GEMEENTE HEUSDEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Heusden

Nr. 41817

25 januari 2024

Beleid informatiebeveiliging en privacy 2024-2028 Gemeente Heusden

Het college van Heusden heeft in de vergadering van 16 januari 2024

besloten:

- het 'Beleid informatiebeveiliging en privacy 2024- 2028 Gemeente Heusden' vast te stellen;
- het 'Informatiebeveiligingsbeleid 2019-2021' en 'Privacybeleid 2018' van de gemeente Heusden tegelijkertijd in te trekken.

namens het college van Heusden,

de secretaris,
mr. H.J.M. Timmermans

1 Inleiding

1.1 Het belang van informatiebeveiliging en privacy

Informatie, waaronder persoonsgegevens, is een van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, transparant en proactief verantwoording aflegt en met minimale middelen maximale resultaten behaalt.

"Inwoners, ondernemers en overheidspartners moeten te allen tijde kunnen vertrouwen op een betrouwbare gemeentelijke informatievoorziening en zorgvuldig beheer van (hun persoons) gegevens. Daarom beschouwt het college adequate informatieveiligheid en borging van privacy als van essentieel belang, vooral in een tijd van digitalisering en ketenafhankelijkheid."

[1]

Dit behoort standaard onderdeel te zijn van alle dienstverlenings- en bedrijfsvoeringsprocessen. Het is niet alleen weten welke informatierisico's de continuïteit en de kwaliteit van de dienstverlening kunnen bedreigen. Het is ook weten wat de consequenties zijn als informatie niet beschikbaar of integer is, of door onbevoegden is in te zien of te wijzigen. Immers, onvoldoende informatiebeveiliging en onrechtmatige verwerkingen van persoonsgegevens kunnen leiden tot onacceptabele risico's. Voor het bedrijfsproces van de gemeente, maar ook voor de personen wiens persoonsgegevens worden verwerkt (ook wel betrokkenen genoemd).
Incidenten en inbreuken op deze processen kunnen bijvoorbeeld voor de gemeente leiden tot discontinuïteit, financiële schade en imagoverlies. Voor betrokkenen kan dit leiden tot risico's voor hun rechten en vrijheden en hun belemmeren in wie zij (willen) zijn.
Informatiebeveiliging en borgen van privacy is veel meer dan alleen het beveiligen van informatiesystemen. Het gaat ook om het gedrag van mensen in de organisatie, over de wijze waarop bestuur en management het voorbeeld geven en anticiperen op veiligheidsrisico's, en over het aantoonbaar maken dat de gemeente een betrouwbare ketenpartner is. Het daarbij rechtmatig verwerken van persoonsgegevens en het minimaliseren van risico's voor betrokkenen is vooral een organisatievraagstuk.

1.2 Doel van het beleid

Het beleid op informatiebeveiliging en privacy biedt ondersteuning aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

1.3 Reikwijdte van het beleid

Het beleid is van toepassing op:

1) Coalitieprogramma 2022-2026 " Heusden Nu en Straks": Heusden

- alle verwerkingen van (persoons)gegevens waar het college (verwerkings)verantwoordelijk en die vallen onder AVG (voor de verwerking van politiegegevens is een Beleid Wet politiegegevens opgesteld).
- alle onderdelen van de organisatie
- de (gegevensverwerkings)processen waar het college verantwoordelijk voor is en die zijn uitbesteed, ingekocht of op een andere manier zijn georganiseerd, zoals deelname in een rechtspersoon (bijvoorbeeld een gemeenschappelijke regeling)
- de gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden
- de gehele data-levenscyclus: van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag (zowel digitaal als analoog) tot en met de (eventueel) archivering en vernietiging ervan
- alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de gehele levenscyclus, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie
- de ICT systemen, maar ook op de fysieke beveiliging, proces automatiseringssystemen, personele processen en het informatiebeveiligingsbewustzijn van gebruikers

Dit beleid is hét overkoepelende beleid met een organisatiebrede werking. Dit beleid vormt de kapstok met als uitgangspunten de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO). Het is van toepassing op alle overige (deel)beveiligingsplannen die bijvoorbeeld opgesteld worden voor de basisregistraties BRP, BGT, BRO en de BAG, maar ook DigiD, Suwinet, Paspoorten en ID-bewijzen. De betreffende beveiligingsplannen staan echter op zichzelf en dat blijft zo omdat daarin de specifieke maatregelen, procedures, regelingen en bijlagen in zijn opgenomen.

1.4 Opzet van het beleid - kapstokmodel

Voor het beleid wordt het 'kapstokmodel' toegepast. Het college van B&W geeft middels voorliggend document richting door het stellen van uitgangspunten. Dit beleid vertaalt zich naar een plan dat door het MT wordt vastgesteld. Vanuit dit beleid en het tactisch plan worden waar nodig operationele plannen, acties en procedures opgesteld. Dat gebeurt onder verantwoordelijkheid van het lijnmanagement.

1.5 Geldigheid van het beleid

Het college van burgemeester en wethouders is eigenaar van dit beleidsdocument. Het beheer, opstellen en actueel houden van het beleidsdocument is de verantwoordelijkheid van de Chief information officer (CISO) en Privacy officer (PO) namens het management.
Dit beleid treedt in werking op de datum dat het is vastgesteld door het college van burgemeester en wethouders. Hiermee komen het tot dat moment van toepassing zijnde 'Informatiebeveiligingsbeleid 2019-2021' en 'Privacybeleid 2018' van de gemeente Heusden te vervallen.
Dit beleid is 5 jaar geldig en wordt minimaal één keer per jaar geëvalueerd onder leiding van de CISO en PO. Tussentijdse bijstelling is mogelijk als daarvoor aanleiding is. Aanpassing van het beleid kan plaatsvinden met het oog op:

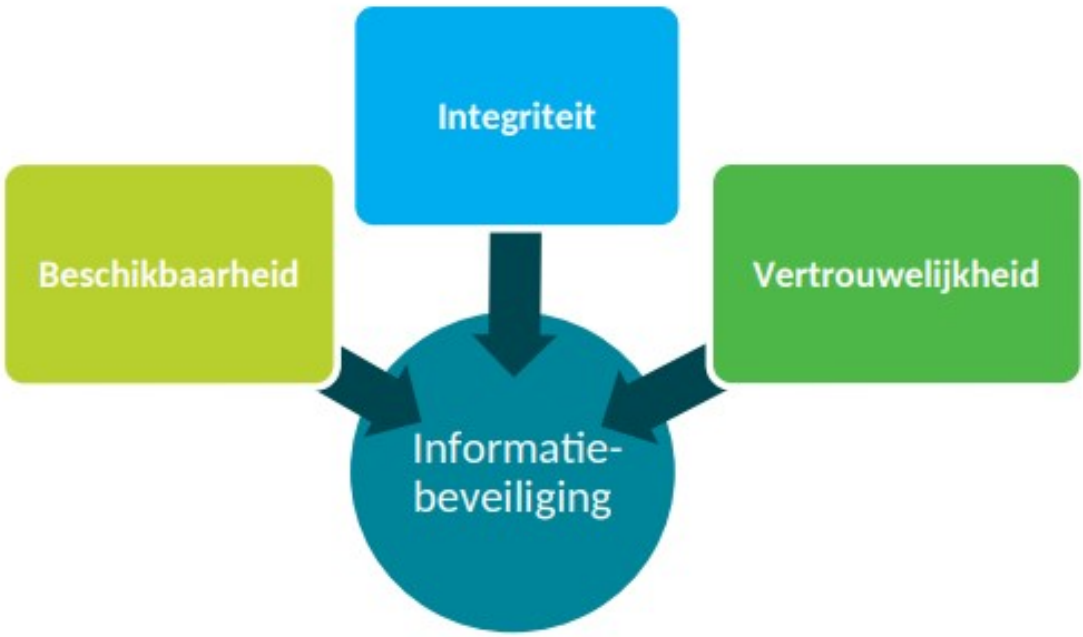
- de toereikende, de tactische en de operationele uitvoering ervan;
- de stand van de techniek (beveiliging en bedreiging);
- voortschrijdend inzicht;
- veranderende wet- en regelgeving of organisatie.

2 Informatiebeveiliging en privacy

2.0 Informatiebeveiliging en privacy
In dit hoofdstuk is uiteengezet wat het belang van informatiebeveiliging en privacy is. Als ook wat de visie en doelen zijn op dit gebied.

2.1 Wat is informatiebeveiliging
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen ter bevordering van de beveiliging wat omvat:

- **Beschikbaarheid**: Informatie dient beschikbaar te zijn op het moment dat het nodig is, wat eisen stelt aan de beschikbaarheid van informatiesystemen en databases.
- **Integriteit**: De gebruiker moet erop kunnen vertrouwen dat informatie juist, volledig, tijdig en geoorloofd is. Handhaving hiervan is verankerd in procesafspraken, maar ook in maatregelen die ongeoorloofde of ongewenste (expres of per ongeluk) mutaties tegengaan.
- **Vertrouwelijkheid**: Gebruikers en belanghebbenden moeten er op kunnen vertrouwen dat informatie alleen beschikbaar is voor die gebruikers die het nodig hebben voor de uitvoering van hun functie en niet onnodig ter inzage van anderen is.



2.2 Wat zijn privacy en gegevensbescherming
In een digitale samenleving is de bescherming van persoonsgegevens essentieel. Privacy en de bescherming van persoonsgegevens vormen een grondrecht. Privacy is een voorwaarde om vrij te zijn in wie je bent, wat je doet en om jezelf verder te ontwikkelen. Iedere persoon dient de controle te behouden over zijn eigen gegevens. Wat betekent dat deze persoon weet welke gegevens er van hem worden verzameld, wat daarmee gebeurt en hoe deze zijn beschermd. Elke betrokkene (de persoon wiens persoonsgegevens wij verwerken) mag erop rekenen dat wij zijn persoonsgegevens volgens de privacy wetgeving verwerken.
Dit betekent dat we ons houden aan de zes basisbeginselen uit de AVG waaraan elke verwerking van persoonsgegevens moet voldoen:

1. rechtmatig, behoorlijk en transparant;
2. doelbinding;
3. minimale gegevensverwerking;
4. juistheid;
5. opslagbeperking en;
6. integriteit en vertrouwelijkheid.

In het kader van het beginsel van de integriteit en vertrouwelijkheid, kent de AVG o.a. de verplichting dat passende technische en organisatorische beveiligingsmaatregelen moeten worden getroffen. Het

gaat daarbij om de effectiviteit van de beveiliging. Is deze niet op orde, dan kan privacy niet voldoende worden gegarandeerd.

2.3 Dreigingsbeeld
Data als ook de digitale veiligheid wordt steeds belangrijker. Dit heeft te maken met de informatiesamenleving waarin wij leven. We zijn meer online dan ooit. We werken digitaal, we winkelen digitaal, we volgen onderwijs digitaal en we ontmoeten elkaar steeds vaker digitaal. De snelle digitalisering die dit mogelijk maakt biedt ons veel kansen, maar het brengt ook risico's met zich mee. Want, doordat we zo digitaal zijn, zijn we er ook heel afhankelijk van geworden.

<u>De gemeente is afhankelijk van betrouwbare informatie(systemen)</u>
De gemeente is en wordt in steeds grotere mate afhankelijk van betrouwbare informatiesystemen en data. Door IT-ontwikkelingen ontstaan er kansen om de dienstverlening en bedrijfsvoering verder te innoveren, maar deze IT-ontwikkelingen maken de organisatie ook vatbaarder voor digitale dreigingen. Dit omdat er steeds meer gebruik wordt gemaakt van Cloud toepassingen en internet-of-things apparaten, maar ook omdat bijvoorbeeld remote werken een belangrijke plek heeft ingenomen.

<u>Digitale dreigingen nemen toe en de gemeente heeft belangen te beschermen</u>
Het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Autoriteit Persoonsgegevens (AP) en de Informatiebeveiligingsdienst voor gemeenten (IBD) constateren dat overheden steeds vaker het doelwit worden (en gaan worden) van digitale aanvallen. Ransomware aanvallen, digitale spionage, verstoring van de ICT, datalekken en diefstal van informatie nemen toe. Overheden hebben zogenaamde 'kroonjuwelen' (te beschermen belangen) die bewaakt moeten worden.. Denk hierbij aan bevolkingsdata, privacygevoelige informatie, (bovenregionale) beleidsstukken, informatie over bedrijfseconomische ontwikkelingen, aanbestedingsinformatie, vertrouwelijke bedrijfsgegevens, de IT-omgeving, onze medewerkers en hun kennis, etc.

<u>Cyberaanvallen op IT-leveranciers hebben impact</u>

De Autoriteit Persoonsgegevens geeft in haar datalekkenrapportage[2] aan dat het aantal meldingen van cyberaanvallen fors toeneemt. Zo'n 9% van de 21.151 gemelde datalekmeldingen omvat cyberaanvallen in 2022 (dit was nog 5% in 2020). Alleen al door de grootste drie cyberaanvallen bij ICT-leveranciers zijn van ongeveer 900.000 patiënten of cliënten medische persoonsgegevens gelekt. Ook de gemeente Heusden maakt in grote mate (en steeds meer) gebruik van IT-leveranciers.

<u>Dreigingsbeeld voor de gemeenten</u>
De Informatiebeveiligingsdienst voor gemeenten (IBD) geeft op basis van grondig onderzoek jaarlijks een dreigingsbeeld[3] uit, waarin de belangrijkste risico's staan voor gemeenten en waarover de gemeenten periodiek worden geïnformeerd. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.4 Doelen op het gebied van informatiebeveiliging en privacy
Elke overheidsorganisatie moet de Baseline Informatiebeveiliging Overheid (BIO) volgen als basis voor informatiebeveiliging en voldoen aan de eisen van de Algemene verordening gegevensbescherming (AVG) voor een rechtmatige, behoorlijke en zorgvuldige verwerking van persoonsgegevens.
Beide vereisen duidelijke technische en organisatorische beheersmaatregelen die moeten worden uitgevoerd. Door middel van dit beleid en uitwerking in concrete maatregelen wordt hier aantoonbaar aan voldaan.

Goede informatiebeveiliging vereist het handhaven van betrouwbare informatie(systemen) die beschikbaar, juist, volledig en actueel zijn, met de juiste beveiligingsniveaus. Dit zorgt voor veilig en verantwoord gegevensgebruik, voorkomt schade door verstoring of misbruik van informatie(systemen), en, indien nodig, zorgt voor herstel. De AVG verplicht deze beveiliging, met name bij persoonsgegevens, aangezien gegevensbescherming een essentieel onderdeel is van de privacywetgeving. Door het toepassen van de basisbeginselen op alle verwerkingen met persoonsgegevens, wordt privacy geborgd.

Met het continu werken aan onze informatiebeveiliging en privacyborging hebben wij tot doel:
- Het bijdragen aan de realisatie van de maatschappelijke opgave die wij als gemeente hebben en hierbij de risico's te beheersen (voor zowel de organisatie als de betrokkenen) die hierop een negatieve impact hebben.

2) Jaarrapportage meldplicht datalekken 2022 | Autoriteit Persoonsgegevens
3) Producten - Informatiebeveiligingsdienst

- Er een governance aanwezig is, die ervoor zorgt dat informatiebeveiliging geborgd is in beleid en processen en waarbij aansluitend de verantwoordelijkheden en rollen zijn belegd.
- Adequaat en proactief wordt geacteerd wanneer informatiebeveiligingsincidenten en/of datalekken zich voordoen.
- Er structureel wordt ingezet op het bewustzijn bij bestuur, management en medewerkers, zodat:
    - Men weet waarom het beleid van toepassing is
    - Men weet hoe zij het beleid moeten naleven.
    - Beleid wordt nageleefd.

2.5 Risicogebaseerde benadering

100% beveiliging van informatie bestaat niet. Dat maakt de organisatie gesloten en is niet realistisch. Het voldoende weerbaar zijn tegen dreigingen houdt de organisatie open en verbonden met de (veranderende) behoeften en wensen van de maatschappij. Dit betekent dat op bestuurlijk en management niveau keuzes gemaakt moeten worden welke risico's (voor de organisatie en/of betrokkenen) wel en welke risico's niet geaccepteerd worden. Voor de risico's die niet geaccepteerd worden, worden passende beheersmaatregelen getroffen die zich richten op het voorkomen van risico's of het adequaat herstellen van een incident dat zich heeft voorgedaan. Het proces van risicomanagement staat daarom centraal in dit beleid.

De centrale rol van risicomanagement in dit beleid leent zich eveneens goed voor het waarborgen van privacy. Want ook de AVG voorziet in en verplicht zelfs een risico gestuurde benadering. Het grootste verschil is dat het accepteren van risico's niet is toegestaan in zoverre dat een overtreding van de wet zou betekenen. Maar het risico voor betrokkene(n) is wel degelijk leidend in de soort en hoeveelheid maatregelen die een organisatie moet nemen, en zelfs welke verwerkingen van persoonsgegevens überhaupt zijn toegestaan.

2.6 Wet- en regelgeving

Naast onze doelen op het gebied van digitale weerbaarheid willen we voldoen aan geldende wet- en regelgeving. Voor het verwerken van persoonsgegevens gelden met name de volgende wettelijke kaders:

- Algemene verordening gegevensbescherming (Europees);
- Uitvoeringswet Algemene verordening gegevensbescherming (nationaal);
- Vakspecifieke wetgeving, zoals de Jeugdwet, Participatiewet en de Wmo (nationaal).

Daarnaast zijn onder andere ook de volgende wetten en normen relevant:

- De Baseline Informatiebeveiliging Overheid (BIO): beschrijft welke beheersmaatregelen wij verplicht zijn om te nemen om de informatie te beschermen
- De beveiligingsmaatregelen die het Rijk voorschrijft aan gemeenten inzake paspoorten en identiteitskaarten; Basisregistratie Adressen en gebouwen; DigiD; Basisregistratie Grootschalige Topografie; Suwinet; Basisregistratie Personen; Basisregistratie Ondergrond; en Wet politiegegevens (Wpg). Hierover legt het college jaarlijks ook verantwoording af aan de rijksoverheid en de gemeenteraad. Deze verantwoording gebeurt via ENSIA.
- De Archiefwet: voor de bewaartermijnen van (persoons)gegevens.
- De lijst van (verplichte) open standaarden van het Forum Standaardisatie. Dit beschrijft met welke standaarden wij moeten werken om bijvoorbeeld informatie veilig te versturen per e-mail, systemen te kunnen koppelen of informatie op onze website op de juiste wijze aan te bieden aan de bezoekers.
- De Wet open overheid (Woo): bepaalt onder welke voorwaarden persoonsgegevens openbaar gemaakt moeten worden ten behoeve van overheidstransparantie.

3 Heusdense principes en uitgangspunten

3.1 Heusdense principes

Dromen en doen: wij zijn de gemeente voor doeners met een droom. Als MogelijkMakers stellen we de klant centraal, gaan de dialoog aan, werken samen, spreken aan en nemen verantwoordelijkheid. Deze kernwaarden passen we intern en extern toe. De grenzen van de wet bepalen onze speelruimte, maar om dromen leidend te laten zijn worden mogelijkheden gezocht om initiatieven waar de maken. Hierbij worden soms de randen van het speelveld opgezocht.

Figuur 1 Heusdense kernwaarden

Naast onze **kernwaarden** als MogelijkMakers zijn er een aantal leidende principes die veel terugkomen in de organisatie:

- **Vertrouwen**: wij durven te vertrouwen op de goede intenties van de meeste mensen. Dit geldt zowel voor inwoners als voor collega's. Hoewel we uitgaan van vertrouwen wil dit niet zeggen dat we blind zijn voor minder goede intenties. Daarom zetten we in op slim vertrouwen: het uitgangspunt is vertrouwen, maar met analyses en/of gerichte controles zoeken we bevestiging dat dit uitgangspunt terecht en bruikbaar is;
- **Maximum gezond verstand, minimum bureaucratie**: wij doen een beroep op de eigen verantwoordelijkheid van iedereen. Dit krijgt de voorkeur boven het stellen van regels.

Bovenstaande is wie en wat we zijn als organisatie. Dit is dus ook van toepassing wanneer het gaat om informatiebeveiliging en privacy. Daarnaast hebben we te maken met wettelijke kaders en verantwoordingsplichten.

3.2 Heusdense uitgangspunten

De doorvertaling van bovenstaande Heusdense principes, wettelijke kaders en verantwoordingsplichten leidt tot de volgende uitgangspunten voor dit beleid:

1. Met onze informatiebeveiliging willen wij ervoor zorgen dat wij onze **maatschappelijke opgaves** realiseren, rekening houdend met geldende wet- en regelgeving.
2. Naleving van **de BIO en de AVG (en eventuele toekomstige relevante wet- en regelgeving)** vormt de basis voor onze informatiebeveiliging en rechtmatige verwerking van (persoons)gegevens.
3. Deze regelgeving is tevens leidend en bepalend voor de **leveranciers** en andere partners met wie wordt samengewerkt. Informatiebeveiliging en privacy worden ook meegenomen bij het opzetten en uitvoeren van **(keten)samenwerking**. Er worden afspraken gemaakt op het gebied van Informatiebeveiliging en privacy en op de naleving wordt toegezien.
4. Het inrichten van de informatievoorziening volgens dit beleid in opzet, bestaan en werking, geeft **afdoende garantie** voor onze informatiebeveiliging en het rechtmatig verwerken van persoonsgegevens.
5. Het **beveiligingsniveau is in lagen uitbreidbaar**. Dit betekent dat de basis uitgaat van de BIO en de AVG. Daar waar nodig of vereist, worden extra maatregelen getroffen boven op dit basisniveau. Een uitgevoerde risicoanalyse kan hiertoe aanleiding geven. Daarnaast kan wet- en regelgeving hier ons toe verplichten.
6. Dit beleid en deze beleidsregels worden uitgewerkt in een **tactisch plan** zodat de naleving van het beleid op tactisch en operationeel niveau is opgezet en wordt nageleefd.

7. Bij de start van **projecten**, het inrichten **processen** en het **inkopen** of **uitbesteden** van systemen wordt een risicoanalyse vroegtijdig uitgevoerd en expliciet een besluit genomen door de risico-eigenaar (lijn manager) op de beheersing van de gevonden risico's en de opvolging van het advies.
8. Het primaire uitgangspunt voor dit beleid is **risicomanagement**. Wij hanteren voor informatiebeveiliging de risicomanagementsystematiek volgens de BIO (een afgeleide van de NEN-ISO 27001 en 27002-normen). Hiervoor brengen wij continu risico's in beeld, treffen waar nodig passende beheersmaatregelen en monitoren wij of de beheersmaatregelen over de tijd heen nog steeds effectief en efficiënt werken.
9. Informatie wordt **geclassificeerd** om te bepalen welke beveiligingsmaatregelen nodig zijn. Hierbij is de aard van de informatie in de processen leidend. Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Op basis van een classificatie wordt bepaald hoe deze informatie behandeld dient te worden.
10. Het principe van '**Security and privacy by design and default**'[4] staat centraal. Dit betekent dat optimale privacy en Informatiebeveiliging wordt betracht en dat dit tevens wordt meegenomen bij de ontwikkeling en inrichting van informatiesystemen, processen en diensten.
11. Veilig omgaan met informatie is een **verantwoordelijkheid van alle medewerkers** in de hele organisatie. Verantwoord en bewust gedrag is essentieel. Structureel en planmatig wordt gewerkt aan het **bewustzijn**. Ook hierbij gaan wij uit van onze Heusdense principes.
12. Via de **P&C-cyclus** wordt horizontaal **verantwoording** afgelegd door het college van B&W aan de gemeenteraad. Er wordt gewerkt conform de plan-do-check-act verbetercyclus. De verticale verantwoording aan de verantwoordelijke stelselhouders leunt op de horizontale verantwoording en vindt plaats door middel van ENSIA. Voor implementatie en uitwerking van voorliggend beleid, wordt een doorvertaling gemaakt van dit beleid in een tactisch plan voor Informatiebeveiliging en privacy. Dat plan wordt waar nodig vertaald in vakspecifieke procedures en/of werkwijzen. Dit gebeurt in ieder geval voor het waarborgen van de eisen die voortvloeien uit de verschillende stelsels, zoals Suwinet, DigiD en de basisregistraties (waaronder BRP, BAG, BGT, BRO).
13. **Vakspecifiek(e) procedures, werkinstructies** en dergelijke ten aanzien van Informatiebeveiliging en privacy worden op het laagst mogelijke niveau vastgesteld door de verantwoordelijke. Indien het alleen betrekking heeft op één team, dan kan de lijnmanager dit op het laagste niveau vaststellen.
14. We gebruiken een **beveiligingsmodel**[5] waar de digitale identiteit als ook het digitale apparaat altijd eerst expliciet geverifieerd worden voordat het toegang krijgt tot onze data. Hierbij worden niet meer rechten verstrekt dan noodzakelijk (need-to-know) en gebruik gemaakt van tweefactorauthenticatie. Aansluitend wordt onze gehele IT-infrastructuur en onze data (ongeacht waar deze staat) passend beveiligd. Er vindt uitgebreide monitoring en logging plaats om digitale dreigingen vroegtijdig te signaleren en te herkennen.
15. Wij gaan er vanuit dat er een reële kans is te worden getroffen door een digitale dreiging. Wij zorgen ervoor hierop voorbereid te zijn om zo de impact te minimaliseren en snel te kunnen herstellen van een incident. Hiermee zo de afgesproken **bedrijfscontinuïteit** te garanderen.

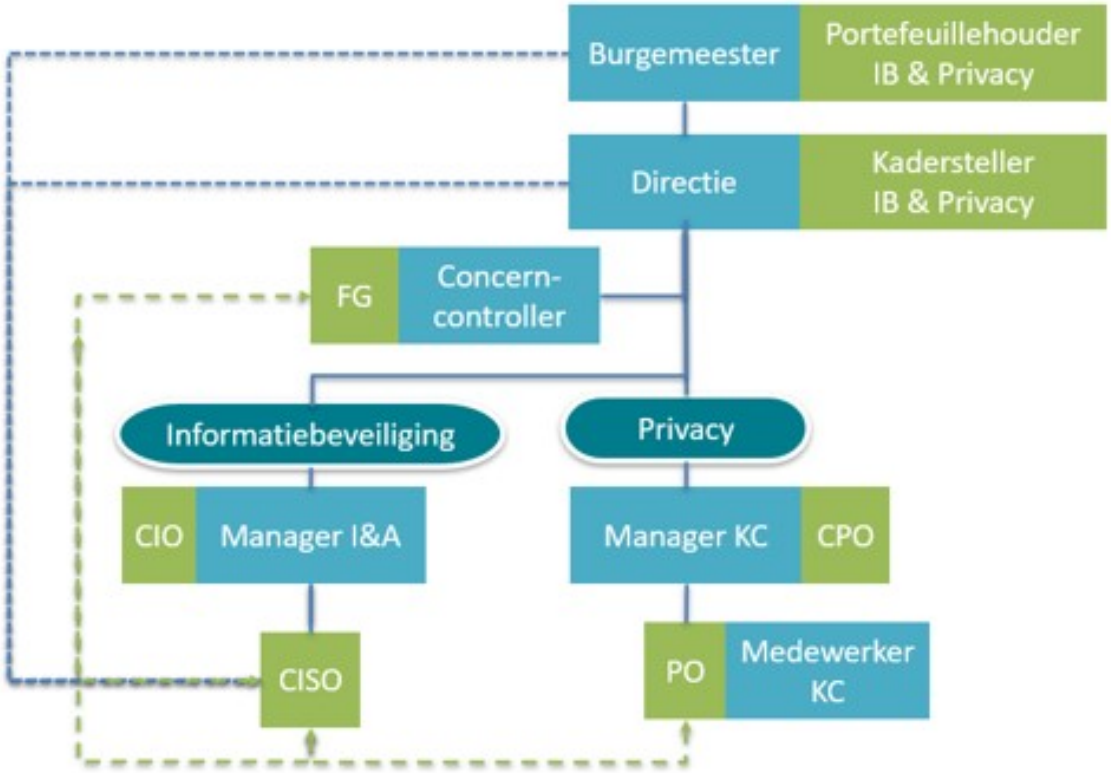
4 Organisatie van informatiebeveiliging en privacy waarborging

4.0 Organisatie van informatiebeveiliging en privacy waarborging

Door het inrichten van een informatiebeveiligings- en privacy organisatie zorgt de gemeente Heusden voor passende aandacht en sturing. Iedereen die werkt binnen de gemeentelijke organisatie heeft een verantwoordelijkheid. Op hoofdniveau wordt dit op vier niveaus ingericht. In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De CISO en PO ondersteunen, adviseren, coördineren en bewaken of dit beleid wordt nageleefd.

4) https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht#privacy-by-design-en-default

5) Uitleg beveiligingsmodel door Nationaal Cyber Security Centrum (NCSC).



Toewijzing	Verantwoordelijkheid	Taken en bevoegdheden
Het college van B&W	Bestuurlijk eindverantwoordelijk	1. Bepalen van de visie en richting (kaderstellend) 2. Randvoorwaarden voor invoering van het beleid. 3. Bestuurlijk eindverantwoordelijk voor Informatiebeveiliging en privacy
Gemeentesecretaris	Ambtelijk eindverantwoordelijk	1. Vaststellen gewenst niveau van beleid en richtlijnen en het I&P tactisch plan. 2. Herkennen en bewaken van de risico's. 3. Ambtelijk eindverantwoordelijk voor Informatiebeveiliging en privacy
FG	Toezichthoudend	Onafhankelijk toezicht houden op de naleving van de AVG-bepalingen binnen de organisatie.
CISO en PO	Ondersteunend, adviserend, coördinerend en controlerend	Adviseren over en overzicht houden op voortgang alsmede de effectiviteit van de invoering en ontwikkeling van beleid en richtlijnen.
CIO, CPO en lijnmanagement	Uitvoerend	Verantwoordelijk voor de uitvoering van dit beleid en richtlijnen binnen de eigen processen

College van B&W
Het college van B&W is bestuurlijk eindverantwoordelijk voor de Informatiebeveiliging en privacy van haar gemeente. Binnen het college van B&W zijn Informatiebeveiliging en privacy in een portefeuille belegd. Het college stelt het beleid voor Informatiebeveiliging en privacy vast en legt verantwoording af aan de gemeenteraad en stelselverantwoordelijken via de ENSIA[6].

Gemeentesecretaris
Is ambtelijk eindverantwoordelijk voor de Informatiebeveiliging en privacy van de organisatie.
Dit houdt in:

6) https://vng.nl/projecten/ensia

- Dat de eisen uit het beleid informatiebeveiliging en privacy zijn geïmplementeerd binnen de processen van de organisatie;
- Dat de benodigde capaciteit en middelen beschikbaar zijn voor de uitvoering van het beleid informatiebeveiliging en privacy;
- Dat het belang van doeltreffende informatiebeveiliging gecommuniceerd wordt naar de organisatie;
- Dat er passende informatiebeveiligingsdoelstellingen zijn voor de organisatie;
- Dat de organisatie deze informatiebeveiligingsdoelstellingen bewerkstelligt;
- Dat het beleid informatiebeveiliging en privacy continue verbetert.

Functionaris Gegevensbescherming (FG)
De positie en taken van de FG zijn wettelijk verankerd in de AVG (art. 37 en 38 AVG). In de basis betekent dit dat de FG onafhankelijk toezicht houdt op de naleving van de AVG door de gemeente. Daarnaast geeft de FG gevraagd en ongevraagd advies over onderwerpen en kwesties die de privacy rechten raken van inwoners of de medewerkers van de gemeente. De FG ziet tevens toe op de naleving van de AVG en bijbehorend gemeentebeleid.

Chief Information Security Officer (CISO)
De CISO coördineert, bewaakt en neemt deel aan de uitvoering van het managementproces rond informatiebeveiliging (PDCA-cyclus). De CISO ontwikkelt, in samenwerking met de uitvoerende organisatieonderdelen, operationele richtlijnen en procedures voor Informatiebeveiliging en continue verbetering. De CISO coördineert en bewaakt de uitvoering van het informatieveiligheidsbeleid en verhoogt en houdt het bewustzijn rond informatieveiligheid op peil door het opstellen en uitvoeren van een bewustwordingsplan. De CISO ondersteunt de organisatie met gevraagd en ongevraagd advies. De CISO kan opdracht geven om audits uit te voeren voor informatiebeveiliging. De CISO heeft een rechtstreekse rapportagelijn richting het college en de directie.

Privacy officer (PO)
De PO ondersteunt de organisatie bij de uitvoering en implementatie van de privacyregels. De PO coördineert de afhandeling van datalekken en AVG-privacyverzoeken. Tevens ondersteunt de PO de organisatie met het uitvoeren van DPIA's en geeft het (on)gevraagd advies op het gebied van privacy. Verder draagt de PO namens het management zorg voor de administratieve organisatie op het gebied van privacy (zoals het verwerkingsregister, datalekregister, benodigde procedures e.d.). Samen met de CISO houdt de privacy officer de bewustwording onder collega's op peil om te handelen volgens de AVG-principes en Informatiebeveiliging. De PO coördineert relevante audits, waaronder ENSIA en Wpg.

Chief Information Officer (CIO)
De organisatiebrede rol van CIO wordt ingevuld door de clustermanager Informatie en Automatisering. De CIO adviseert directie en bestuur over de strategie rond Informatiebeveiliging en zorgt voor de noodzakelijke middelen. De CIO is verantwoordelijk voor het functioneren van het managementproces rond informatieveiligheid (PDCA-cyclus). De CIO beoordeelt eventuele rest-risico's op het gebied van informatiebeveiliging na afstemming met de lijnmanager en beslist wanneer deze moeten worden voorgelegd aan de directie.

Chief Privacy Officer (CPO)
De organisatiebrede rol van CPO wordt ingevuld door de Clustermanager Kwaliteitscontrol. De CPO adviseert directie en bestuur over de strategie rond privacy en zorgt voor de noodzakelijke middelen. De CPO is verantwoordelijk voor het functioneren van het managementproces rond privacy (PDCA-cyclus). De CPO beoordeelt eventuele rest-risico's op het gebied van privacy na afstemming met de lijnmanager en beslist wanneer deze moeten worden voorgelegd aan de directie.

Het lijnmanagement
De lijnmanager is als proces- en risico-eigenaar verantwoordelijk voor Informatiebeveiliging en borging van privacy binnen zijn/haar organisatieonderdeel (afdelingen, opgave of programma).
De verantwoordelijkheden als eigenaar behelzen onder andere:
- Risico's identificeren en indien nodig te mitigeren;
- Eventuele restrisico's voorleggen aan CPO en/of CIO
- Bekend zijn met het beleid voor informatiebeveiliging en privacy en deze specifiek implementeren binnen de afdeling;
- De medewerkers van de afdeling in staat stellen het beleid uit te voeren door duidelijke instructies en het laten volgen van bewustzijnstrainingen;
- De medewerkers van de afdeling in staat stellen om afwijkingen op het beleid en incidenten te kunnen identificeren en melden;
- Zorgdragen dat informatiebeveiliging en privacy zijn geborgd bij de inkoop van diensten en producten;

- Zorgdragen dat verbeteringen worden doorgevoerd waar afwijkingen zijn geconstateerd;
- Betrokken zijn bij of verzorgen van de training en begeleiding van de medewerkers op het gebied van het informatiesysteem/de applicatie;
- Beheren en onderhouden van de bij het informatiesysteem/de applicatie behorende gebruikers-documentatie.

De medewerkers
Alle medewerkers (inclusief inhuur, uitzendkrachten, stagiaires etc.) van de gemeente zijn zich bewust van het beleid en de onderliggende richtlijnen en procedures en handelen daarnaar. Hierin worden zij gestuurd door hun leidinggevenden en geadviseerd door de PO en CISO (team I&P). Bij (noodzakelijke) registratie van tot personen herleidbare gegevens moet worden voldaan aan de AVG.

4.1 Rapportagestructuren
De CISO en FG rapporteren en geven gevraagd en ongevraagd advies aan de directie en (de portefeuille-houder van) het college van B&W. Het college is het hoogste besluitvormend gremium voor Informatiebeveiliging en privacy.

De rapportage over Informatiebeveiliging volgt het stramien van de P&C cyclus.

Rapportage Informatiebeveiliging & Privacy	Toelichting
Paragraaf bedrijfsvoering in de jaarrekening	Verantwoording (voorbereid door de CISO of PO) van het college van B&W aan de gemeenteraad
Jaarverslag FG	Jaarverslag van de FG aan het College van B&W
Incidentele rapportages, afhankelijk van actualiteit (over voortgang, risico's, beoordelingen e.d.)	Van de CISO of FG aan de gemeentesecretaris en de portefeuillehouder
ENSIA-rapportage	Verantwoording aan toezichthouders: RvIG: informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO) BKWI: Informatiebeveiliging Suwinet (BIO) Logius: Informatiebeveiliging DigiD DGBRW: Datakwaliteit en -integriteit BAG, BGT, BRO Verantwoording aan gemeenteraad via jaarverslag.

5 Naleving en evaluatie

5.0 Naleving en evaluatie
Beheersmaatregelen worden getroffen om risico's te verminderen. Om de controle over de risico's te waarborgen is het noodzakelijk regelmatig na te gaan of maatregelen nog werken en nog steeds de beoogde veiligheid bieden.

De gemeente Heusden controleert periodiek de maatregelen die voortkomen uit dit beleid door controles vanuit de Administratieve organisatie en interne controle (AO/IC), ENSIA, interne assessments en externe audits ten aanzien van (kosten)effectiviteit, privacy en informatiebeveiliging.
Periodiek wordt gerapporteerd over informatiebeveiliging en privacy (risico's, effectiviteit getroffen maatregelen, voortgang te treffen maatregelen e.d.).

Op basis van o.a.:
- incidenten, datalekken en beveiligingsissues
- interne en externe audits/ controles/ pentesten
- leveranciersbeoordelingen;
- uitgevoerde risicoanalyses;
- (kwetsbaarheids)meldingen;

worden waar nodig corrigerende en/of preventieve maatregelen doorgevoerd. Maatregelen worden geselecteerd met het doel dat de kans op herhaling wordt geminimaliseerd. Of waardoor de doeltreffendheid van het managementsysteem wordt verbeterd en het geleverde product of dienst beter aansluit op de eisen van de burger, bedrijven en partners.
Een werknemer van de gemeente Heusden gaat zorgvuldig en functioneel om met privacy- en organisatiegegevens. Niet naleven van dit beleid voor informatiebeveiliging en privacy kan daarom ook disciplinaire maatregelen tot gevolg hebben. Zoals aangegeven in het personeelshandboek van de gemeente Heusden.

namens het college van Heusden,
de secretaris,
mr. H.J.M. Timmermans

Bijlage 1 Afkortingen en toelichting

AVG	De afkorting AVG staat voor **Algemene Verordening Gegevensbescherming**. Dit is dé privacywetgeving, die sinds mei 2018 in de hele Europese Unie (EU) geldt. Goed om te weten: de AVG is ook bekend onder de Engelse naam: General Data Protection Regulation (GDPR).
BIO	Per 1 januari 2020 is de **Baseline Informatiebeveiliging Overheid** (BIO) van kracht. BIO is het normenkader voor informatiebeveiliging binnen de gehele overheid, op basis van actuele ISO-normatiek. Voorheen hadden de verschillende bestuurslagen (gemeenten, rijk, waterschappen en provincies) elk hun eigen baseline. Voor gemeenten was dat de BIG: Baseline Informatiebeveiliging Gemeenten.
BRP	De **Basisregistratie Personen** (BRP) is een databank met persoonsgegevens van personen die in Nederland wonen of gewoond hebben. Het gaat om gegevens als naam, burgerservicenummer (BSN), geslacht, geboortedatum, geboorteplaats en adres.
BGT	BGT staat voor **Basisregistratie Grootschalige Topografie**. Het is de digitale kaart van Nederland. Hierop ziet u onder andere percelen, water, groen, gebouwen en wegen.
BRO	De **Basisregistratie Ondergrond** (BRO) bevat gegevens over geologische en bodemkundige opbouw van de Nederlandse ondergrond.
BAG	De **Basisregistratie Adressen en Gebouwen** (BAG) bevat gegevens van alle adressen en gebouwen in Nederland. Het Kadaster beheert de BAG en stelt de gegevens op verschillende manieren beschikbaar, waaronder de BAG Viewer.
DigiD	DigiD is een afkorting van **Digitale Identiteit** en is een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren, een soort digitaal paspoort voor overheidsinstanties.
Suwinet	De **Gemeenschappelijke elektronische Voorziening Suwi** (GeVS, ook wel Suwinet genoemd) is een elektronische infrastructuur die is ontwikkeld om ervoor te zorgen dat de Suwi-ketenpartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.
ENSIA	ENSIA (**Eenduidige Normatiek Single Information Audit**) is ontstaan vanuit een gezamenlijk initiatief van gemeenten en de ministeries van BZK en SZW. Het doel van ENSIA is om tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te komen, gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). ENSIA structureert verantwoording over de BRP, DigiD, BAG, BGT, BRO en Suwinet.
PDCA-cyclus	De PDCA-cyclus (**Plan-Do-Check-Act**) is een methode waarmee je stap voor stap je werk, prestaties en organisatie beter kunt maken om zo continu te verbeteren.
ISO-normen	De Baseline Informatiebeveiliging Overheid (**BIO**) is geheel gestructureerd volgens **NEN-ISO/IEC 27001:2017** en NEN-ISO/IEC 27002:2017. De BIO beschrijft de invulling van deze normen voor de overheid, maar vervangt deze niet.