gemeente
Hoeksche Waard

Strategisch informatiebeveiligingsbeleid gemeente Hoeksche Waard 2020-2024

Inhoud

1. Vertrekpunt informatiebeveiligingsbeleid

Deze beleidsnota beschrijft het strategische informatiebeveiligingsbeleid Gemeente Hoeksche Waard voor de jaren 2020 tot 2024 en vervangt het in 2019 vastgestelde "Gemeentelijk Informatiebeveiligingsbeleid 2019-2020[1]". Met de komst van het normenkader BIO (Baseline Informatie Overheid), is de gemeente genoodzaakt om een nieuw en passend informatiebeveiligingsbeleid te formuleren. Het strategische beleid borduurt voort op het Kompas en de beleidsfilosofie van gemeente Hoeksche Waard. Verder is deze nota richtinggevend en kaderstellend. Het wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau, zoals het informatiebeveiligingsplan (IBP) en werkinstructies op operationeel niveau.

Met dit "Strategisch Informatiebeveiligingsbeleid 2020-2024" zet de Gemeente Hoeksche Waard een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren, hierbij rekening houdend dat informatiebeveiliging een *proces* is, waar continue aandacht voor nodig is de komende jaren.

1.1 Wat is informatiebeveiliging

Onder informatiebeveiliging wordt verstaan: "Het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen". Kernpunten daarbij zijn *beschikbaarheid*, *integriteit* (juistheid) en *vertrouwelijkheid* van persoonsgegevens en alle informatiestromen.

Het informatiebeveiligingsbeleid geldt voor alle processen[2] van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het (politiek) bestuur, alle processen en op personen; alle medewerkers, burgers en externe partijen.

[1] Informatiebeveiligingsbeleid 2019-2020; http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/Historie/Hoeksche%20Waard/CVDR622812/CVDR622812_1.html.
[2] Alle processen: hierin wordt verwezen naar alle processen waarin informatiestromen lopen.

2. Inleiding

2.1 Doel van dit beleid

Het doel van deze beleidsnota is het bieden van een stip op de horizon ten aanzien van informatiebeveiliging voor de gemeente Hoeksche Waard voor een periode van 3 jaar. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen Informatiebeveiligingsplan.

2.2 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente Hoeksche Waard en haar externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen (bijvoorbeeld ENSIA). Deze worden in aanvullende documenten geformuleerd.

In het Strategisch beleid geven wij geen limitatief overzicht van onderliggende documenten. Wel dienen vastgestelde beleidsdocumenten voor de bedrijfsvoering zich expliciet te conformeren aan het informatiebeveiligingsbeleid.

3.Aandachtspunten voor informatiebeveiliging

3.1 Plaats van het strategische beleid

Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid voor de gemeente Hoeksche Waard. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het twee jaar geldend te schrijven 'Gemeentelijk Informatiebeveiligingsplan', welke goedgekeurd dient te worden door het directieteam.

3.2 Dreigingsbeeld Nederlandse Gemeenten

Het Dreigingsbeeld Nederlandse Gemeenten[3] geeft een actueel zicht op incidenten en factoren uit het verleden aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is voor de gemeente Hoeksche Waard een indicatie en informatiebron om nieuwe risico's en dreigingen te identificeren. De CISO is namens de gemeente Hoeksche Waard aangemeld bij de Informatiebeveiligingsdienst (IBD, VNG) en ontvangt periodiek berichten en rapportages hierover. Deze worden hierop meegenomen in de incidentenrapportages.

3.3 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente Hoeksche Waard kent naast het hierboven genoemde dreigingsbeeld natuurlijk ook een eigen systeem waarin incidenten worden vastgelegd. Het functioneren en behoud van dit systeem zijn de verantwoordelijkheid van directeur met portefeuille bedrijfsvoering en worden gewaarborgd door (integrale/) informatieveiligheid. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het uitvoeren en actualiseren van het beleid.

3.4 Randvoorwaarden

Belangrijke randvoorwaarden om dit beleid te implementeren zijn:

1. De informatiebeveiligingstaken zijn belegd binnen de bedrijfsprocessen en de benodigde kwalitatieve en kwantitatieve resources zijn beschikbaar gesteld.
2. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
3. Medewerkers gaan verantwoordt om met (persoons)gegevens en andere informatie(systemen), spreken elkaar aan op onveilig gedrag en melden mogelijke hiaten direct aan de leidinggevenden.
4. De informatiebeveiliging maakt deel uit van afspraken met ketenpartners en dienstenleveranciers.
5. Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd bij alle lagen binnen de organisatie, ketenpartners en externe partijen.

[3] Het dreigingsbeeld NL/IBD: https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2019-2020/.

6. Er zijn voldoende maatregelen geïmplementeerd die zorgen dat kwetsbaarheden in bedrijfsprocessen worden verkleind. Hierdoor worden informatiebeveiligingsincidenten verkleind en de effecten van de incidenten beperkt.
7. Periodiek worden onafhankelijke audits uitgevoerd om vast te stellen of de vereiste maatregelen uit het beleid in voldoende mate zijn geborgd.
8. De digitale weerbaarheid wordt verhoogd door de basis op orde te brengen.
9. Security en privacy by design principes worden toegepast bij innovaties. Denk hierbij aan common ground, internet of things (IoT) en datagedreven werken.

Deze randvoorwaarden zijn van belang om informatiebeveiliging te borgen binnen de gemeente Hoeksche Waard.

3.5 Doelen Informatiebeveiliging
De gemeente Hoeksche Waard kent de volgende strategische doelen voor het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging;
- Adequate bescherming bieden van bedrijfsmiddelen;
- Het minimaliseren van risico's van menselijk gedrag;
- Het voorkomen van ongeautoriseerde toegang;
- Het garanderen van correcte en veilige informatievoorzieningen;
- Het beheersen van de toegang tot informatiesystemen;
- Het waarborgen van veilige informatiesystemen;
- Het adequaat reageren op incidenten;
- Het beschermen van kritieke bedrijfsprocessen;
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
- Het waarborgen en integreren van het privacybeleid;

- Het waarborgen van de naleving van dit beleid.

De vertaling van deze strategische doelen zal verder tot uiting komen in het Informatiebeveiligingsplan.

4.Ontwikkelingen

De gemeente Hoeksche Waard maakt veel ontwikkelingen mee op verschillende niveaus. De reden dat het informatiebeveiligingsbeleid geactualiseerd dient te worden is door een wijziging in de wet- en regelgeving, de ontwikkelingen die de gemeente Hoeksche Waard als fusiegemeente heeft doorstaan, de 10 basis principes ten aanzien van informatiebeveiliging opgesteld door de Informatiebeveiligingsdienst (VNG) en het dreigingsbeeld opgesteld door het NCSC welke continue in beweging is.

4.1 Een nieuwe baseline voor informatiebeveiliging

De BIO (Baseline Informatiebeveiliging Overheid) is sinds 1-1-2019 het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement, in tegenstelling tot de voormalige Baseline Informatiebeveiliging Gemeente (BIG)-richtlijnen. Dat wil zeggen dat proceseigenaren nu meer dan voorheen dienen te werken volgens de aanpak van de ISO-27001, waarbij risicomanagement centraal staat. Dit houdt voor het directie- en management team in, dat zij op voorhand keuzes en continu afwegingen dienen te maken of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Deze processen dienen te worden geregistreerd en deze zullen periodiek gecontroleerd door de CISO.

4.2 Handvaten voor de rol van de bestuurder

De 10 principes voor de informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader[4] BIO en gaan over de waarden die het college aan de organisatie en zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilig cultuur;

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Informatiebeveiliging is van iedereen;

2. Informatiebeveiliging is risicomanagement;

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

3. Risicomanagement is onderdeel van de besluitvorming;

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

4. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;

[4] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en de Verenigde Nederlandse Gemeenten (VNG).

Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.

5. Informatiebeveiliging is een proces;

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

6. Informatiebeveiliging kost geld;

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

7. Onzekerheid dient te worden ingecalculeerd[5];

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

8. Verbetering komt voort uit leren en ervaring;

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

9. Verbetering komt voort uit leren en ervaring;

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

10. Het bestuur controleert en evalueert;

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het waarborgen van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en

[5] Het incalculeren van onzekerheden; besluiten worden gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

partners van de gemeente, daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

5. Organiseren van informatiebeveiligingsbeleid

De gemeenteraad, College van Burgemeester en Wethouders, de directie en het management team spelen een cruciale rol binnen de gemeente Hoeksche Waard bij het waarborgen van dit informatiebeveiligingsbeleid.

5.1 Het belang van betrokkenheid

Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, van de risico's die de gemeente hiermee loopt op basis van de opgestelde richtlijnen[6]. Ook draagt het team van managers verantwoordelijk voor het uitdragen, het ondersteunen en bewaken van dit informatiebeveiligingsbeleid. Hierover wordt via een processysteem gerapporteerd. De CISO gebruikt deze rapportages om het informatiebeveiligingsniveau periodiek te toetsen en om vanuit security invalshoek de gemeente Hoeksche Waard te adviseren.

Het directieteam bepaalt uiteindelijk welke van deze risico's acceptabel of onacceptabel zijn. De risico's worden aangeboden door de CISO. Verder geeft het directieteam een duidelijke richting aan informatiebeveiliging en demonstreert hiermee dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente.

De CISO en concerncontroller faciliteert en adviseert de organisatie met en bij het informatiebeveiligingsbeleid. Verder zal dit Informatiebeveiligingsbeleid ook fungeren als toetsingskader om te bepalen in hoeverre de gemeente 'in control' is.

De Burgemeester is eindverantwoordelijk voor de informatiebeveiligingsniveau binnen de gemeente Hoeksche Waard, het informatiebeveiligingsniveau kent namelijk een directe link met cybersecurity en daarmee met de digitale veiligheid(en weerbaarheid) van de gemeente.

Het College van Burgemeester en Wethouders zijn verantwoordelijk voor het goedkeuren en waarborgen van de inhoud van het informatiebeveiligingsbeleid. Tot slot is het informatiebeveiligingsbeleid in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan de gemeenteraad toekent.

5.2 Alle medewerkers

- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Medewerkers dienen bij afwijkingen, incidenten of vragen een melding te doen.

[6] Deze richtlijnen komen voort uit het Informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

5.3 Gemeenteraad en het College van Burgemeester &Wethouders

- Het College van B&W stelt het strategisch informatiebeveiligingsbeleid vast, (minimaal) eens per 4 jaar.
- Informatiebeveiliging is een (veiligheids-)zorg van de Burgemeester.
- De gemeenteraad houdt hier toezicht op.

5.4 Het Directieteam

- De directie stelt het informatiebeveiligingsplan vast, eens per 2 jaar.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp-specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoording valt.
- De directeur met de portefeuille bedrijfsvoering is bovendien verantwoordelijk voor het waarborgen van het incidentmanagementprocedure.

5.5 Teammanagers (proceseigenaren)

- De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij zorg dragen.
- Teammanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- Beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico afwegingen te kunnen maken.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk om de basis op orde te krijgen voor de gemeente en het behalen van de doelen die gesteld zijn door het College van B&W[7].

5.6 Concerncontroller & CISO

- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C cyclus.
- De Concerncontroller bewaakt het algemeen belang van de gemeente ten aanzien van informatiebeveiliging.
- Tijdens P&C cyclus dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van

[7] Vertrekpunt hierin is: de ‘basis op orde’; weten waar we als organisatie staan en naartoe werken. Let op, dit is een continue proces.

de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.

6. Rapportagemomenten voor informatiebeveiliging

6.1 Verantwoordingstraject ENSIA

De gemeente Hoeksche Waard verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator[8] wordt aangewezen, deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teammanagers/proceseigenaren. Deze leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Ook is er een aansluitbeleid die jaarlijks geëvalueerd wordt door de CISO.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de Collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het College van B&W aan dat men op de hoogte is van de actuele stand van zaken m.b.t. de ENSIA onderdelen. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen.

De betrokkenheid van het College van B&W is essentieel, en laat zien dat de gemeente Hoeksche Waard informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Tot slot beantwoordt de gemeente Hoeksche Waard algemene vragen ten aanzien van de ENSIA[9]die ontsloten worden op www.waarstaatjegemeente.nl (een platform van de VNG).

6.2 Periodieke toetsing

De CISO is verantwoordelijk om het directieteam twee maal per jaar te verzien van een incidentenrapportage en/of een stand ten opzichte van de BIO normeringen. Door dit te doen wordt het directieteam periodiek op de hoogte gesteld van uitdagingen en aandachtspunten op het gebied van informatiebeveiliging. Deze kunnen incidenteel of structureel van aard zijn.

Het directieteam bepaald of deze informatie gedeeld dient te worden met de betreffende Portefeuillehouder(s) of het gehele College B & W. De concerncontroller en CISO adviseren en faciliteren hierin.

[8] ENSIA-coördinator: Voor de gemeente Hoeksche Waard, de CISO;
[9] Ontsluiting informatie ENSIA op waarstaatjegemeente.nl;
https://www.waarstaatjegemeente.nl/dashboard/dashboard/zoekresultaat/?search=Informatie informatieveiligheid en privacy.