelijk impact op het beheertarief) in opdracht gegeven.

De tweede categorie betreft doorontwikkelen. Doorontwikkelen gaat over evolutionaire aanpassingen. In veel gevallen kleinere functionele of technische wijzigingen, merendeels gepushed vanuit de product of de producent. Deze min of meer standaard wijzigingen in het IT-landschap en in de dienstverlening van de dienstverlener zijn onderdeel van de reguliere beheer dienstverlening, waarmee ze onderdeel zijn van het standaard beheertarief en dus van de inschrijfprijs van dienstverlener.

De dienstverlener stelt in overleg met PNB roadmaps op waarin LCM (Life Cycle Management) en doorontwikkeling van de standaard werkplek verschijningsvormen en de diensten zijn opgenomen. Dienstverlener neemt hierin het initiatief, ook in het bespreken daarvan met PNB. Het is de gezamenlijke verantwoordelijkheid van dienstverlener en PNB om de roadmaps actueel te houden.

Beheerteam dienstverlener

In het verleden is gebleken dat het voor een extern beheerteam, werkend op afstand, en voor interne PNB-oplosgroepen niet altijd eenvoudig was om elkaar goed te begrijpen. Dit kan de samenwerking tussen de eerste/tweede en derde lijn bemoeilijken en minder efficiënt maken waardoor vertragingen en ergernis kunnen ontstaan. In de overtuiging van PNB draagt een goede zichtbaarheid van de dienstverlener positief bij in het beeld dat PNB-gebruikers hebben bij de dienstverlening en dienstverlener. PNB is er van overtuigd dat indien de beheerorganisatie of het beheerteam dat dienstverlener inzet bij PNB en PNB fysiek dicht bij elkaar zitten dit een oplossing kan zijn voor beide issues. Het uitgangspunt voor de dienstverlening is dan ook dat minimaal één beheerder (en bij voorkeur twee) één dag (8 uur) per week fysiek aanwezig is bij OnsLoket op het provinciehuis in Den Bosch voor het uitvoeren van regulier beheertaken, als vraagbaak voor OnsLoket en ter bevordering van de samenwerking tussen PNB en dienstverlener.

Consultancy ondersteuning

PNB verwacht van de dienstverlener dat hij in ieder geval voor 70 uur per jaar consultancy-ondersteuning op lokatie biedt op basis van structurele inzet (1 dag per maand) voor het geven van informatie en het sparren met functioneel beheer m.b.t. vragen en vraagstukken die in de periode daarvoor zijn opgekomen. Hoewel structureel, is het PNB's voorkeur om uit te gaan van een strippenkaart, zodat er meer flexibiliteit is in geval

bijvoorbeeld een vraagstuk niet tot het volgende bezoekomoment kan wachten, of indien er op enig moment minder onderwerpen zijn dan voor een volle dag.

5.2 Scope van de dienstverlening

De scope van de werkplek dienstverlening is op het hoogste niveau als volgt verdeeld:

1. Moderne werkplek dienstverlening
2. Applicatie dienstverlening

Deze scope is van toepassing op dienstverlening zowel voor alle werkplek verschijningsvormen en productiviteitsapplicaties van de Provincie als voor die van de Provinciale Staten.

5.2.1 Moderne werkplek dienstverlening

Tot de scope van de moderne werkplek dienstverlening behoort:

1. Beheer, onderhoud en doorontwikkeling werkplek verschijningsvormen
2. Beschikbaar stellen en houden van applicaties
3. Beschikbaar stellen en onderhouden van drivers t.b.v. randapparatuur
4. Security binnen de kavel

Werkplek verschijningsvormen en beheer

Zoals in hoofdstuk 3.2 reeds aangegeven onderscheidt PNB de volgende 5 verschijningsvormen: CYOD, BYOD, AVD, smartphones en specials. Daarnaast neemt de smartphone een speciale plaats in v.w.b. beheer. Op hoofddlijnen zijn de volgende elementen onderdeel van de standaard werkplek beheerdienst:

Werkplek verschijningsvorm	CYOD	BYOD	AVD	Special	SmartPhone
Firmware & drivers	X		X	X	
Image uitrol			X		
Config management (intune, autopilot, conditional access etc.)	X	X	X	X	X
Security werkplek	X		X	X	X
MDM					X
Lifecycle management	X		X	X	X

5.2.2 Applicatie dienstverlening

Tot de scope van de applicatie dienstverlening behoort:

1. Structurele consultancy-ondersteuning functioneel beheer (strippenkaart)
2. Technisch-(applicatie) beheer
3. Beheer user- en groepsdata
4. Security binnen de kavel

5.2.3 Detailbeschrijving scope

In meer detail behoren minimaal de volgende onderdelen tot de scope:

Algemeen	○ Inrichten, beheren en onderhouden van die delen van de Azure tenant(s) van PNB die benodigd zijn om de werkplek verschijningsvormen en (M365) applicaties en functionaliteiten op de werkplek te leveren. Denk hierbij naast monitoring, alerting, reporting en provisioning ook aan ITIL-processen als: Incident, Change, Problem, Security, Patch, Continuity en Config management, Request fulfilment. • Technisch testen van wijzigingen en van oplossingen voor incidenten en problems. • Deelnemen en actief bijdragen aan relevante overleggen op operationeel en tactisch niveau. • Deelnemen aan CAB.op bl • In geval van een crisissituatie deelnemen aan het provinciaal crisisteam. • Organiseren, inrichten en beschikbaar stellen van benodigde middelen voor technische testen • Operationele regie binnen het kavel en zorgen voor de aansluiting op aangrenzende kavels en diensten binnen het ICT-landschap
-----------------	---

	• Opstellen van roadmaps voor de moderne werkplek en productiviteitsapplicaties op basis van relevante ontwikkelingen vanuit de markt. • Implementeren van Microsoft ontwikkelingen die op basis van push vanuit Microsoft geleverd worden. • Het realiseren, updaten en aan PNB beschikbaar stellen van werkinstructies, packaging documentatie, HLD's, LLD's en andere voor PNB relevante documentatie. • Ondersteunen bij cost,- en licentiemanagement. • Het borgen van de informatiebeveiliging m.b.t. de binnen de kavel behorende diensten en producten conform de voorwaarden van PNB. • Het creëren, onderhouden en updaten van back-up koppelingen in samenwerking met de back-up dienstverlener. • Het waarborgen van een veilige dienstverlening en een veilige moderne werkplek binnen dit kavel. • Uitvoeren operationele regie over de dienst en zorgen voor de aansluiting op en afstemming met de aangrenzende kavels binnen het ICT-landschap.
Moderne werkplek	• Beheer, onderhoud en doorontwikkeling moderne werkplek van alle werkplek verschijningsvormen: ○ Het dagelijks beheer, onderhoud en de beveiliging (reactief, proactief en perfectief) van alle verschijningsvormen en met alle onderliggende technologie. Zie ook 1^e bullit Algemeen voor verbijzondering. ○ Het beheren, onderhouden, aanpassen of verwijderen van alle bijbehorende policies gerelateerd aan alle verschijningsvormen. ○ Het bewaken, bijsturen, informeren en adviseren m.b.t. de gebruikerservaring. ○ Het monitoren van alle werkplek verschijningsvormen. ○ Aansluiten op centrale PNB faciliteiten t.b.v. van monitoring ○ Ondersteunen van ontsluiting van applicatie specifieke hardware (bv. dongles). ○ Registeren en up-to-date houden van moderne werkplek gerelateerde CI's in de PNB CMDB. ○ Beschikbaar stellen en onderhouden drivers, t.b.v. randapparatuur. • Printing ○ Zorgdragen voor correcte werking printers vanuit gebruikersperspectief. ○ Toetsen of de softwareversies op de werkplek verschijningsvormen up-to-date zijn in geval van SaaS-applicaties. ○ Beheren, onderhouden, updaten en upgraden van printersoftware inclusief printerdrivers op en t.b.v. alle werkplek verschijningsvormen. ○ Het creëren, beheren, updaten en verwijderen van printqueues t.b.v. printfunctionaliteit op het SafeQ platform of, wanneer die wordt vervangen, op de nieuwe Cloud printing oplossing. ○ Het maken, beheren en updaten van werkinstructies t.a.v. de beheerdienst betreffende printing. • Security binnen de kavel: ○ Het aantoonbaar beveiligen en veilig houden van de moderne werkplek. ○ Het aansluiten op de aansluitvoorwaarden van de PNB SOC dienstverlener. ○ Het creëren, beheren, onderhouden en updaten van koppelingen met de SOC partner en andere kavel eigenaren. ○ Het proactief opvolgen en oplossen van security incidenten binnen dit kavel. • Integratie user- en groepsdata • VIP support dienst voor specifieke gebruikersgroep.
Applicaties	• Beschikbaar stellen van M365 applicaties, overige applicaties en SaaS applicaties op alle werkplek verschijningsvormen. ○ Het creëren, installeren, beschikbaar stellen, beheren, updaten en verwijderen van de standaard applicaties. ○ Het beschikbaar stellen (inclusief snelkoppeling) van zowel de standaard als de overige en de SaaS applicaties. ○ Het, indien nodig en gewenst, verwijderen van de (toegang tot) de standaard, overige en SaaS applicaties ○ Het updaten van de standaard applicaties en snelkoppeling van de SaaS applicaties. ○ Het controleren en valideren van aangeboden intakes en rapporteren over afwijkingen van voorwaarden. ○ Valideren en technisch accorderen in OTAP-straat van wijziging op de moderne werkplek. ○ Het valideren of de juist lidmaatschap gekoppeld is aan de betreffende applicatie. ○ Het opstellen, onderhouden en beschikbaar stellen van werkplekgerichte documentatie.

	○ Het toepassen van LCM op standaard applicaties inclusief M365. ○ Het ondersteunen, troubleshooten en verhelpen van problemen van de door dienstverlener gemaakte packages. Supporten van package. ○ Het doorontwikkelen van de M365 omgeving. ○ Het adviseren en beveiligen van M365 omgeving. ○ Ondersteuning t.b.v. functioneel beheer PNB door structurele inzet van consultant op locatie PNB voor beantwoorden inhoudelijke vragen, sparring en kennisoverdracht t.a.v. werkplekgerelateerde vraagstukken. Inzet één dag per maand (75 uur op jaarbasis). ○ Technisch beheren, onderhouden, inrichten en beschikbaar stellen van M365 Office en browser invoegtoepassingen/plugins. ○ Signaleren van relevante nieuwe en/of aangepaste M365 toepassingen en de onderliggende technologie • Technisch beheer Power Platform (Power BI, Power Apps, Power Automate, Power Pages, & Copilot) op basis van de door PNB vastgestelde governance en richtlijnen. • Configureren en beheren van technische koppelingen met andere systemen of applicaties. • User en groepsdata
--	--

Opmerking bij tabel: voor een compleet overzicht van applicaties binnen de standaard applicatieset verwijzen we u naar Bijlage 2. Huidige situatie.

5.3 Verwachtingen t.a.v. de dienstverlener en de dienstverlening

PNB verwacht van de dienstverlener/dienstverlening het volgende:

1. Adequaat beheer, ondersteuning en bewaking kwaliteit conform overeengekomen service levels

De dienstverlener biedt PNB haar standaard SLA met concrete en adequate servicelevels aan en werkt en levert conform. Uiteraard voldoet het SLA aan de beschreven servicelevels zoals opgenomen in de eisen omtrent de dienstverlening. Naast dat de dienstverlener de continuïteit van de moderne werkplek dienstverlening en de werkplek verschijningsvormen bewaakt, verwacht PNB ook dat hij aantoonbaar continu met PNB meedenkt en proactief handelt. Dat zit zelfs in het DNA van de dienstverlener! Hierbij valt te denken aan:

- a) 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) Wijzigingen en verzoeken worden door dienstverlener vóór uitvoering kritisch bekeken en beoordeeld en daar waar het beter, handiger of sneller kan, wordt dat met PNB besproken. De dienstverlener doet vervolgens op een pragmatische manier een voorstel, zonder dat het tot noemenswaardige vertraging leidt. Ook worden alle wijzigingen en verzoeken gecontroleerd op juistheid en volledigheid. Waar nodig wordt proactief informatie opgehaald door de dienstverlener.
- c) Naast de ontwikkeling van de toepassingen op de dienst is ook de ontwikkeling van de installed base c.q. de moderne werkplek omgeving zelf van essentieel belang. PNB wil dat altijd op actuele versies gewerkt wordt. PNB verwacht van de dienstverlener dat hij dit borgt en dat hij vroegtijdig impact en doorlooptijd van updates en upgrades in kaart brengt en de implementatie daarvan is onderdeel van de dienst. En dat, onderbouwd, wordt aangegeven wanneer hiervan moet worden afgeweken.
- d) Dienstverlener geeft PNB inzicht in hoe hij gestructureerd en meerdere keren per jaar PNB informeert en uitdaagt na te denken over potentiële mogelijkheden voor het implementeren van innovatieve functionaliteit m.b.t. M365 en andere Microsoft producten, moderne werkplek verschijningsvormen en andere relevante producten en services. Hierbij doet de dienstverlener concrete, realistische voorstellen die bijdragen aan het bereiken van de doelen en de ambitie van PNB en waarvan het resultaat leidt tot een duidelijke meerwaarde voor PNB.
- e) PNB verwacht dat de dienstverlener bij wijzigingen of bij het oplossen van incidenten en problemen altijd eerst zelf de benodigde technische testen succesvol heeft afgerond en de wijziging of oplossing vervolgens ter acceptatie aanbiedt aan een beperkte PNB gebruikersgroep.
- f) Doordat de dienstverlener zich verdiept in de bedrijfsprocessen van PNB kan de dienstverlener de impact van de verstoringen in de werkplekomgeving heel goed inschatten.

2. Actieve en open communicatie

De dienstverlener heeft een nieuwsgierige en betrokken grondhouding en communiceert proactief en transparant over de dienstverlening, de voortgang, uitdagingen en verbeterpunten zowel in geval van positief als van negatief nieuws. PNB verwacht daarbij dat communicatie situationeel en afhankelijk van

de doelgroep wordt ingezet. Dienstverlener rapporteert in de afgesproken frequentie daar waar alles volgens overeengekomen proces verloopt en zij rapporteert en communiceert ook buiten het gangbare proces, met aangepaste frequentie en inhoud als de situatie daarom vraagt. Hierbij neemt dienstverlener uiteraard het initiatief.

Zowel PNB als dienstverlener spreken elkaar open en eerlijk aan over daar waar de verwachtingen uit elkaar lopen en hoe die weer met elkaar te verenigen. Dit draagt sterk bij aan het wederzijds vertrouwen en het stelt PNB in staat om snel in te spelen op knelpunten en kansen.

Communicatie speelt zich af tussen mensen, derhalve verwacht PNB dat dienstverlener oog heeft voor en invulling geeft aan dit persoonlijke aspect, bijvoorbeeld met de inzet van een vast klantteam.

3. Doorontwikkeling van de moderne werkplek dienstverlening

Optimalisatie van en doorontwikkeling op de werkplek verschijningsvormen en applicaties zijn essentieel voor PNB. Van de dienstverlener wordt verwacht dat hij structureel inspeelt op deze behoefte en doorontwikkeling beschouwt als een doorlopend proces dat aansluit bij de visie, doelstellingen en strategie van PNB.

Naast het verdiepen in persona's, bedrijfsprocessen en werkprocessen, verdiept de dienstverlener zich ook blijvend in nieuwe relevante functionele en technische ontwikkelingen en toepassingen in de markt. Dit doet hij onder andere door een actieve afstemming met Microsoft en belangrijke (internationale) communities en dienstverleners. Op basis hiervan legt hij PNB actuele en stevig onderbouwde opties voor en, rekening houdend met de PNB designkaders, hij neemt de opdrachtgever en de PNB beheerorganisatie hierin mee en daarbij adviezen gevend over bruikbaarheid, implementatie en impact van deze ontwikkelingen of toepassingen op de werkplek dienstverlening.

Dit resulteert in roadmaps die bijdragen aan een toekomstbestendige, veilige en optimaal functionerende werkomgeving bij PNB. De dienstverlener heeft een actieve initierende rol bij het opstellen van de roadmaps die in overleg met PNB periodiek worden geüpdatet.

Naast doorontwikkeling en lifecycle management (zie verwachting 4) wil PNB inzicht in de wijze waarop dienstverlener bij voorgestelde innovaties (grote impactvolle wijzigingen die op projectbasis worden voorgesteld en uitgevoerd) besluitvorming en uitvoering door de dienstverlener worden vormgegeven. Afhankelijk van het onderwerp vindt afstemming plaats op tactisch of strategisch niveau.

4. Lifecycle management

PNB verwacht dat de dienstverlener een gestandaardiseerd lifecycle management plan opstelt en onderhoudt voor alle werkplek verschijningsvormen en applicaties. Hiermee zorgt dienstverlener dat hard- en software tijdig worden gepatcht, geüpdatet of vervangen, zodat beschikbaarheid, integriteit, continuïteit en performance nooit in gevaar komen. Dit vraagt een focus op 'continuous deployment' dat aansluit bij de update-cycli van leveranciers zoals Microsoft.

De dienstverlener is verantwoordelijk voor het ophalen van ontbrekende informatie bij PNB. Het plan wordt continu onderhouden, aangepast en uitgevoerd op basis van nieuwe inzichten, veranderende omstandigheden en gemaakte afspraken, steeds in afstemming met PNB. Het lifecycle management van de standaard applicatieset valt binnen de dienstverlening.

6 Regie en samenwerking

6.1 Inleiding

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 kavel, samenwerking en het WAAROM en WAT van de dienstverlening. Dat 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 (zie Bijlage Architectuur bij PNB). 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 kavel, 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. 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 en voor de gebruikers steeds beter gewaardeerde 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 strategische 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.

6.2 Scope

Tot de scope van de regie en samenwerking behoort:

1. Samenwerken (op locatie) 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.

6.3 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 daarvan op aangrenzende diensten. Hierbij heeft de dienstverlener een duidelijk beeld van en ervaring met hoe de grensvlakken optimaal wordt ingevuld in samenwerking met verschillende externe partijen. De dienstverlener zorgt ervoor dat de relevante rolverdeling, verantwoordelijkheden, governance, overlegstructuren en verwachtingen over en weer helder zijn voor alle betrokken partijen en dat de communicatie- en escalatielijnen duidelijk zijn. Het initiatief voor afstemming ligt bij de Moderne werkplek dienstverlener. Daarnaast voldoet de dienstverlener aan de aansluitvoorwaarden van de SOC-dienstverlener en informeert de dienstverlener de SOC-dienstverlener tijdig en volledig over de status van security incidenten en deelt hij alle door PNB en SOC-dienstverlener voor regievoering alle noodzakelijke security gerelateerde data realtime.

3. Koppeling ITSM-tool en service management processen

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 kavelen heen mogelijk maken en de PNB ITSM tool 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 koppeling is niet alleen een technische koppeling (API), maar behelst ook de gekoppelde integratie van de ITIL-processen. Het resultaat is dus een geïntegreerde service (integratie) management proces omgeving waarin de ITSM-omgeving van de dienstverlener en die van PNB (en van eventuele andere kaveleigenaren) zodanig met elkaar zijn verbonden dat informatie en activiteiten van de genoemde ITIL-processen zonder vertraging tussen partijen worden uitgewisseld. Van dienstverlener wordt verwacht dat de technische en proceskoppeling opgeleverd aan PNB nadat er sprake is van een aantoonbare succesvolle koppeling.

De dienstverlener verzorgt de API-koppeling vanuit zijn organisatie en onderhoudt deze koppeling tijdens de contractlooptijd. PNB verzorgt de API-koppeling en de processen aan zijn kant.

7 Informatiebeveiliging en privacy

7.1 Inleiding

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 NIS2, Cyberbeveiligingswet (Cbw), ISO27001- en BIO 2.0-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 dienstverleners 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 of combinanten 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 (state of compliance vanuit de BIO) 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 PNB SOC-dienstverlener

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 regie voerende rol ten aanzien van security incidenten- en kwetsbaarhedenmanagement over de IT kavel. De rol van de security dienstverlener gaat dus verder dan alleen het melden van incidenten en kwetsbaarheden. Hij fungeert als aanjager over security incidenten en stelt eisen ten aanzien van security en compliance vanuit 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 verplicht ze een verwerkersovereenkomst hebben getekend.

7.2 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 IT-infrastructuur 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 de M365 omgeving.
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.

7.3 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 securitycomponenten binnen de moderne werkplek kavel Van de dienstverlener wordt verwacht dat hij volledig transparant is ten aanzien van de beveiligingsstatus en -updates van de werkplek omgeving. 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. 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 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.

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 de te treffen maatregelen. Van de samenwerkende partijen, en dus ook van de werkplekdienstverlener, 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 in een te vormen Computer Security Incident Response Team (CSIRT).

4. Wet- en regelgeving

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, Cbw 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 en moderne werkplek-omgeving. Dienstverlener verbetert dus de moderne werkplek omgeving 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.

8 Eisen

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

#	Eis algemeen
1.	Dienstverlener verklaart dat hij voldoet aan alle in de leidraad en daarbij behorende bijlage(n) genoemde voorwaarden en eisen die aan de opdracht zijn gesteld.
2.	Dienstverlener conformeert zich aan geldende en 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, 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 om niet.
4.	Partijen zullen uitkomst van de benchmark bespreken en hieraan eventueel passende consequenties verbinden.
#	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 correct (goed verstaanbaar) 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 gedocumenteerd te zijn en voor PNB te allen tijde beschikbaar te zijn (voorbeelden, maar niet limitatief: handleidingen, beschrijvingen, designs).
2.	Technische of andere 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.

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.	De transitie geeft minimaal invulling aan de scope zoals beschreven in het betreffende hoofdstuk.
3.	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.
4.	De implementatie van de transitie wordt uitgevoerd tegen de door dienstverlener afgegeven vaste prijs.
5.	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.
6.	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 en**Doorontwikkeling:**

#	Kwaliteitseis
1.	De aangeboden dienstverlening en doorontwikkeling voldoet minimaal aan de in dit document en aan de in de bijlage Huidige situatie 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 of andere 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. Dit houdt ook in eventueel geschreven code en/of tooling om processen te automatiseren eigendom is van PNB en tijdens na afloop van het contract, indien gewenst, gebruikt kan blijven worden.
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 geïmplementeerd.
5.	Dienstverlener plant periodiek overleg in met PNB en derde partijen/oplossgroepen, zoals maandelijkse operationele overleggen en kwartaal overleggen op strategisch niveauactief. In deze overleggen worden de voortgang, prestaties en eventuele knelpunten besproken, evenals plannen voor doorontwikkeling van de dienstverlening. Deze overleggen dragen bij aan een transparante en constructieve onderlinge relaties.
6.	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 en getest door de dienstverlener.
7.	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 en recovery dienstverlening voor de provincie.
8.	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.
9.	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.

10.	Alle informatiesystemen ten dienste van de dienstverlener beschikken over voorzieningen voor adequate en actuele bescherming tegen ongewenste invloeden.
11.	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.
12.	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 werkt volgens ITIL en levert vanuit dat oogpunt periodiek rapportages aan waarvan de details verder zullen worden uitgewerkt in een SLA en een DAP. Een template van PNB van beide documenten wordt meegeleverd. Maandelijks zal de dienstverlening worden besproken a.d.h.v. een door de dienstverlener opgestelde Service Level Rapportage.
15.	Incident Management: voor P1 incidenten eist PNB een 24/7 servicewindow met hierbij de volgende tijden: reactietijd van <15 minuten en oplostijd van <4uur.
16.	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).
17.	De werkplekomgeving voor de Provinciale Staten (PS) en de omgeving voor het ambtelijke apparaat zijn, vanuit beheerperspectief, volledig van elkaar gescheiden (functiescheiding).
18.	Dienstverlener accepteert de aansluitvoorwaarden van de PNB SOC-dienstverlener en hij volgt de security events, gemeld door de SOC-dienstverlener, op conform die aansluitvoorwaarden.
19.	Om een groei van de gebruikerstevredenheid te meten bepaalt de dienstverlener, in overleg met en ter accordering van PNB het startpunt en het streefcijfer. Vanaf het startpunt wordt minimaal 4 keer per jaar gemeten en gerapporteerd wat de afwijking is van de gebruikerstevredenheid t.a.v. het startpunt en t.a.v. het streefgetal.
20.	Dienstverlener conformeert zich aan de PNB naamgevingsconventie voor alle binnen de scope (technische) aan te maken objecten.

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 gezamenlijkheid op te pakken.
6.	Dienstverlener biedt ten behoeve van IT-meldingen en -vragen een deskundige servicedesk aan, dat wil zeggen 'een tweedelijns ondersteuning', die als aanspreekpunt rechtstreeks in contact staat met <i>OnsLoket</i> of functioneel beheer 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.
9.	De leverancier moet bereid zijn om nauw samen te werken met andere externe partners van PNB.
10.	Dienstverlener neemt deel aan de relevante of noodzakelijke strategische, tactische en operationele overleggen.

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 uitvoeisels 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 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.
5.	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 kavel van de moderne werkplek.
6.	Dienstverlener heeft de kennis- en expertise op het gebied van afhandeling van security incidenten (onderzoek, oplossing en rapportage).
7.	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.
8.	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.
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 neemt in geval van een security incident of calamiteit deel aan een eventueel crisisteam.
11.	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.
12.	PNB bepaalt wie de eigenaar is of wordt van de securityoplossingen/-systemen.
13.	Alle informatiesystemen ten dienste van de dienstverlener beschikken over voorzieningen voor adequate en actuele bescherming tegen ongewenste invloeden.
14.	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.
15.	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.

BIJLAGE: Architectuur bij PNB

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 visiedocument 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 Cloud 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.

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

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.



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 dienstverleners 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.