

Kaderbrief 2027 - iRvN

Inleiding

Zoals gebruikelijk schetst iRvN in deze kaderbrief de belangrijkste ontwikkelingen en keuzes die de komende jaren richtinggevend zijn voor de samenwerking.

De kaderbrief vormt daarmee de basis voor bestuurlijke en financiële afwegingen. De onderwerpen die hierin worden benoemd, zullen samen met de deelnemers verder worden uitgewerkt en vertaald naar de ontwerpbegroting die in het voorjaar van 2026 wordt voorgelegd.

De digitale ontwikkeling van deelnemers en van iRvN kent een duidelijke richting: veilig, volwassen en efficiënt werken binnen een betrouwbare infrastructuur. Dat vraagt blijvende aandacht voor informatieveiligheid, modernisering van de werkplek, cloudtechnologie en samenwerking. Deze beweging is noodzakelijk om onze publieke taak goed te kunnen uitvoeren, maar zij is niet budgettair neutraal. De keuze om als regio te investeren in volwassenheid en veiligheid is daarmee geen kostenverhoging omwille van techniek, maar een investering in continuïteit, kwaliteit en bestuurlijke betrouwbaarheid.

Ontwikkelingen en kansen

De digitale omgeving verandert snel en dat biedt kansen om de gemeentelijke dienstverlening slimmer, veiliger en toekomstbestendig te maken. Het applicatielandschap van deelnemers verandert ingrijpend, wordt flexibeler en innovatiever. Dat vraagt van iRvN ondersteuning op meerdere fronten, zowel on premises als in de cloud, en leidt tot meer aandacht voor regie, beveiliging, leveranciers- en contractmanagement.

Informatieveiligheid ontwikkelt zich verder: iRvN verwacht in 2026 aantoonbaar herhaalbaar en voorspelbaar te werken op het gebied van informatieveiligheid, zoals bedoeld in de Baseline Informatiebeveiliging Overheid (BIO). (De Baseline Informatiebeveiliging Overheid – BIO – is de landelijke norm die overheidsorganisaties verplicht om informatie en systemen zó te beveiligen dat beschikbaarheid, integriteit en vertrouwelijkheid structureel zijn gewaarborgd.) Dit betreft het zorgvuldig omgaan met informatie, het beheersen van risico's en het borgen van processen die de continuïteit van de dienstverlening ondersteunen.

Voor iRvN is het Third Party Mededeling (TPM)-traject een belangrijk instrument om aan te tonen dat de eigen processen en maatregelen voldoen aan de overeengekomen BIO-afspraken tussen iRvN en deelnemers. Voor de deelnemers betekent het dat voor vragen vanuit eigen auditors over processen die door iRvN uitgevoerd worden (zoals back up en rechtentoekenning binnen in-, door- en uitstroom) verwezen kan worden naar iRvN. De ontwikkelingen rond informatieveiligheid maken duidelijk dat dit een doorlopend proces is, waarin nieuwe technologie, veranderende dreigingen en aangescherpte wetgeving voortdurend aanpassing

vragen. We zullen hierin waarschijnlijk nooit ‘klaar’ zijn, maar wél blijvend aantoonbaar werken aan verbetering, borging en volwassenheid.

De toepassing van kunstmatige intelligentie biedt nieuwe mogelijkheden om processen slimmer in te richten, de dienstverlening te verbeteren en medewerkers te ondersteunen. iRvN ontwikkelt, zo veel als mogelijk samen met deelnemers, hiervoor instrumenten, kennis en kennisontwikkeling bij de deelnemers, en ook de mogelijkheid om AI in de eigen omgeving en infrastructuur te gebruiken, zodat deelnemers AI verantwoord en veilig kunnen toepassen.

Daarnaast voert iRvN concrete projecten uit die bepalend zijn voor de kwaliteit van de dienstverlening. Voorbeelden hiervan zijn de aanbesteding en implementatie van het netwerk (2025–2027), de heroriëntatie op TopDesk, verdere uitbouw van in-, door- en uitstroomprocessen en autorisatietoekenning en -monitoring, het sturen op KPI’s voor techniek en dienstverlening, en de verdere uitrol en implementatie van M365 en nieuwe Office-versies.

Voor de doorontwikkeling van M365 is in de afgelopen jaren, naast structurele inzet, ook incidentele capaciteit beschikbaar gesteld. Deze tijdelijke aanvulling maakte het mogelijk om te blijven ontwikkelen en in te spelen op de verschillende ambities, tempo’s en behoeften van de deelnemers. In het eerste kwartaal van 2026 brengen iRvN en de deelnemers gezamenlijk in beeld welke structurele inzet vanaf 2027 nodig is om het platform stabiel en toekomstbestendig te beheren en door te ontwikkelen.

De combinatie van structurele en incidentele inzet heeft de afgelopen jaren de noodzakelijke flexibiliteit geboden om te leren, te ontwikkelen en voortgang te boeken binnen een dynamisch speelveld. Ook in de komende periode blijft het belangrijk om ruimte te houden voor die wendbaarheid: deelnemers verschillen in ambitie en tempo, en geopolitieke en technologische ontwikkelingen maken dat prioriteiten kunnen verschuiven.

Big Tech en geopolitieke ontwikkelingen

De digitale werkelijkheid wordt steeds sterker beïnvloed door geopolitieke ontwikkelingen en de afhankelijkheid van grote, vaak mondiale leveranciers. Deze ontwikkeling raakt ook de deelnemers in het Rijk van Nijmegen: terwijl het gebruik van cloudtoepassingen toeneemt, worden vraagstukken rond data-opslag, privacy, continuïteit en digitale soevereiniteit steeds meer bestuurlijke thema’s.

iRvN acht het daarom noodzakelijk om kritisch te blijven op het gebruik van deze leveranciers en op het risico van lock-ins. Tegelijkertijd is het onvermijdelijk dat bestaande afspraken en diensten niet van de ene op de andere dag kunnen worden beëindigd. De uitdaging is om binnen deze realiteit bewuste bestuurlijke keuzes te maken over waar data zich bevindt, onder welke voorwaarden deze wordt beheerd en hoe afhankelijkheden worden geminimaliseerd.

iRvN onderzoekt in 2026 actief alternatieven waar dit mogelijk is, en implementeert die – samen met deelnemers – waar dit zinvol en uitvoerbaar is. Daarmee dragen we gezamenlijk bij aan een

evenwichtige, toekomstbestendige en bestuurlijk verantwoorde digitale infrastructuur voor de regio.

Eigen infrastructuur

Naast de beweging naar cloud en SaaS blijft de eigen infrastructuur van iRvN van groot belang. Deze infrastructuur moet robuust en veilig zijn, maar tegelijk flexibel genoeg om in te kunnen spelen op vraagstukken en opgaven die nu nog niet bekend zijn. Daarmee legt iRvN een duidelijke verbinding met de cloudstrategie en de hybride werkplekconcepten die in ontwikkeling zijn.

Ook bij verdere 'versaasing' en cloudmigratie blijft er noodzaak voor de aanwezigheid, inrichting, monitoring en beheer van veilige mobiele devices (laptops en smartphones), bekabelde en veilige infrastructuur en access points. Hiervoor organiseert iRvN 24/7 bewaking, monitoring en respons (voortdurende opvolging).

De huidige Citrix-omgeving blijft voorlopig bestaan, maar iRvN verwacht dat het gebruik daarvan de komende jaren geleidelijk zal afnemen. Deze ontwikkeling sluit aan bij de regionale cloudstrategie, waarin deelnemers stap voor stap hun on-premises applicaties uitfaseren en overstappen op SaaS- en clouddiensten. In dat licht is het van belang dat de volgende aanbesteding voor de on-premises back-up en storage — die formeel in 2026 moet starten en in 2027 moet zijn afgerond — qua omvang minimaal kan blijven.

Met betrekking tot de Citrix-omgeving inventariseert iRvN het Citrix-gebruik en stimuleert alternatieven. Het is een keuze van de deelnemers of en hoe deze alternatieven worden ingezet.

De verdere uitvoering van de regionale cloudstrategie vraagt om incidentele middelen voor uitwerking en implementatie. Op dit moment is sprake van een globale inschatting, waarbij afgesproken is dat iRvN in een vervolgoopdracht gevraagd zal worden de visie en strategie te vertalen naar een concrete technische doelarchitectuur. Daarbij wordt ook rekening gehouden met een strategisch personeelsontwikkelingstraject, waarvoor naar verwachting eenmalig circa €250.000 aan ontwikkelkosten en €400.000 aan frictiekosten nodig zal zijn. De precieze detaillering hiervan zal onderdeel uitmaken van die vervolgoopdracht.

De cloudstrategie is geen technologische keuze op zichzelf, maar een noodzakelijke stap om de continuïteit te waarborgen en toekomstbestendig te blijven. De incidentele middelen die hiervoor nodig zijn, zijn een investering in kwaliteit en wendbaarheid, niet louter een kostenpost.

In aansluiting op de cloudstrategie en de verdere migratie van gemeentelijke data naar Microsoft 365, zal iRvN vanaf 2026 de back-upvoorziening voor M365 implementeren. Deze voorziening is essentieel voor de continuïteit en herstelbaarheid van gegevens en sluit aan bij de eisen uit de BIO en NIS2.

Voor de uitvoering hiervan worden vanaf 2026 kosten gemaakt van €500.000 per drie jaar. Deze structurele voorziening wordt vanaf 2027 opgenomen in de meerjarenbegroting.

Regionale i-samenwerking

In de regio loopt een traject om te verkennen hoe de samenwerking op het gebied van informatisering verder kan worden versterkt. De Kring van gemeentesecretarissen heeft hiervoor in 2025 het initiatief genomen. Het proces richt zich op het in beeld brengen van de huidige situatie, het formuleren van scenario's en het voorbereiden van bestuurlijke keuzes.

De eerste analyses laten zien dat de i-functie bij veel deelnemers qua omvang en positionering nog niet overal aansluit op de toenemende digitale opgaven. De uitkomsten van het traject worden eind 2025, begin 2026 verwacht en kunnen van invloed zijn op de verdere invulling van de opdracht en rol van iRvN vanaf 2027.

Dienstverlening van iRvN

iRvN is een ICT-dienstverlener en een samenwerkingsverband van en voor de deelnemers. De dienstverlening van iRvN is erop gericht deelnemers in staat te stellen hun publieke taak goed en betrouwbaar uit te voeren. Dat vraagt om een professionele organisatie die voortdurend meebeweegt met de veranderende eisen van de digitale samenleving.

Door samenwerking bundelt iRvN kennis en kracht, waardoor schaalvoordelen worden gerealiseerd, de kwaliteit stijgt en risico's afnemen. Zo maakt iRvN namens de deelnemers waar wat afzonderlijk niet haalbaar zou zijn.

Daarnaast meet iRvN systematisch hoe de dienstverlening wordt ervaren. Uit de laatste metingen blijkt een overwegend positief beeld (IT Happiness 7,3), maar ook verbeterpunten, zoals de werkplekomgeving. Deze signalen neemt iRvN nadrukkelijk mee in de verdere ontwikkeling van de diensten en de actualisatie van de diensten- en productencatalogus.

Beveiliging van hardware

De beveiliging van hardware staat onverminderd hoog op de agenda. Geopolitieke spanningen, de toename van cyberaanvallen en de inzet van kunstmatige intelligentie vergroten de druk op systemen. Voor iRvN betekent dit dat hardware en netwerken continu, dag en nacht, worden gemonitord en getest. Het is noodzakelijk dat het MDM/MAM-beleid op korte termijn wordt vastgesteld, zodat iRvN en de deelnemers mobiele apparaten op een uniforme, veilige en beheersbare wijze kunnen inzetten en beheren.

De implementatie van het MDM/MAM-beleid vergt een substantiële investering in licenties, projecturen en beheer. Op basis van een eerste analyse wordt uitgegaan van een projectinvestering van circa €270.000 en een structurele jaarlijkse stijging van de kosten met ongeveer €1,1 miljoen. Het betreft een eerste inschatting die is gebaseerd op een algemene analyse van benodigde licenties, beheerinzet en het aantal te beheren devices. De nadere

detaillering van deze financiële gevolgen zal plaatsvinden op basis van een opdracht aan iRvN en betrokkenen uit de regio om de implementatie verder uit te werken en voor te stellen hoe het beleid praktisch kan worden ingevoerd.

Deze investeringen zijn onlosmakelijk verbonden met de keuze om de digitale omgeving van de deelnemers veilig, beheersbaar en toekomstbestendig te houden. Veiligheid en volwassenheid vragen structurele inzet, maar leveren ook continuïteit, efficiëntie en vertrouwen op.

Informatieveiligheid

Als samenwerkingsorganisatie draagt iRvN, namens de deelnemers, een bijzondere verantwoordelijkheid voor het veilig beheren van infrastructuur, haar eigen bedrijfscontinuïteitsplan en het zorgvuldig omgaan met gegevens van inwoners en bedrijven. Regionale samenwerking is hierbij onmisbaar. De gezamenlijke inzet van CISO's, het Regionaal Tactisch Overleg en iRvN versterkt de positie van de deelnemers en verhoogt het niveau van beveiliging.

Tegelijkertijd blijft iRvN voldoen aan wettelijke verplichtingen, zowel nationaal (BIO2) als Europees (NIS2). Omdat wet- en regelgeving zich ontwikkelt in de pas met nieuwe dreigingen, geldt dit ook voor de organisatie. Het is daarom van groot belang dat iRvN aantoonbaar een volwassen niveau bereikt en behoudt in informatieveiligheid en procesborging. Daarnaast vraagt beveiliging nadrukkelijk ook om bewustzijn (awareness) bij alle medewerkers en gebruikers; het veilig omgaan met informatie en systemen is een gezamenlijke verantwoordelijkheid.

De verdere versterking van informatieveiligheid vraagt ook om aanvullende middelen. De eisen uit nationale en Europese regelgeving (BIO2, NIS2) en de toename van digitale dreigingen maken structurele investeringen onvermijdelijk. Over de financiële vertaling hiervan wordt in het Regionaal Strategisch I-Overleg nadere afstemming gezocht.

Duurzaamheid

In eerdere stukken, zoals de Tussenrapportage 2025 en de Begroting 2026–2029, heeft iRvN duurzaamheid expliciet benoemd als thema. iRvN zet deze lijn door en werkt aan duurzaamheid in zowel de manier van werken als in het verwerken van apparatuur en middelen. Daarnaast besteedt iRvN aandacht aan de groene mobiliteit van medewerkers en, waar het kan, heeft zij aandacht voor het energieverbruik en de duurzaamheidsimpact bij aanbestedingen van clouddiensten, SaaS-oplossingen en AI-toepassingen. Duurzaamheid blijft daarmee een integraal onderdeel van de strategie van iRvN en van de samenwerking met de deelnemers.

Externe context

De landelijke bewegingen rond Nederlandse Digitaliseringsstrategie (NDS), NL DIGIbeter Agenda Digitale Overheid, Common Ground, Samen Organiseren en Collectivering Digitalisering zijn richtinggevend voor de keuzes die deelnemers gezamenlijk maken. Ook vraagstukken rond datasoevereiniteit en de beweging naar een ICT3.0-wereld, waarin de toegevoegde waarde van informatisering centraal staat, spelen nadrukkelijk mee. iRvN ziet het als een gezamenlijke

opgave om de landelijke ontwikkelingen op het gebied van digitalisering te vertalen naar de regionale praktijk. Daarbij vervult iRvN een ondersteunende en verbindende rol, in nauwe samenwerking met de gemeenten die hierin beleidsmatig het voortouw hebben.

Uitdagingen en aandachtspunten

De genoemde ontwikkelingen komen allemaal tegelijk, terwijl het bestaande werk onverminderd doorgaat. Dat vraagt van iRvN voortdurende aandacht voor de noodzakelijke balans tussen voortgang en continuïteit. We bevinden ons in een overgangsfase van oude, lokaal ingerichte voorzieningen naar moderne, regionale oplossingen. Oud en nieuw zullen tijdelijk naast elkaar bestaan, omdat de overstap gefaseerd moet verlopen. Op termijn is dat niet houdbaar. De komende jaren staan daarom in het teken van vernieuwing, afbouw en keuzes die leiden tot een toekomstbestendige inrichting — met bijbehorende financiële consequenties, doordat tijdelijk in beide omgevingen middelen en capaciteit nodig zijn.

Traditioneel technisch beheer neemt af, maar de behoefte aan advisering, regievoering, audits en procesgericht werken groeit. Daarmee verandert de aard van het werk en neemt ook de complexiteit toe. Deze toegenomen complexiteit wordt zichtbaar in de combinatie van cloud en on-premises, in de strenger wordende eisen voor digitale veiligheid en in de voortdurende afhankelijkheid van leveranciers.

Daar komt bij dat de arbeidsmarkt krap blijft, zeker voor specialistische functies. Tot nu toe lukt het iRvN om vacatures in te vullen en medewerkers te behouden, maar dat vraagt blijvende aandacht voor opleiding, ontwikkeling en inhuur waar nodig.

Daarnaast nemen de kosten toe. Geopolitieke ontwikkelingen leiden tot hogere kosten bij leveranciers en de noodzaak om zowel in cloudvoorzieningen als in on-premises infrastructuur te blijven investeren zorgt voor een dubbele belasting. In de Kaderbrief 2026 en de Tussenrapportage 2025 heeft iRvN dit al benoemd. Samen met het Regionaal Strategisch I-Overleg werkt iRvN daarom aan vertalingen in geld en tijd, zodat de financiële impact beheersbaar blijft en in de begroting kan worden opgenomen.

Wat er moet gebeuren

Om dit alles in goede banen te leiden, is nauwe samenwerking en afstemming nodig. Deelnemers en iRvN bepalen samen wat lokaal moet worden opgepakt en wat regionaal beter georganiseerd kan worden.

Binnen de eigen organisatie bouwt iRvN verder aan een robuuste en wendbare structuur. De indeling in Beheer & Beveiliging en Dienstverlening heeft zich bewezen als een duidelijke en effectieve basis en wordt verder geoptimaliseerd. Tegelijkertijd breidt iRvN de aandacht uit naar regievoering, communicatie, kwaliteit en audits, service level management en procesgericht werken. Ook projectmatige samenwerking met de deelnemers wordt steeds belangrijker om vernieuwing in co-creatie tot stand te brengen.

Met 5.600 werkplekken behoort iRvN tot de grotere samenwerkingsverbanden in Nederland. Dit brengt een verantwoordelijkheid met zich mee die alleen kan worden gedragen door blijvend te investeren in professionalisering. Dat geldt voor de techniek, maar zeker ook voor de organisatiekracht en de mensen die het werk uitvoeren.

Tot slot

De digitale transitie, de cloudstrategie, informatieveiligheid, de moderne werkplek, de toepassing van AI en de borging van een robuuste infrastructuur komen in de komende periode samen. Dat betekent dat er veel werk op iRvN afkomt. Het realiseren van deze digitale ambities vraagt om bestuurlijk besef dat kwaliteit, veiligheid en samenwerking structurele investeringen vergen. De beweging die we als regio maken is daarmee niet gericht op uitbreiding, maar op versterking: we investeren vandaag om ook morgen betrouwbaar, efficiënt en veilig te kunnen werken.