Gemeente Haarlem

Collegebesluit

Onderwerp Informatiebeveiligingsbeleid 2019-2023	
Nummer	2018/812821
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hotting, E.
Telefoonnummer	023-5115061
Email	ehotting@haarlem.nl
Kernboodschap	Het doel van deze beleidsnota is het presenteren van het normstellend beleid voor de Informatieveiligheid. Door veranderende omstandigheden is het huidige Informatiebeveiligingsbeleid niet langer toereikend. De organisatie kan door de snel toenemende compliancy-druk niet langer rapporteren op de in het huidige beleid voorgeschreven wijze. Daarnaast wordt in het nieuwe beleid aangesloten op de geheeld nieuwe Baseline voor Informatieveiligheid, welke vanaf 2019 voor de gehele overheid geldt: De BIO. Het huidige beleid is gebaseerd op de BIG. Het nieuwe beleid met de nieuwe baseline verschuift de nadruk weer naar het proces van eigen risicoafwegingen en zorgt er bovendien voor dat het bestuur goed 'in control' blijft. Dit beleid is opgesteld in nauw overleg met de opstellers van de BIO en de Informatiebeveiligingsdienst. Haarlem is daarmee de eerste gemeente die deze stap zet, mede veroorzaakt door het onderzoek van de Rekenkamercommissie in Haarlem.
Behandelvoorstel voor commissie	Niet van toepassing
Relevante eerdere besluiten	- Aanstelling IT-auditor (2017/34120), zoals besproken in het college van 28 februari 2017 - Mandatering bevoegdheid tot verstrekken van opdrachtbevestigingen aan interne IT auditor (2018/7523), zoals besproken in het college van 16 januari 2018) - Vaststellen Collegeverklaring ENSIA 2017 (2018/222795) zoals besproken in de collegevergadering van 8 mei 2018

Besluit College d.d. 18 december 2018	Het college van burgemeester en wethouders Besluit: 1. Het Strategisch Informatiebeveiligingsbeleid 2019 – 2023 vast te stellen. de secretaris, de burgemeester,

1. Inleiding

Het doel van deze beleidsnota is het presenteren van het normstellend beleid voor de Informatieveiligheid. Door veranderende omstandigheden is het huidige Informatiebeveiligingsbeleid niet langer toereikend. De organisatie kan door de snel toenemende compliancy-druk niet langer rapporteren op de in het huidige beleid voorgeschreven wijze. Daarnaast wordt in het nieuwe beleid aangesloten op de geheeld nieuwe Baseline voor Informatieveiligheid, welke vanaf 2019 voor de gehele overheid geldt: De BIO. Het huidige beleid is gebaseerd op de BIG.

De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Het nieuwe beleid met de nieuwe baseline verschuift de nadruk weer naar het proces van eigen risicoafwegingen en zorgt er bovendien voor dat het bestuur goed 'in control' blijft. Dit wordt o.a. gerealiseerd door de rapportagecyclus in te richten volgens ENSIA. Het beleid wordt daarmee weer uitvoerbaar voor de organisatie en stelt de organisatie in staat om te werken zoals gewenst, namelijk op basis van risicoanalyses.

Dit beleid is opgesteld in nauw overleg met de opstellers van de BIO en de Informatiebeveiligingsdienst. Haarlem is daarmee de eerste gemeente die deze stap zet, mede veroorzaakt door het onderzoek van de Rekenkamercommissie in Haarlem.

In 2019 wordt de rol van Chief Information Security Officer ingevuld door er een volwaardige functie van te maken. Vanuit deze functie wordt het in het nieuwe beleid aangekondigde beleid op tactisch niveau verder uitgewerkt en een sterk verbeterde rapportage richting directie en college opgezet.

2. Besluitpunten college

Het college besluit het Strategisch Informatiebeveiligingsbeleid 2019 – 2023 vast te stellen.

3. Beoogd resultaat

Met het nieuwe Informatiebeveiligingsbeleid wordt de organisatie in staat gesteld te rapporteren op een manier die past bij de vanuit het Rijk opgelegde jaarlijkse ENSIA audit. De taken en verantwoordelijkheden welke nodig zijn om de informatiebeveiligingsbeleid te borgen zijn zodanig verdeeld dat de gehele organisatie bij gaat dragen aan de uitvoering van het beleid.

4. Argumenten

1. Door snelle ontwikkelingen is het huidige Informatiebeveiligingsbeleid niet langer uitvoerbaar zonder zeer grote extra inspanning. Het nieuwe beleid is gericht op het uitvoerbaar maken met de huidige organisatie.
2. De rapportage naar het college en de raad wordt verbeterd en krijgt een hogere frequentie.
3. Dit besluit heeft geen financiële consequenties.

5. Risico's en kanttekeningen

n.v.t

6. Uitvoering

n.v.t

7. Bijlagen

A. Informatiebeveiligingsbeleid 2019-2023