Reactie op technische vragen van Leon Zoet (CDA) over het ICT raadsvoorstel.

Technische vragen:

1. Borging onafhankelijkheid van de raad in één centrale ICT-omgeving
Het voorstel plaatst raadsleden in dezelfde Microsoft-werkplekomgeving als de ambtelijke organisatie, beheerd door dezelfde ICT-leverancier.
De toelichting over “logische scheiding” is te beperkt om onafhankelijkheid te garanderen.
Vragen

1. Hoe wordt technisch geborgd dat ambtenaren geen toegang kunnen krijgen tot raadsdocumenten, e-mails, OneDrive, Teams-chats of loggegevens van raadsleden?
2. Welke beheerders (gemeentelijk of SLTN) hebben technisch toegang tot raadsaccounts, en hoe wordt dit beperkt?
3. Is er een gescheiden beheerstructuur voor de raad, of vallen raadsaccounts onder hetzelfde beheerteam als de organisatie?
4. Komt er een periodieke audit om toegang tot raadsdata te controleren?

Reactie

1. Toegang wordt ingericht op basis van Active Directory groepen die beheerd worden door onze ICT partner. Enkel leden van de gemeenteraad zullen toegevoegd worden aan groepen die rechten geven op de omgeving van de gemeenteraad en enkel gemeentelijke medewerkers worden toegevoegd aan groepen die rechten geven op de gemeentelijke omgeving. E-mails en OneDrive zijn persoonlijk en enkel inzichtelijk voor de betreffende gebuiker. Teams chats zijn enkel zichtbaar voor leden van de Teams groep en/of Teams kanaal. Loggegevens zijn inzichtelijk voor medewerkers van de ICT partner.
2. Enkel medewerkers van de ICT partner hebben technisch toegang tot de raadsaccounts.
3. Het beheer van de omgeving van de gemeenteraad zal belegd worden bij de ICT partner, dus het beheer wordt niet bij een andere beheeroganisatie belegd.
4. Raadsleden en de bijbehorende rechten worden opgenomen in een autorisatiematrix. Periodiek zal deze matrix gespiegeld worden aan de toegekende rechten en indien nodig aangepast, waarbij de matrix leidend is.
   Ook zal de omgeving meegenomen worden in de jaarlijkse audit, uitgevoerd door een onafhankelijke externe partij.

2. Verplichte inzet van Microsoft Office E5
Het voorstel schrijft Microsoft Office E5 voor alle raadsleden en fractieassistenten voor.
Er ontbreekt een analyse waarom E5 nodig is en welke alternatieven zijn onderzocht.
Vragen

5. Welke specifieke beveiligingseisen uit de Baseline Informatiebeveiliging Overheid, Network and Information Security Directive 2 en Algemene Verordening Gegevensbescherming maken E5 noodzakelijk?
6. Is een vergelijking gemaakt tussen Microsoft Office E3, E3 met beveiligingsmodules en E5?
7. Gebruikt de ambtelijke organisatie zelf ook E5, en zo ja: is dit een vereiste uniformiteit?

Reactie

5.

BIO-onderdeel	Vereiste	Waarom E5 noodzakelijk is
Logging & Monitoring	Centrale logging, correlatie, detectie afwijkend gedrag, 24/7 monitoring	E3 mist geavanceerde detectie, correlatie en threat hunting
Incidentdetectie en -respons	Continue monitoring, automatische incidentdetectie, forensische analyse	Alleen E5 heeft geautomatiseerde incidentafhandeling, attack disruption en diepgaande forensics
Identiteits- en toegangsbeheer	Sterke authenticatie, risicogebaseerde toegang,	Risk-based policies + Identity Protection + PIM ontbreken in E3

BIO-onderdeel	Vereiste	Waarom E5 noodzakelijk is
	bescherming beheeraccounts	
Beheer van beheerdersrechten	Strikte controle op adminrechten, logging, segregation of duties	Alleen E5 biedt just-in-time toegang + volledige audittrail
Bescherming van gevoelige data	Datalekpreventie, classificatie, versleuteling, monitoring van datastromen	Endpoint DLP en auto-classificatie zijn E5-only
Insider Threat Management	Inzicht in risicovol gedrag van medewerkers, detectie datalekken	Insider Risk & Communication Compliance zijn E5-only
Threat Intelligence	Actuele dreigingsinformatie, inzicht in dreigingen	Threat Explorer & TI feeds zijn niet beschikbaar in E3
Kwetsbaarheidsbeheer	Inventarisatie kwetsbaarheden, continue monitoring	Alleen E5 heeft ingebouwde TVM (Threat & Vulnerability Management)
Weerbaarheid tegen geavanceerde aanvallen	Detectie zero-days, mitigatie supply chain aanvallen	E5 heeft geavanceerde EDR/XDR en attack disruption

NIS2-onderdeel	Vereiste	Waarom E5 noodzakelijk is
Logging & monitoring	“Loggen en monitoring voor detectie van cybersecurity-incidenten”	NIS2 vereist continue monitoring — E3 kan dit niet leveren
Incident handling	“Detectie, reactie op incidenten en herstel”	E5 biedt automatische incidentrespons; E3 niet
Crisis- en operationeel beheer	Proactieve dreigingsanalyse & coördinatie	Threat Intelligence vereist E5
Supply chain security	Beheer van risico’s in ketens	Alleen E5 detecteert identity breaches, malware, privilege misuse
Aanvalspreventie en EDR	NIS2 verplicht geavanceerde EDR	E3 heeft géén EDR; alleen antivirus
Cryptografie & toegang	Sterke authenticatie + monitoring identiteit	Risk-based CA & Identity Protection ontbreken in E3
Bewustwording / threat simulation	Testen van weerbaarheid	Attack Simulation is E5-only

AVG-onderdeel	Vereiste	Waarom E5 noodzakelijk is
Integriteit & vertrouwelijkheid	Bescherming tegen ongeoorloofde toegang	Risk-based CA, Identity Protection, PIM zijn nodig
Evaluatie van maatregelen	Continue toetsing, monitoring en evaluatie	Vereist XDR, forensics en geavanceerde auditfuncties
Datalekdetectie	Datalekken moeten snel gedetecteerd en gemeld worden	Endpoint DLP, XDR en auto-classification zijn noodzakelijk
Register van verwerkingsactiviteiten	Inzicht in datastromen	Auto-labeling en DLP rapportages in E5 geven dit inzicht
Privacy by Design	Minimale toegangsrechten, logging, detectie, dataclassificatie	Vereist identity governance & dataprotectie die in E3 ontbreekt
Accountability	Aantoonbaarheid van beveiligingsmaatregelen	E5 biedt uitgebreide auditlogs en detecties

6. De gemeentelijke organisatie is enkele jaren geleden overgestapt van E3 met add-ons naar de E5 suite omdat dit onder VNG voorwaarden voordeliger is.
7. De gemeentelijke organisatie is enkele jaren geleden overgestapt van E3 met add-ons naar de E5 suite omdat dit onder VNG voorwaarden voordeliger is.

3. Advies aan raadsleden om zelf een particuliere Virtual Private Network aan te schaffen
Het voorstel adviseert raadsleden om zélf een particuliere Virtual Private Network (zoals NordVPN) aan te schaffen voor openbare wifinetwerken.
Vragen
8. Waarom wordt niet gekozen voor een centrale, gemeentelijk beheerde beveiligde netwerkoplossing?
9. Hoe past het gebruik van particuliere VPN-diensten binnen de beveiligingslijnen van de Baseline Informatiebeveiliging Overheid?

Reactie
8. Het is niet toegestaan om op openbare Wi-Fi te werken.
Als het echt niet anders kan, raden we NordVPN aan boven het werken op een niet-versleutelde openbare Wi-Fi.
9. De Baseline Informatiebeveiliging Overheid is gebaseerd op risicomanagement. Op basis van een risicoanalyse is het advies voor een VPN-oplossing gekomen als veiliger alternatief voor het werken op een niet-versleutelde openbare Wi-Fi.

4. Verplicht gebruik van privémobiele telefoons voor Multifactor Authenticatie
Het voorstel verplicht raadsleden hun eigen mobiele telefoon te gebruiken voor multifactor-authenticatie.
Vragen
10. Is deze verplichting getoetst aan de Algemene Verordening Gegevensbescherming en de gemeentelijke kaders voor apparatuurgebruik?
11. Wordt er een alternatief geboden voor raadsleden die geen geschikte telefoon hebben of hun privételefoon niet willen koppelen aan gemeentelijke beveiligingssystemen?

Reactie
10. Bij de medewerkers van de gemeente komt het MFA-verzoek binnen op hun gemeentelijke smartphone, maar de gemeenteraad beschikt niet over een door de gemeente beheerde smartphone. Hierdoor is er geen ander alternatief meer beschikbaar.
11. Nee, de Microsoft Authenticator app is vereist voor toegang tot de omgeving.

5. Formele indieningsroute via College van Burgemeester en Wethouders ontbreekt
Het voorstel erkent dat het niet via het College van Burgemeester en Wethouders is aangeboden, terwijl dit verplicht is volgens artikel 3.3.2 van het Rechtspositiebesluit decentrale politieke ambtsdragers.
Vragen
12. Wat is de reden dat deze wettelijke procedure niet is gevolgd?
13. Komt er alsnog een formeel Collegevoorstel inclusief de vereiste bruikleenovereenkomst?

Reactie
12. Artikel 3.3.2 van het Rechtspositiebesluit decentrale politieke ambtsdragers luidt: Het college van burgemeester en wethouders stelt ten laste van de gemeente aan een raadslid, een wethouder of de burgemeester voor de duur van de uitoefening van zijn functie informatie- en communicatievoorzieningen ter beschikking. Onder informatie- en communicatievoorzieningen wordt ook verstaan de daarbij behorende abonnementen.
Uw raad krijgt via het raadsvoorstel dat om praktische redenen door de griffier is opgesteld een voorziening ter beschikking. Daarmee is de wettelijke procedure gevolgd.
Uw raad heeft overigens in de Verordening raads- en commissielelden en fractieassistenten 2016 het volgende opgenomen:
Artikel 6 Informatie- en communicatievoorzieningen raads- en commissieleden

1. Een raads- of commissielid tekent een bruikleen overeenkomst wanneer hem ten laste van de gemeente voor de duur van de uitoefening van zijn functie informatie- en communicatievoorzieningen ter beschikking worden gesteld bedoeld in artikel 3.3.2 Rechtspositiebesluit decentrale politieke ambtsdragers. Het college stelt het model van de bruikleenoverenkomst vast.
2. Een raads- of commissielid levert na beëindigingvan zijn functie de ter beschikking gestelde informatie- en communicatievoorzieningen in bij de gemeente

13. Nee, dat is niet nodig. Zie de toelichting bij vraag 12
De bruikleenovereenkomst komt pas bij de uitleen van de middelen.

6. Niet-aanbesteden wordt genoemd, maar zonder juridische onderbouwing
Het voorstel motiveert dat uitbreiding van het bestaande SLTN-contract geen aanbesteding vereist.
Vragen

14. Op basis van welk exacte juridisch artikel uit de Aanbestedingswet mag uitbreiding zonder aanbesteding?
15. Hoe is vastgesteld dat dit geen “wezenlijke wijziging” van de bestaande opdracht vormt?

Reactie

14. Aangezien er met deze toevoeging geen overschrijding van de contractwaarde volgt is een aanbesteding niet nodig/verplicht.
15. Het toevoegen van domein raadnieuwkoop.nl en de bijbehorende gebruikers aan de huidige omgeving inclusief de afscherming van het gedeelte wat hiervoor gebruikt wordt heeft geen wezenlijke wijzing tot gevolg ten aanzien van de dienstverlening van de ICT partner zoals contractueel vastgelegd en/of zoals uitgevraagd tijdens het aanbestedingstraject. Juridisch gezien is dit een uitbreiding van het aantal gebruikers, wat afgevangen is binnen het contract met de ICT partner op basis van schaalbaarheid.

7. Onjuiste of onvolledige uitgangspunten bij aantal fractieassistenten
Het document erkent 30 mogelijke fractieassistenten maar rekent met 18.
Vragen

16. Waarom is gekozen voor het gemiddelde van 18 in plaats van het formeel mogelijke maximum van 30?
17. Hoe worden kosten gedekt als het aantal fractieassistenten later hoger blijkt dan 18?

Reactie

16. Een praktische- en kostenoverweging:
Waarom op voorhand al teveel notebooks bestellen als die toch niet worden gebruikt? Er worden er genoeg besteld dat iedere fractie vanaf het begin direct kan beginnen na de verkiezingen. Zodra er zicht is op een groter aantal fractieassistenten, dan worden de notebooks direct bijbesteld (waarbij een kleine order mogelijk sneller geleverd kan worden dan een grote order).
Bij 30 is dan meer geld nodig dan bij 18, terwijl de notebooks ook nog eens op de plank blijven liggen.
Tot slot staat het aantal van 30 ook niet vast. Meerdere partijen kunnen zich nog aanmelden voor verkiezingen en / of krijgen alle partijen wel genoeg stemmen voor een zetel?
17. Zolang de overschrijding niet te hoog is, is er niets aan de hand en wordt die gewoon verantwoord in de jaarrekening. In de Kadernota van het jaar erop wordt dan een hoger bedrag geraamd.
Maar is deze informatie nodig om het raadsvoorstel te verbeteren?

8. Helpdeskberekening is gebaseerd op aannames zonder onderliggende data
Het voorstel gaat uit van 2 meldingen per fractie per maand tegen €19,90 per incident.
Vragen

18. Op welke historische of vergelijkende gegevens is de inschatting van 2 meldingen per maand gebaseerd?
19. Wat is de financiële bandbreedte als het aantal meldingen substantieel hoger uitpakt?

Reactie

18. Deze berekening is niet afkomstig vanuit het team ICT.
    Geen historische of vergelijkende gegevens. Slechts ‘natte vinger werk’. Bij een volgende raming zullen de kosten wel gebaseerd kunnen zijn op de dan opgebouwde historie.
19. Stel dat het nodig is om naar de raad terug te komen, dan zal dat bij een Kadernota aan te passen zijn.
    De raad heeft immers budgetrecht.

9. Beveiliging van geheime documenten onvoldoende uitgewerkt
Het voorstel benoemt geen procedure voor digitale verwerking van geheime stukken; wel een papieren kluisoptie.
Vragen
20. Welke digitale maatregelen gelden voor geheime documenten binnen de Microsoft E5-omgeving (downloadrestricties, printbeperkingen, encryptie, logging)?
21. Komt er een formeel protocol voor het digitaal verwerken van geheime en vertrouwelijke stukken binnen IBABS en Microsoft 365?

Reactie
20. Op dit moment zijn er geen downloadrestricties en geen printbeperkingen. Encryptie en logging is wel aanwezig op de E5-omgeving.
21. Nee, tenzij de raad hierop staat. Het kán opgesteld worden.

10. Raadsleden niet betrokken tijdens opstellen voorstel
Het document vermeldt dat raadsleden “niet intensief betrokken” zijn geweest.
Vragen
22. Wat is de reden dat raadsleden niet eerder zijn betrokken bij een voorstel dat hun eigen werkvoorzieningen raakt?
23. Komt er alsnog een consultatieronde?

Reactie
22. Artikel 3.3.2 van het Rechtspositiebesluit decentrale politieke ambtsdragers luidt: Het college van burgemeester en wethouders stelt ten laste van de gemeente aan een raadslid, een wethouder of de burgemeester voor de duur van de uitoefening van zijn functie informatie- en communicatievoorzieningen ter beschikking. Onder informatie- en communicatievoorzieningen wordt ook verstaan de daarbij behorende abonnementen.
    Voor alle overheidsorganisaties geldt dat wij onze beschikbare middelen sober en doelmatig dienen in te zetten. Met het voorliggende voorstel komen meerdere belangen samen: de beschikbaarheid van ICT middelen om het ambt van raadslid te kunnen vervullen, aan te sluiten bij hetgeen aangeboden wordt aan de medewerkers in dienst van de gemeente Nieuwkoop, de digitale veiligheid wordt gewaarborgd, wij anticiperen op nieuwe wet- en regelgeving op het gebied van informatiebeveiliging. Gekozen is om het mee te delen aan de leden van het presidium. Zij hebben het raadsvoorstel op 23 oktober 2025 per mail ontvangen met het verzoek om het te delen met fractiespecialisten, zodat ‘consultatie per mail’ / ‘technische vragen stellen’ zo vroeg mogelijk zou kunnen.
23. Nee.

11. Geen implementatie-of trainingsplanning richting maart 2026
Vragen
24. Wat is de planning voor inrichting, testen, uitlevering en adoptie vóór 18 maart 2026?
25. Worden raadsleden en fractieassistenten getraind in veilig werken binnen de nieuwe omgeving?

Reactie
24. Er is op dit moment geen planning voor inrichting testen uitlevering en/of adoptie, deze kan pas gemaakt worden na een definitief besluit.
    NB: raad wordt 1 april 2026 geïnstalleerd..
25. Dat lijkt de griffie een zeer goed idee. De griffie gaat het bij het introductieprogramma inplannen.

12. Financiële afschrijvingsvraag – ontbrekende informatie

Het voorstel zegt dat de €50.000 wordt geactiveerd en afgeschreven op basis van levensduur.

Vragen

26. Wat is de gehanteerde afschrijvingsperiode voor hardware en software?
27. Is activatie van softwarekosten in lijn met de financiële verordening van de gemeente?

Reactie

26. 4 jaar
27. Het is in lijn met de financiële verordening. De € 50.000 die wordt geactiveerd betreft de aanschaf van de notebooks, wat geen software betreft maar hardware.
    De jaarlijkse softwarekosten worden, net als de rest van de organisatie, onderdeel van het ICT-beheerplan en gaan ten laste van het begrotingssaldo

13. Kosten voor 2026 ontbreken in de begroting

De structurele €21.000 wordt pas opgenomen in het ICT-beheerplan 2027–2030, terwijl de laptops in maart 2026 operationeel moeten zijn.

Vragen

28. Hoe worden de kosten in 2026 (aanschaf, licenties, inrichting, support) gedekt?
29. Is hiervoor een begrotingswijziging nodig?

Griffier

28. De aanbesteding voor het beheer van de ICT middelen van de gemeentelijke organisatie heeft een groot voordeel opgeleverd. Het eerste jaar kunnen de kosten hieruit gefinancierd worden.
29. Nee

14. Total Cost of Ownership ontbreekt

Vragen

30. Kan een Total Cost of Ownership-overzicht worden verstrekt voor de gehele periode 2026–2030, inclusief hardware, licenties, beheer, helpdesk, beveiliging, training en vervangingskosten?
31. Zijn indirecte kosten (bijvoorbeeld training, adoptie, monitoring, auditing, vervanging bij schade) opgenomen in het totaalbedrag?

Reactie

30. Eenmalige investering € 50.000. Structurele lasten € 21.000 (5 jaren). Total Cost of Ownership € 155.000
31. Monitoring en auditing zijn structurele kosten bij ICT-partner. Training en adoptie zijn aanvullende diensten die niet in het voorstel zitten. Vervanging bij schade door verwijtbaar gedrag valt onder de bruikleenovereenkomst. Vervanging bij schade door onverwijtbaar gedrag is voor kosten van de gemeentelijke organisatie.

Donderdag 4 december is er om 19.00 uur een presentatie / toelichting over dit onderwerp.