Gemeente Helmond

Strategisch informatiebeveiligingsbeleid

Gemeente Helmond 2020 – 2024

Aan:	College B&W, Directie Team Bedrijfsvoering
Auteur:	D. Edelaar
Datum:	december 2019
Status:	definitief
Afschrift:	CIO office, DSPO's, Kernteam

Inhoudsopgave

1 Ambitie Informatieveiligheid

Gemeente Helmond ambieert een duurzame, sociale en economisch vitale toekomst. Om dit te realiseren zijn er diverse programma's geformuleerd vanuit de strategische agenda 2019-2025. Het profiel en de ambitie van de gemeente is bepalend voor de informatievoorziening en hiermee bepalend voor de informatieveiligheid. Bij de thema's Sociale Stad, Toekomstgericht Werken en Omgevingswet is de borging van informatieveiligheid van belang. Om de ambitie zoals opgenomen in de strategische agenda waar te maken is een solide inrichting van informatiebeveiliging noodzakelijk. Het bestuur maakt hierbij op basis van risicomanagement bewuste keuzes om informatieveiligheid te borgen en om kwetsbaarheden in de bedrijfsvoering te minimaliseren. Veiligheids- en imagorisico's voor de organisatie en het bestuur - zoals afpersing, diefstal van persoon- en bedrijfsgegevens, uitval van ICT-diensten- worden hiermee verkleind.

Een solide inrichting van informatiebeveiliging aan de voorkant voorkomt gedoe achteraf. Om deze solide inrichting te bereiken, is het noodzakelijk om op het gebied van informatieveiligheid te professionaliseren. Het huidige volwassenheidsniveau van informatiebeveiliging van gemeente Helmond[1] ligt tussen niveau 1 en 2. De ambitie is om in 2024 volwassenheidsniveau 4 te bereiken. Zodra dat niveau bereikt is, heeft de organisatie informatieveiligheid geborgd binnen haar processen. Zij voldoet aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda.

Noodzakelijke randvoorwaarde om deze groei te bereiken, is de beschikbaarheid van kwalitatieve en kwantitatieve resources op de afdelingen. Met de inrichting van een decentrale Informatieveiligheid en privacy organisatie die vanaf juli 2019 is gestart, is een significante, eerste stap gezet. Met deze inrichting groeit de gemeente vanuit organisatieonderdelen en kan integraal worden gewerkt aan het verbeteren van de informatieveiligheid en privacy.

Dit strategische informatiebeveiligingsbeleid 2020-2024 is het kader om gemeentelijke informatie te beschermen en draagt bij aan een verdere professionalisering van informatiebeveiliging.

[1] Resultaten meting2018: geclassificeerd conform het volwassenheidsmodel NBA-LIO/NOREA

2 Inleiding

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie én vertrouwelijke omgang met informatie is essentieel voor een gemeente omdat het de basis is voor juist en efficiënt handelen. Gemeente Helmond heeft haar ambities vastgelegd in de strategische agenda en dient hierbij transparant te zijn richting haar inwoners en proactief verantwoording af te leggen aan interne en externe toezichthouders. Dit strategische informatiebeveiligingsbeleid is het kader voor informatiebeveiliging.

2.1 Doel van dit beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Dit beleid geldt voor de jaren 2020 tot en met 2024 en vervangt het "Informatiebeveiligingsbeleid gemeente Helmond 2015-2019". Het is het bestuurlijk kader om de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens en andere informatie(systemen) te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving. Dit strategische informatiebeveiligingsbeleid is gericht op het :

- Verstevigen van de governance
  De verantwoordelijkheid voor informatieveiligheid is primair in de lijn belegd. Dit betekent een centrale rol voor afdelingsmanagers.
- Risico gebaseerd sturen
  Dit betekent dat het management verantwoordelijk is voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.
- Integratie in de planning- en control cyclus
  Dit betekent dat informatieveiligheid dient te worden opgenomen in de integrale P&C-cyclus. Implementatie en verantwoording vindt plaats via de planning zoals opgenomen in de bedrijfsvoering kalender. Er vindt een uniforme verantwoording plaats aan interne en externe toezichthouders.

Dit beleid draagt bij aan een verdere professionalisering van informatieveiligheid en hiermee aan het behalen van de gestelde doelen in de strategische agenda.

2.2 Scope van het strategische informatiebeveiligingsbeleid

Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het heeft betrekking op het politiek bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.
Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen.

3 Beleidskader Informatieveiligheid

3.1 Plaats van dit beleid

Het strategisch informatiebeveiligingsbeleid is in lijn met de relevante landelijke en Europese wet- en regelgeving. Het strategisch informatiebeveiligingsbeleid is een onderdeel van het informatiebeleid en bestaat uit de volgende documenten:

1. strategische informatiebeveiligingsbeleid
2. tactische informatiebeveiligingsbeleid
3. specifieke beleidskaders
4. informatiebeveiligingsbeleidsplan(nen)

In het tactische beleid staan onderwerp-specifieke beleidsregels die de implementatie van informatiebeveiliging verplicht stelt. De uitwerking van het strategische en het tactische beleid staat opgenomen in het informatiebeveiligingsplan. Dit plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

Voor bepaalde kerntaken gelden op grond van wet-en regelgeving specifieke (aanvullende) beveiligingseisen[2]. Hiervoor gelden specifieke beleidskaders en/of informatiebeveiligingsplannen. Het onderwerp privacy is in een apart beleid[3] opgenomen.

3.2 Grondslagen

Dit strategische informatiebeveiligingsbeleid is gebaseerd op:

- NEN-ISO/IEC 27001:2017
- NEN-ISO/IEC 27002:2017
- Baseline Informatiebeveiliging Overheid (BIO)[4] en de 10 principes voor informatiebeveiliging (zie hoofdstuk 4).
- De architectuurprincipes van de gemeente (zie paragraaf 3.3)

3.3 Architectuurprincipes

Architectuurprincipes zijn richtinggevend en helpen gemeenten om bewust keuzes te maken bij het inrichten van de gemeentelijke processen, bijhorende informatievoorziening en zijn de basis om informatiebeveiliging te implementeren.
De gemeente Helmond volgt hierbij landelijke richtlijnen. [5]
De acht GEMMA basisprincipes zijn:

1 Onze gemeente denkt vanuit de positie van de klant.
2 Onze gemeente gebruikt generieke processen en functies.
3 Onze gemeente voert regie over uitbestede diensten.
4 Onze gemeente biedt de klant een goede informatiepositie.
5 Onze gemeente digitaliseert haar diensten en processen.
6 Onze gemeente stelt openbare gegevens als open data beschikbaar.
7 Onze gemeente hergebruikt gegevens.
8 Onze gemeente gaat op een vertrouwde manier met gegevens om.

Deze architectuurprincipes zijn nader uitgewerkt in de informatiearchitectuur[6].

[2] zoals BRP, PNIK, DigiD, SUWI, BAG, BGT, BRO, AVG, Privacy beleid
[3] https://zoek.officielebekendmakingen.nl/gmb-2018-168572.html
[4] uitgebracht door de interbestuurlijke werkgroep Normatiek in 2018
[5] Nederlandse Overheid Referentie Architectuur (NORA) en de daarvan afgeleide Gemeentelijke Model Architectuur (GEMMA).
[6] file:///C:/Users/doriniee/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/brochure%20Informatiearchitectuur%20(1).pdf

3.4 Uitgangspunten

De belangrijkste uitgangspunten van dit informatiebeveiligingsbeleid zijn:

1. Dit beleid vormt samen met het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan het kader om informatieveiligheid in de organisatie te borgen.
2. Informatiebeveiliging mag niet ten koste gaan van de veiligheid van personen.
3. Het bestuur, de directie en de (afdelings)managers dragen dit beleid uit en sturen op de implementatie van dit beleid.
4. Informatiebeveiliging is georganiseerd. Het management heeft continu aandacht voor het vergroten van het bewustzijn van medewerkers om zo de menselijke schakel te versterken.
5. De rol van de coördinator van informatiebeveiliging (Chief Information Security Officer: CISO), is ingevuld.
6. Regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid zijn vastgesteld.
7. Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én de coördinatie op dit proces is informatieveiligheid binnen de organisatie verankerd.
8. Informatiebeveiliging is een onderdeel van risicomanagement.

3.5 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. Medewerkers kennen de beveiligingsprocedures en gebruiken deze procedures. Medewerkers zijn daarnaast op de hoogte van eisen die vanuit wet- en regelgeving aan hun bedrijfsprocessen gesteld worden en kennen deze kaders.
3. Medewerkers gaan verantwoord 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.
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 Smart City, kunstmatige intelligentie (AI).

Zolang deze uitgangspunten en randvoorwaarden niet zijn ingericht is de informatieveiligheid niet voldoende geborgd.

4 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van dit informatiebeveiligings-beleid zijn hieronder beschreven.

4.1 Een nieuwe baseline voor informatieveiligheid

De Baseline Informatiebeveiliging Overheid (BIO) is vanaf 2020 het nieuwe normenkader voor de gehele overheid. Deze baseline is ten opzichte van de Baseline Informatiebeveiliging Gemeenten (BIG) meer gericht op risicomanagement. De bestuurders en de (afdelings)managers hebben een prominente rol met betrekking tot informatiebeveiliging en met de komst van de BIO een cruciale rol met betrekking tot risicomanagement. Hierbij maakt het bestuur en het management op voorhand keuzes en continu afwegingen of informatie in bestaande en nieuwe processen adequate beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

De BIO helpt het management bij het nemen van haar verantwoordelijkheid ten aanzien van informatiebeveiliging. In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus gedefinieerd met bijbehorende verplicht in te richten beveiligingsmaatregelen. Het management bepaalt op basis van een risicoafweging, hoe aan deze beveiligingsmaatregelen kan worden voldaan. Waar naleving (nog) niet volledig mogelijk is, maakt het management de aanwezige risico's inzichtelijk aan hun stakeholders.

Het management legt verantwoording af over de risicoafweging en over de effectieve invulling van de beheersmaatregelen. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over informatiebeveiliging[7]. De BIO biedt hiermee de basis om te zorgen dat informatiebeveiliging geïmplementeerd en geborgd wordt.

4.2 Handvatten voor de rol van de bestuurder

VNG heeft aan het gemeentelijk bestuur de 10 principes van informatiebeveiliging[8] uitgereikt. Deze principes bieden het bestuur handvatten op welke wijze het zijn rol kan invullen bij het borgen van informatiebeveiliging in de gemeentelijke organisatie Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers.

De 10 principes zijn:

1 Bestuurders bevorderen een veilige cultuur;
2 Informatiebeveiliging is van iedereen;
3 Informatiebeveiliging is risicomanagement;
4 Risicomanagement is onderdeel van de besluitvorming;
5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6 Informatiebeveiliging is een proces;
7 Informatiebeveiliging kost geld;
8 Onzekerheid dient te worden ingecalculeerd;
9 Verbetering komt voort uit leren en ervaring;
10 Het bestuur controleert en evalueert.

Deze 10 principes staan nader uitgewerkt in de uitgewerkte rolverdeling van hoofdstuk 6 en in het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

[7] Zie hoofdstuk 8

[8] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf

5 Communicatie en evaluatie van dit beleid

Na vaststelling van dit beleid door het college wordt dit beleid gepubliceerd en via het lijnmanagement gecommuniceerd met medewerkers en relevante externe partijen. Verdere communicatie momenten zijn uitgewerkt in het informatiebeveiligingsplan.

Het strategische informatiebeveiligingsbeleid geldt voor een periode van 5 jaar en wordt met een frequentie van 5 jaar geëvalueerd of eerder bij belangrijke wijzigingen.

6 Organiseren van informatiebeveiliging

De wijze waarop het informatiebeveiligingsbeleid binnen de gemeente is verankerd, vormt het kader van de borging op informatiebeveiliging. Het vaststellen van een beheerkader is van belang om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te borgen.

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit beleid. De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten. Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. Hieronder is toegelicht welke rollen, taken en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn belegd in de organisatie. Overige specifieke rollen behoren te worden uitgewerkt in een bijlage behorende bij de operationele informatiebeveiligingsplannen.

6.1 Gemeenteraad

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

6.2 College van Burgemeesters en Wethouders

Het College van Burgemeester en Wethouders is integraal (politiek) verantwoordelijk voor de borging van informatieveiligheid binnen de gemeente. Zij stelt kaders op voor informatieveiligheid (dit strategische beleid). Bij het onderwerp waardedocumenten is bij wet bepaald dat de bevoegdheid voor het vaststellen van kaders bij de burgemeester ligt in plaats van bij het college. De ambtelijke verantwoordelijkheid op het gebied van informatiebeveiliging is door het college gemandateerd aan de gemeentesecretaris.

Zowel het college van Burgemeester en Wethouders als de Raad (controle functie) kunnen opdracht geven om controle te laten uitvoeren. Het college legt verantwoording af aan de Raad en aan externe toezichthouders. Het college is verantwoordelijk voor de financiën van de gemeente.

6.3 De directie

De directie is ambtelijk verantwoordelijk voor kaderstelling en sturing op tactisch niveau. De directie stuurt hierbij op concernrisico's. De gemeentesecretaris draagt de gemandateerde verantwoordelijkheid voor informatieveiligheid en privacy.

De directie:

- zorgt voor voldoende resources om informatiebeveiliging in de organisatie te borgen.
- adviseert het college van B&W over het vast te stellen strategische beleid.
- zorgt dat het tactische (specifieke) beleid, informatiebeveiligingsplan(nen) en procedures worden opgesteld en vastgesteld.
- draagt het informatiebeveiligingsbeleid uit aan de organisatie en stuurt op concern risico's.

- zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager (eigenaarschap) en ziet erop toe dat de afdelingsmanagers adequate maatregelen nemen.
- zorgt dat de afdelingsmanagers zich verantwoorden over de stand van zaken van informatieveiligheid binnen hun bedrijfsprocessen en rapporteert periodiek over de status zodat het college hierop kan sturen. Spreekt afdelingsmanager aan op naleving van dit beleid ook als verbetermaatregelen niet tijdig worden doorgevoerd.
- controleert of de getroffen maatregelen overeenstemmen met de gestelde eisen en of deze voldoende bescherming bieden.
- informeert de eindverantwoordelijke portefeuillehouder(s) binnen het College gevraagd en ongevraagd over informatiebeveiliging.
- ziet erop toe dat informatiebeveiligingsonderwerpen n.a.v. de rapportage van de CISO onderdeel zijn van de Planning & Control gesprekken en dat risicovolle onderwerpen worden opgenomen in de auditplannen.
- evalueert periodiek het informatiebeveiligingsbeleid. Voor het strategische beleid geldt een periode van 5 jaar of bij belangrijke wijzigingen.

6.4 Afdelingsmanagers (proceseigenaren)

De afdelingsmanagers (proceseigenaren) zijn operationeel eindverantwoordelijk voor de bedrijfsprocessen. De proceseigenaren zijn hiermee eigenaar van de applicaties binnen dit bedrijfsproces. Daar waar applicaties worden gebruikt in meerdere bedrijfsprocessen geldt dat het bedrijfsproces met het hoogst noodzakelijke beveiligingsniveau leidend is. De afdelingsmanagers kunnen hun verantwoordelijkheid niet delegeren, uitvoerende werkzaamheden wel. De afdelingsmanagers zorgen dat de inrichting van informatiebeveiliging en privacy voldoet aan de vereiste wet- en regelgeving. Hierbij worden zij ondersteund door de Decentrale Security en Privacy Officer (DSPO), de CISO en de Functionaris Gegevensbescherming (FG). Afdelingsmanagers rapporteren over de door hun tactisch- en operationeel uitgevoerde activiteiten aan de directie en bestuur[9].

De afdelingsmanagers:

- stellen specifiek beleid, specifieke informatiebeveiligingsplan(nen) en procedures, op en vast en dragen deze uit.
- sturen op beveiligingsbewustzijn, bedrijfscontinuïteit, privacy en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- bespreken beveiligingsincidenten en de consequenties die dit heeft voor beleid en te implementeren beheersmaatregelen
- stellen het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast.
- signaleren vroegtijdig de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- zorgen ervoor dat actuele risicoanalyse(s) worden uitgevoerd. implementeren de noodzakelijke informatiebeveiliging en privacy maatregelen. Deze beveiligingsmaatregelen bepalen zij op basis van risicomanagement en op basis van de kaders die eigen wet- en regelgeving met zich meebrengen.
- bewaken dat gekozen gegevensbeschermingsmaatregelen uit risicoanalyses worden opgenomen in doorontwikkelplannen. Stellen vast of de getroffen maatregelen aantoonbaar worden nageleefd. Rapporteren hierover in de managementrapportages aan de CISO, de directie en het bestuur. Leveren input voor wijzigingen op maatregelen en procedures.

[9] Zie hoofdstuk 8 Rapportagemomenten

- stemmen de inhoudelijke aanpak om informatiebeveiliging te borgen af in het bedrijfsvoeringsoverleg met de afdelingen en/of teams.
- leveren alle informatie aan die nodig is voor het invullen van de jaarlijkse verantwoordingstraject informatiebeveiliging (ENSIA).

Het management wordt hierbij ondersteund door de Decentrale Security en Privacy Officer.

6.5 Decentrale Security & Privacy Officer

De DSPO ondersteunt de afdelingsmanager bij het beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid en privacy voor zijn/ haar bedrijfsproces. De DSPO is het eerste aanspreekpunt voor de afdelingsmanager, de CISO en de FG en ambassadeur voor informatieveiligheid en privacy binnen dit bedrijfsproces.

De DSPO's zijn binnen de gemeente degenen die kaders stellen op het gebied van domein specifieke informatiebeveiliging en beveiligingsbewustzijn. De DSPO bevordert draagvlak bij het management en medewerkers. Tevens monitort de DSPO of de informatiebeveiliging conform de kaders uitgevoerd wordt. Hij is direct betrokken bij de implementatie hiervan in de lijn en kent de processen en relevante wetgeving. Hij zorgt daarmee dat de organisatie specifieke informatiebeveiliging doorvoert in haar processen, conform wet- en regelgeving.

Verder richt de DSPO zich op de uitvoer en naleving van de (domein specifieke) privacywetgeving. De DSPO stelt een data protection impact assessment (DPIA) op en adviseert bij het gebruik van persoonsgegevens. De DSPO toetst bij gegevensaanvragen op doelbinding, rechtmatigheid, proportionaliteit en andere aspecten vanuit de AVG en privacywetgeving. De DSPO rapporteert periodiek over de informatieveiligheid/ privacy aan de afdelingsmanager, CISO en FG.

6.6 Chief Information Officer

De CIO geeft binnen het directieteam op dagelijkse basis invulling aan de sturende rol door besluitvorming in het college van Burgemeester en Wethouders voor te bereiden en toe te zien op de uitvoering ervan. De informatiebeveiligingstaken die hieruit voortvloeien zijn belegd bij de CISO.

6.7 Chief Information Security Officer

De CISO ondersteunt vanuit een onafhankelijke positie de organisatie met betrekking tot het borgen van informatieveiligheid en heeft de mogelijkheid om rechtstreeks aan de directie en/of portefeuillehouder te rapporteren. De CISO is aangesteld volgens een vastgesteld CISO-functieprofiel.

De CISO is binnen de gemeente degene die kaders stelt op het gebied van informatiebeveiliging die voor de gehele organisatie gelden. De CISO stuurt de organisatie aan met betrekking tot informatiebeveiliging. Hiermee zorgt de CISO ervoor dat de organisatie informatiebeveiliging doorvoert in haar processen, conform wet- en regelgeving. Daarnaast creëert de CISO het draagvlak voor informatiebeveiliging binnen de organisatie. De rol van de CISO is vooral adviserend en coördinerend. De CISO stuurt de DSPO's functioneel aan. De CISO is in het kader van het verantwoordingstraject informatiebeveiliging tevens coördinator ENSIA.

Om aan bovenstaande te kunnen voldoen, heeft de CISO de volgende bevoegdheden:

- gevraagd en ongevraagd onderzoek kunnen doen en advies geven aan het college van B&W / Raad
- mogelijkheid tot direct ingrijpen zonder toestemming vooraf bij beveiligingsincidenten
- beschikt over budget en resources

De CISO is geplaatst binnen de afdeling Informatievoorziening en Automatisering-CIO. De CISO voert geen operationele taken uit. Hiermee is het risico geminimaliseerd dat de eigenlijke taken van de CISO blijven liggen en de onafhankelijke positie in het geding komt. Daarnaast heeft de CISO rechtstreekse toegang tot de portefeuillehouder van informatiebeveiliging.

6.8 Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op het gebied van privacy. De FG houdt toezicht op de wijze waarop de organisatie invulling geeft aan maatregelen om aan de privacywetgeving te voldoen. In het privacy-beleid staan de taken van de FG opgenomen.

6.9 IT Auditor

De IT auditor (concern control) is verantwoordelijk voor het opzetten, uitvoeren van risicoanalyses op het gebied van de naleving van informatiebeveiliging en privacy. De IT auditor initieert audits en toetst hierbij op de naleving van het informatiebeveiligingsbeleid.

Om de verantwoordelijkheden in het informatiebeveiligingsgebied te kunnen vervullen dienen de bovengenoemde rollen op het gebied van informatiebeveiliging competent te zijn en de mogelijkheid te hebben om de ontwikkelingen op het gebied van informatiebeveiliging bij te houden.

7 Communicatie stakeholders

7.1 Stakeholders

De gemeente Helmond onderhoudt contacten met relevante overheidsinstanties (zoals externe toezichthouders), speciale belangengroepen (zoals Informatie Beveiligingsdienst Gemeenten) en interne stakeholders. Een nadere toelichting over het contact met de IBD is opgenomen in paragraaf 7.2. Stakeholders worden periodiek op de hoogte gesteld over de stand van zaken rondom informatiebeveiliging. Het onderwerp informatiebeveiliging is een vast onderdeel op de agenda van bestuur en lijnmanagement met als doel om sturing te kunnen geven. In de onderstaande tabel bij paragraaf 7.3 is opgenomen wat de contactmomenten met stakeholders zijn.

7.2 Aansluiting Informatiebeveiligingsdienst Gemeenten

Eén van de doelen van de IBD[10] is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
Wij maken indien nodig gebruik van deze ondersteuning. De IBD informeert de gemeente via vastgestelde contactpersonen namelijk de algemeen contactpersoon informatiebeveiliging (ACIB)[11] en de vertrouwde Contactpersoon Informatiebeveiliging (VCIB)[12].

7.3 Contactmomenten stakeholders

Contactmoment	Deelnemers	Frequentie	Doel
opdrachtgever – opdrachtnemer overleg	bestuurlijk opdrachtgever, ambtelijk opdrachtgever, CIO, CISO, FG	per kwartaal	informeren opdrachtgever over proces

[10] De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING).
[11] Algemene waarschuwingen en informatie met een niet vertrouwelijk karakter
[12] Informatie die vertrouwelijk is van karakter

Contactmoment	Deelnemers	Frequentie	Doel
informatieveiligheid en privacy overleg	CISO, de DSPO en de FG	per kwartaal	afstemming en coördinatie van informatieveiligheid en privacy onderwerpen: De DSPO heeft vooraf afstemming met de proceseigenaar.
presentaties ENSIA verantwoording	proceseigenaren, DSPO, CISO en ambtelijk opdrachtgever	per jaar	In beeld brengen risico's in proces en stand van zaken implementatie informatiebeveiliging input voor bestuurlijke rapportage van CISO aan interne en externe toezichthouders, jaarverslag en Raadsinformatiebrief
ICT crisisoverleg	Gemeentesecretaris, CISO, DSPO, CIO, verantwoordelijke voor het domein waar de crisis betrekking op heeft Eventueel lid van het team communicatie, FG	per incident	grip op crisis input voor analyse en rapportage van incident

8 Rapportagemomenten informatiebeveiliging

Periodieke rapportages vloeien voort uit bovengenoemde contactmomenten met stakeholders. Rapportages worden opgesteld van incidenten, het verantwoordingstraject ENSIA en periodieke rapportages over de stand van zaken van de implementatie van informatiebeveiliging (P&C-cyclus). Aangezien het college en de Raad met name een rol spelen in het verantwoordingstraject wordt dit traject in onderstaande paragraaf toegelicht. In het informatiebeveiligingsplan is een detailplanning opgenomen van dit verantwoordingstraject.

8.1 Verantwoordingstraject ENSIA

Ter afsluiting van het jaarlijkse verantwoordingstraject [13] rapporteren de afdelingsmanagers over de risico's binnen hun bedrijfsprocessen en over de stand van zaken van de implementatie van informatiebeveiliging van het afgelopen jaar. De CISO coördineert dit proces en stelt jaarlijks vóór 1 mei aan de hand van de deelrapportages van de afdelingsmanagers een bestuurlijke rapportage op voor de ambtelijke en bestuurlijke opdrachtgever.

Het college van B&W legt met deze bestuurlijke rapportage, een raadsinformatiebrief én met een aparte paragraaf in het jaarverslag verantwoording af aan zijn interne toezichthouder de gemeenteraad én aan de externe toezichthouders (Rijk)[14]. Op deze wijze kan de ambtelijk en de bestuurlijk opdrachtgever en het college sturen op informatiebeveiliging. Zij kunnen hiermee besluiten nemen om informatiebeveiligingsrisico's tot een acceptabel niveau te brengen.

[13] Verantwoording vindt plaats via de landelijk voorgeschreven systematiek ENSIA (Eenduidige Normatiek Single Information Audit)

[14] In de bijlage behorende bij het informatiebeveiligingsplan staat de detailplanning, rolverdeling en benodigde capaciteit opgenomen.