

Raadsvergadering d.d. 24 oktober 2024

Zaaknummer	Z-23-476907
Documentnummer	DOC-24-829983
Onderwerp	Bestuurlijke kaders Informatiebeveiligingsbeleid
Agendapunt	
Portefeuillehouder(s)	Gerben Gringhuis

Besluit

De raad van de gemeente Medemblik,

gelezen het bijbehorend voorstel van het college van burgemeester en wethouders van Medemblik d.d. 9 juli 2024;

gelet op het raadsbesluit van 29 september 2022 dat het informatiebeveiligingsbeleid aan de raad dient voorgelegd te worden.

Overwegende dat:

De bestuurlijke kaders voor het informatiebeveiligingsbeleid richtinggevend is voor het informatiebeveiligingsbeleid;

besluit

1. Bestuurlijke kaders voor het informatiebeveiligingsbeleid vast te stellen;

Aldus vastgesteld in de openbare vergadering van de raad van de gemeente Medemblik, gehouden op 24 oktober 2024

De griffier,

De voorzitter,



Voorstel van het college d.d.

Ter besluitvorming

Onderwerp

Bestuurlijke kaders Informatiebeveiligingsbeleid

Aanleiding

Op 29 september 2022 heeft de Rekenkamercommissie haar onderzoeksresultaten en aanbevelingen voor de informatieveiligheid van gemeente Medemblik gepresenteerd¹. Eén van de conclusies was dat het informatieveiligheidsbeleid in de gemeente Medemblik niet op orde is. Het beleid is op een te hoog abstractieniveau geschreven en daardoor moeilijk te operationaliseren en net zo moeilijk te monitoren.

De aanbeveling die daaruit voortvloeide was om het Informatieveiligheidsbeleid te herijken en daarbij te voldoen aan de verplichte Baseline Informatiebeveiliging Overheid (BIO) waarbij er oog is voor mens, organisatie en techniek.

Daarnaast zijn in 2023 en 2024 diverse landelijke ontwikkelingen in wet- en regelgeving geweest die invloed hebben op het beleid omtrent informatieveiligheid van een gemeente. Deze ontwikkelingen zijn opgenomen in het beleid.

Voorstel

1. Bestuurlijke kaders voor het informatiebeveiligingsbeleid vast te stellen;

Beoogd resultaat

Het vaststellen van beleidskaders voor het bevorderen van onze informatieveiligheid binnen onze informatievoorziening.

Argumenten

- 1.1 *Dit document geeft kaders hoe wij veilig kunnen werken in onze informatievoorziening.*
In dit document staan bestuurlijke kaders hoe wij informatiebeveiliging organiseren, welke eisen worden gesteld aan de mens, de fysieke beveiliging en de technische beveiliging. Zodat wij op een veilige manier met de gegevens van onze inwoners, ondernemers en medewerkers kan worden gewerkt.
- 1.2 *De bestuurlijke kaders zijn gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).*
De BIO is het verplichte framework voor overheden op het gebied van informatiebeveiliging. Het naleven is gedeeltelijk verankerd in de “Wet Digitale Overheid”

¹ <https://medemblik.bestuurlijkeinformatie.nl/Agenda/Document/e940e245-f6c3-4e27-8e8b-2c28039c2358?documentId=46b216fc-64c4-467b-82d2-b8a20822f3b9&agendatItemId=4fa68eab-8213-4349-a18e-72152b0acc43>



en zal een verdere verankering krijgen in de “Cyberbeveiligingswet²” in 2025.

1.3 *De bestuurlijke kaders bereid ons voor op wettelijke verplichtingen.*

Vanuit Europa is een nieuwe richtlijn opgesteld die strengere eisen en verplichtingen stelt aan de informatiebeveiliging van een organisatie. Deze richtlijn wordt overgenomen in nationale wetgeving. De NIS2 staat voor “Network and Information Security”. De bedoeling van deze richtlijn is het verkleinen van de maatschappelijke en economische impact bij een digitaal incident. Zo krijgen organisaties te maken met een zorgplicht, meldplicht en toezicht (achter- en vooraf) inclusief boete regime. Deze richtlijn wordt in Nederland naar verwachting actief in 2025 onder de “Cyberbeveiligingswet”. Gemeente vallen onder de zwaarste categorie en krijgen te maken met de zwaarste vorm van toezicht onder de wet.

1.4 *Aanbieding is conform raadsbesluit.*

Tijdens de gemeenteraad van 29 september 2022 is besloten dat het informatiebeveiligingsbeleid ter besluitvorming voorgelegd dient te worden aan de raad.

Kanttekeningen

1.1 *Een digitaal incident, zoals een hack of een gijzeling van onze informatievoorziening, kan altijd gebeuren dit risico neemt het beleid niet volledig weg.*

Ongeacht hoe de naleving van dit beleid is kan een digitaal incident altijd gebeuren. Cybercriminelen gebruiken steeds geavanceerdere technieken waardoor, net zoals bij de traditionele (georganiseerde) criminaliteit, lopen wij achter de feiten aan. Het risico op een digitaal incident wordt daarom ook nooit nul. Dit beleid stelt ook eisen aan het opstellen van Bedrijfscontinuïteit Management zodat wij voorbereid zijn bij een digitaal incident.

1.2 *In 2024 komt een nieuwe versie van de BIO uit.*

In de tweede helft van 2024 wordt de BIO versie 2 verplicht gesteld voor alle overheidslagen. De exacte teksten worden in het einde van het tweede kwartaal van 2024 verwacht. In 2023 is een was-woord lijst gepubliceerd waar de wijzigingen zijn opgenomen. Deze zijn verwerkt in het beleid. Daarnaast voorziet het beleid in een PDCA-cyclus waarmee eventueel verdere aanpassingen doorgevoerd kunnen worden.

1.3 *De Nederlandse concept wettekst van de Cyberbeveiligingswet is op 21 mei 2024 gepubliceerd.*

Bij het opstellen van de Nederlandse wettekst is vertraging opgelopen. De oorspronkelijke deadline waarop de Nederlandse wet actief zou moeten zijn was oktober 2024. Dit is inmiddels uitgesteld naar 2025. De consultatieronde van de wettekst is op 21 mei 2024 gestart. De Algemene Maatregel(en) van Bestuur (AMvB) volgen later waarna nadere regelgeving duidelijk wordt. Voor een zo goed mogelijke borging van deze

² <https://www.internetconsultatie.nl/cyberbeveiligingswet/b1>



komende wetgeving zijn de adviezen van de VNG en Informatiebeveiligingsdienst in het beleid opgenomen. Wel blijkt duidelijk uit de Memorie van Toelichting³ van de Cyberbeveiligingswet dat de BIO een wettelijke verankering krijgt voor overheden. Door de BIO, die reeds al verplicht is, verder te implementeren bereiden wij ons voor. Wanneer blijkt dat verdere wijzigingen nodig zijn voorziet het beleid in een PDCA-cyclus waarmee eventuele aanpassingen doorgevoerd kunnen worden.

Financiën

De aanvraag voor de benodigde financiële middelen is ondergebracht in de P&C-cyclus. Middelen die nodig zijn voor 2024 worden via de Lentenota 2024 aangevraagd. De benodigde middelen voor 2025 en verder worden middels de Begroting 2025 aangevraagd.

Uitvoering/evaluatie

De implementatie van dit beleid is beschreven in een Uitvoeringsplan Informatiebeveiliging.

Communicatie

De implementatie, inclusief diverse communicatiemomenten, zijn onderdeel van een Uitvoeringsplan Informatiebeveiliging.

Bijlagen

DOC-24-845965 Bestuurlijke kaders informatiebeveiligingsbeleid

Commissie d.d.

³ <https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12562>

