Oordeelsvormende vergadering Papendrecht

Voorstel
Openbaar

Vergadering van 16 januari 2025
Zaaknummer: 2024-0111090

Strategisch Informatiebeveiligingsbeleid 2025 - 2029

Bevoegde portefeuillehouder: Jan Dirk van der Borg

Wettelijke basis (aanvullend)
Op dit moment geldt de Baseline Informatiebeveiliging Overheid voor gemeente voor informatiebeveiliging. Sinds 17 oktober 2024 geldt de Network and Information Security directive (NIS2-richtlijn). Deze is vastgesteld door de Europese Unie (EU) en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2-richtlijn wordt momenteel vertaald naar Nederlandse wetgeving ingaande 2e of 3e kwartaal 2025.

Fatale termijn:
Het is wenselijk het Strategisch informatiebeveiligingsbeleid Drechtsteden 2025-2029 zo spoedig mogelijk in werking te laten treden na vaststelling door de raad op 30 januari 2025.

Gevraagd besluit

1. Kennis te nemen van het door het college en de burgemeester voor de gemeentelijke organisatie vastgestelde Strategisch informatiebeveiligingsbeleid Drechtsteden 2025-2029.
2. Het Strategisch informatiebeveiligingsbeleid Drechtsteden 2025-2029 vast te stellen.

Inhoud

Inleiding
Informatieveiligheid is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en onze dienstverlening, cyberdreigingen, digitale aanvallen, de decentralisatie van overheidstaken, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Informatieveiligheid raakt de gehele bedrijfsvoering en verdient samen met privacybescherming continu aandacht. Hoe gevoeliger/waardevoller de (persoons)gegevens zijn, hoe meer maatregelen er getroffen moeten worden om deze gegevens te beschermen tegen onrechtmatige toegang en/of misbruik en/of manipulatie.
Conform wet- en regelgeving beschikken de gemeenten in onze regio over een Strategisch Beleid Informatiebeveiliging (hierna: IB Beleid) In dit IB beleid zijn de kaders vastgelegd om zorg te dragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatievoorziening, waardoor we de continuïteit van onze dienstverlening aan burgers, bedrijven en samenwerkingspartners kunnen bewerkstelligen.
Het laatst vastgestelde IB Beleid heeft een looptijd van 2020 tot 2024.Het huidige IB Beleid is conform wetgeving nog geldig totdat nieuw beleid is vastgesteld.
In de loop van 2023 heeft de Chief information security officer (CISO) Drechtsteden het initiatief genomen het IB Beleid te actualiseren. De directe aanleidingen daarvoor waren:

- Het einde van de looptijd van het huidige IB Beleid.
- Het eerdere samenwerkingsverband van het Service Centrum Drechtsteden (SCD) binnen de Gemeenschappelijke Regeling Drechtsteden is per 1 januari 2022 gewijzigd. Het voormalige SCD werd opgeheven en is “as-is” overgegaan in de Service Gemeente Dordrecht.
- Geo-politieke ontwikkelingen brengen veranderingen in het dreigingsbeeld.

De gemeenteraad heeft eerder aangegeven graag meer aangesloten te willen worden op ICT gerelateerde onderwerpen. Gepland is dat op 6 februari 2025 tijdens de beeldvormende

raadsvergadering een interactieve sessie zal plaatsvinden over de impact van de nieuwe Europese informatiebeveiligingswetgeving.

Beoogd effect
Zorg dragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatievoorziening waardoor we de continuïteit van onze dienstverlening aan burgers, bedrijven en samenwerkingspartners kunnen bewerkstelligen volgens de geldende wet- en regelgeving.

Argumenten
2.1 Een meerjarig regionaal strategisch informatiebeveiligingskader dient te worden vastgesteld.
De Baseline Informatiebeveiliging Overheid schrijft het hebben van een geactualiseerd informatiebeveiligingsbeleid voor. Met het vaststellen van het regionale strategisch informatiebeveiligingsbeleid voor de jaren 2025 tot 2029 kijken we vooruit en voldoen we aan die plicht.
2.2 De kaderstellende bevoegdheid ligt bij de raad.
Het Strategisch Informatiebeveiligingsbeleid Drechtsteden geeft een richtinggevend beleidskader met leidende principes teneinde de wettelijke eisen in te vullen. Het geeft een kapstok voor het onderliggende uit te werken tactische en operationele informatieveiligheidsbeleid, waarvoor elk jaar een uitvoerend beleidsplan zal worden opgesteld. Gezien de kaderstellende bevoegdheid wordt de raad voorgesteld dit beleid vast te stellen.
2.3 Elk bestuursorgaan dient het Informatieveiligheidsbeleid vast te stellen.
Zowel het college, de burgemeester als de raad moet, voor zover het zijn of haar bevoegdheid betreft, het informatieveiligheidsbeleid vaststellen. Elk bestuursorgaan is er zelf verantwoordelijk voor dat de door hem uitgevoerde verwerking van (persoons)gegevens op zorgvuldige wijze geschiedt en dat er voldaan wordt aan de eisen van informatieveiligheid. Door vaststelling door de raad gelden de leidende principes uit het beleid ook voor de verwerkingen door de griffie. Het informatieveiligheidsbeleid geeft hier invulling aan.
2.4 Alle betrokken regionale Drechtstedengemeenten stellen het strategisch informatiebeveiligingsbeleid vast.
De gemeente blijft verantwoordelijk voor het vaststellen van het informatiebeveiligingsbeleid ondanks dat bepaalde bevoegdheden zijn gemandateerd aan de Service Gemeente Dordrecht. Met het afzonderlijk vaststellen van dit Strategisch Informatiebeveiligingsbeleid Drechtsteden stellen de in totaal zeven gemeenten (Alblasserdam, Dordrecht, Hardinxveld-Giessendam, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht en Zwijndrecht) en drie gemeenschappelijke regelingen (Dienst Gezondheid & Jeugd, GR Sociaal en de omgevingsdienst Zuid-Holland Zuid) een richtinggevend strategisch informatiebeveiligingskader vast.
2.5 De uitvoering van het beleid wordt opgepakt door de Service Gemeente Dordrecht.
Het Strategisch Informatiebeveiligingsbeleid Drechtsteden is van toepassing op de geleverde dienstverlening door of vanuit de Service Gemeente Dordrecht en alle uit te voeren processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen), inclusief gegevensverwerking die in de Cloud zijn of worden ondergebracht.
2.6 Gebruik is gemaakt van het beleidsmodel van de Informatiebeveiligingsdienst (IBD).
Als basis voor het opstellen van strategisch beleid is gebruik gemaakt van de handreiking van de Informatiebeveiligingsdienst (IBD). Door de Chief Information Security Officer (CISO) en door de gemeentelijke leden binnen het Periodiek Informatiebeveiliging Overleg Drechtsteden (PIO-D) is dit aangepast aan de Drechtsteden context. Het beleid is echter een levend document. Ieder jaar zal de Drechtsteden binnen het PIO-D gezamenlijk het beleid evalueren en waar nodig bijstellen en ter besluitvorming aanbieden.

Kanttekeningen
2.1 Lokaal afwijken van het regionale IB beleid is mogelijk.
Relevante wetgeving is van toepassing voor alle deelnemers binnen het regionale samenwerkingsverband. Er is binnen de uitvoering van het beleid ruimte voor lokale afwijkingen en prioriteringen op basis van het “pas toe of leg uit” principe mits dit de continuïteit van de bedrijfsvoering niet in gevaar brengt. De afwegingen om af te wijken van het IB beleid worden door de lokale proceseigenaar schriftelijk vastgelegd. De Chief Information Security Officer geeft hierop een advies. De afwijking dient voorafgaand aan de uitvoering te worden geaccepteerd door de bevoegde manager.

Financiën
De uitvoering van het informatiebeveiligingsbeleid gebeurt vooralsnog met bestaande budgetten. Afhankelijk van het verschil tussen huidige en gewenste en veranderende wettelijke situatie zal er separaat budget nodig zijn. Dit zal separaat aan u worden voorgelegd of worden meegenomen in de bijdrage aan de Service Gemeente Dordrecht (SGD).

Uitvoering
Het Strategisch Informatiebeveiligingsbeleid Drechtsteden vormt de kaders voor het verder jaarlijks uit te werken beleidsplan op tactisch en operationeel niveau. Het Strategisch Informatiebeveiligingsbeleid Drechtsteden is de basis om informatiebeveiliging op een goede manier te borgen in onze processen. De jaarlijkse informatiebeveiligingsplannen worden verwerkt in de begroting onder de paragraaf bedrijfsvoering -informatiebeveiliging.
Het primaire uitgangspunt voor onze informatieveiligheid is en blijft risicomanagement. Dat vereist een integrale aanpak, goed opdrachtgeverschap, onderlinge samenwerking en risicobewustzijn, waarbij ieder organisatieonderdeel is betrokken. De nadruk komt hierdoor te liggen op de governance rondom onze informatieveiligheid. Ook de Baseline Informatiebeveiliging Overheid 2 en de Network and Information Security directive (NIS2-richtlijn) sluiten hierop aan door de verantwoordelijkheid voor informatiebeveiliging in de organisatie(s) nadrukkelijk neer te leggen bij het bestuur en de proceseigenaren. Deze verantwoordelijkheid brengt met zich mee dat de proceseigenaren de risico's op het niveau van de werkprocessen/informatiesystemen in beeld hebben met als doel het implementeren en onderhouden van passende organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen. Overblijvende (rest)risico's worden op het juiste bestuurs- / managementniveau geaccepteerd.

Communicatie & participatie
Intern zal publicatie plaatsvinden op SID, in het Handboek AO en in het personeelshandboek. Extern wordt het gepubliceerd op www.officielebekendmakingen.nl.

Duurzaamheid & ecologie
Niet van toepassing.

ICT
Niet van toepassing.

Alle relevante stukken zijn voor u ter inzage gelegd.

Burgemeester en wethouders van Papendrecht,

Bijlagen

1. Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025-2029.pdf
2. Samenvatting Strategisch Informatiebeveiligingsbeleid.docx