ADVIESNOTA voor burgemeester en wethouders **Openbare besluitenlijst**

Zaaknummer:

Medewerker	:	Wessel Hemels (en Stephanie Scholten)
Team	:	Bedrijfsvoering en Communicatie
Datum	:	8 juli 2024
Portefeuillehouder	:	burgemeester Sietske Poepjes

BIJLAGEN:
☒ Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2024 –
☒ Raadsmededeling informatiebeveiligingsbeleid 2024 –

AFSTEMMING MET
☒ Portefeuillehouder tijdens PO van 24 juni jl.

☒ Openbaar
☐ Vertrouwelijk

ONDERWERP
Informatiebeveiligingsbeleid 2024

BESLUIT burgemeester en wethouders
1. Het informatiebeveiligingsbeleid 2024 vast te stellen
2. De raadsmededeling vast te stellen en aan te bieden aan de gemeenteraad

SAMENVATTING

Met het geactualiseerde informatiebeveiligingsbeleid zetten de DOWR-gemeenten een volgende richtinggevende en kaderende stap voor de komende jaren om de beveiliging van persoonsgegevens en andere gemeentelijke informatie te continueren en voort te bouwen op de stappen die in de voorgaande jaren door de DOWR-gemeenten gezet zijn op het gebied van informatieveiligheid en privacy.

Deze beleidsvernieuwing omvat tevens de voorbereiding op de implementatie van belangrijke nieuwe wet- en regelgeving, waaronder de Network and Information Systems Directive (NIS2) en daaruit voortkomend de Baseline Informatiebeveiliging Overheden (BIO) 2.0 norm die naar verwachting eind 2024 wettelijk verankerd zal worden. Hoewel de BIO 2.0 nog niet definitief is vastgesteld, nemen we reeds stappen om ons voor te bereiden op de verwachte aankomende veranderingen. Dit onderstreept onze proactieve benadering en ons streven naar een tijdige en effectieve naleving van de nieuwe regelgeving.

AANLEIDING

In overeenstemming met de Informatiebeveiligingsdienst gemeenten (IBD) en de VNG wordt de werkwijze gehanteerd dat het strategisch beleid bestuurlijk door de drie gemeenten moet worden goedgekeurd. Alle onderliggende (tactische/operationele) beleidsstukken zijn in lijn met dit strategisch beleid én de BIO waardoor volstaat om goedkeuring te verkrijgen. De 14 tactische beleidstukken zijn vastgesteld door de directie.

Het management DOWR-I heeft alle beleidsstukken individueel beoordeeld en akkoord bevonden. Daarnaast is het ook, ter informatie en om duiding te geven, aan de regiegroep, het CIO overleg, directieberaad DOWR en de directie voorgelegd. Hier zijn ook geen bezwaren opgetekend.
Met het geactualiseerde informatiebeveiligingsbeleid zetten de DOWR-gemeenten een volgende richtinggevende en kaderende stap voor de komende jaren om de beveiliging van persoonsgegevens en andere gemeentelijke informatie te continueren en voort te bouwen op de stappen die in de voorgaande jaren door de DOWR-gemeenten gezet zijn op het gebied van informatieveiligheid en privacy.

BEOOGD RESULTAAT
De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Met de vaststelling van het beleid voldoen we aan dit kader.

KADER
- Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2024
- Baseline Informatiebeveiliging Overheden (BIO 2.0): in 2024 van kracht
- i-Visie najaar 2022

ARGUMENTEN VOOR

Voor:
1.1 De ontwikkelingen op het gebied van informatieveiligheid gaan snel wat de noodzaak geeft tot actualisatie van het informatiebeveiligingsbeleid
Als er een terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties geven voor de toekomst, is dat digitale veiligheid. Digitale veiligheid vraagt om een voortdurende en complexe evenwichtsoefening om uiteenlopende belangen, het voldoen aan wet- en regelgeving, en digitale dreigingen in balans te krijgen en te houden.
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten wijst op een toenemende dreiging, wat wordt bevestigd door voorbeelden van cyberaanvallen op gemeentelijke organisaties in de afgelopen jaren. Het laat zien dat ransomware-aanvallen frequenter voorkomen en ernstigere gevolgen hebben, zoals verstoring van dienstverlening. Bovendien vertoont software meer kwetsbaarheden, waarop we proactief moeten reageren. In lijn hiermee is het essentieel dat we controle blijven uitoefenen over de ketens van onze dienstverlening. Hierbij valt te denken aan de contracten die we afsluiten, de gestelde eisen en de informatie die we delen met leveranciers.

Belangrijke veranderingen ten opzichte van voorgaande jaren zijn:
- Geoblocking:

Dit is een maatregel die ervoor zorgt dat onze digitale systemen niet toegankelijk zijn vanuit landen die bekend staan om hun actieve cyberoffensieven. Dit betekent dat we de toegang tot onze digitale diensten beperken voor locaties waarvan we weten dat ze een verhoogd risico vormen voor cyberaanvallen. Hierdoor kunnen we de veiligheid van onze systemen versterken en de kans op potentiële bedreigingen verminderen.

- Contractbeheer:

We hebben ons contractbeheer versterkt door beveiligingseisen op te nemen in de contracten met informatieverwerkende leveranciers. Deze eisen zorgen ook ervoor dat leveranciers de gemeente op de hoogte stellen van mogelijke risico's.

- Wachtwoorden:

Het wachtwoordbeleid is vernieuwt vanwege nieuwe technologieën en mogelijkheden. Dit is gedaan om de algehele beveiliging te verbeteren. Tegelijkertijd is er ook aandacht besteed aan het gebruiksvriendelijkheid. Deze veranderingen zijn bedoeld om een betere balans te creëren tussen verbeterde beveiliging en een meer gebruiksvriendelijke ervaring voor de gebruikers.

- Nieuwe werkplek:

Het beleid voor telewerken is aangepast naar een nieuw werkplekconcept met meer flexibiliteit, waarbij gebruik wordt gemaakt van laptopwerkplekken. Dit bevordert een modernere en efficiëntere werkomgeving voor onze medewerkers.
Ook sluiten we met dit beleid aan op de nieuwe i-Visie. Deze aansluiting is minstens zo belangrijk om actief bij te dragen aan de bredere strategische visie op het gebied van digitalisering van onze gemeenten.

ARGUMENT TEGEN
Onvoldoende capaciteit en budget voor toekomstige uitvoering.

RISICO’S
n.v.t.

FINANCIËN

Er wordt momenteel een inschatting gemaakt van de verwachte toename in kosten als gevolg van de nieuwe wetgeving. Op dit moment is het huidige budget toereikend, maar we anticiperen op een stijging vanaf 2025.

DUURZAAMHEID
n.v.t.

PARTICIPATIE
n.v.t.

COMMUNICATIE
Nadere communicatie naar aanleiding van dit besluit is niet noodzakelijk.

PLANNING EN UITVOERING
Na vaststelling van het college van het strategisch informatiebeveiligingsbeleid (bijlage 1) is het informatiebeveiligingsbeleid van kracht.