

Strategie Informatiebeveiliging gemeente Heemstede 2020-2024

1. Inleiding

Deze nota beschrijft de strategie voor de informatiebeveiliging voor de jaren 2020 tot 2024 en vervangt het in 2017 vastgestelde 'Strategisch en Tactisch Gemeentebreed Informatieveiligheidsbeleid 2017'. Deze nota is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met deze strategie voor de informatiebeveiliging voor de jaren 2020 tot 2024 zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor deze strategie is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) zie bijlage A. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage B.

1.1 Wat is informatiebeveiliging?

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van processen, informatievoorzieningen en gegevens aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

De strategie voor informatiebeveiliging geldt voor alle processen 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 politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.2 Ambitie en visie van de gemeente op het gebied van informatieveiligheid

De gemeente Heemstede hecht grote waarde aan een goede dienstverlening voor haar burgers en bedrijven op alle diverse vlakken waar de gemeente verantwoordelijk voor is. Ook wil de gemeente een betrouwbare en transparante partij zijn naar haar burgers en bedrijven. Hiervoor is het noodzakelijk dat de informatie die wij verzamelen, bijhouden en verwerken en publiceren te allen tijde beschikbaar is, juist en actueel is (integer) en, indien van toepassing, alleen toegankelijk is voor degenen die toegang moeten hebben (vertrouwelijk). De gemeente wil meegaan met nieuwe ontwikkelingen en technologie om de dienstverbetering verder te verbeteren.

1.3 Leeswijzer

In hoofdstuk 2 wordt de kern van de strategie uiteengezet. Deze strategie wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door het managementteam) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de domeinmanagers, de Chief Information Security Officer (CISO), het dreigingsbeeld van de Informatiebeveiligingsdienst (IBD) en de uitkomsten van de jaarlijkse zelfaudit over informatiebeveiliging. In het plan staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in de strategie is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

2. Strategie

2.1 Doel

Het doel van deze nota is het presenteren van de 'Strategie Informatiebeveiliging voor de jaren 2020 tot 2024'. De uitwerking van deze strategie vindt plaats door het opstellen van onderwerp specifieke beleidsdocumenten op tactisch niveau. Daarnaast door het uitwerken naar concrete maatregelen in het jaarlijks bij te stellen informatiebeveiligingsplan.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomangement dan de oude BIG (Baseline Informatiebeveiliging Gemeenten). Dat wil zeggen dat de domeinmanagers nu meer dan vroeger moeten

werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging (zie bijlage B)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging heeft 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.

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 uitvoeren 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 partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 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 daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van 'best practices' bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek (bestaande uit vertegenwoordigers van VNG, IBD, waterschappen, provincies en het rijk) in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

De inhoud en structuur van deze nota zijn afgestemd op die van de ISO27002 en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

2.4 Plaats van strategisch Informatiebeveiliging

De strategie wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven Informatiebeveiligingsplan.

2.5 Scope informatiebeveiliging

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

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK) en de wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele

specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

Bewust wordt in de strategie geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar de strategie gelegd.

2.6 Uitgangspunten

Het bestuur, het managementteam en de onderliggende lijn spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). De strategie Informatiebeveiliging is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van Informatiebeveiliging zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming 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 van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van Burgemeester en Wethouders is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het managementteam en de onderliggende lijn. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Heemstede hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. De strategie Informatiebeveiliging vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke de strategie Informatiebeveiliging vast.
- Het managementteam stelt jaarlijks het informatiebeveiligingsplan vast.
- Het managementteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op de strategie.
- Het managementteam is verantwoordelijk voor het vragen om informatie bij de onderliggende lijn en ziet erop toe dat er adequate maatregelen genomen zijn voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- 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 het managementteam, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De domeinmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het 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 voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Domeinmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Domeinmanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van het hoofd Informatisering, gebaseerd op:
 - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
 - het dreigingsbeeld gemeenten van de IBD;
 - De door de domeinmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.
- Jaarlijks wordt de strategie beoordeeld op veranderende wetgeving, actualiteit of andere oorzaken die een aanpassing van de strategie Informatiebeveiliging vragen.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: managementteam

Het managementteam zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een domeinmanager. Het managementteam zorgt dat de domeinmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het managementteam zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het managementteam stelt het gewenste niveau van de continuïteit van de bedrijfsvoering en vertrouwelijkheid van gegevens vast. Het managementteam draagt zorg voor het uitwerken van tactische in-

formatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. Het managementteam autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Heemstede gezien als een integraal onderdeel van risico-management.

3.2 Uitvoering: domeinmanagers

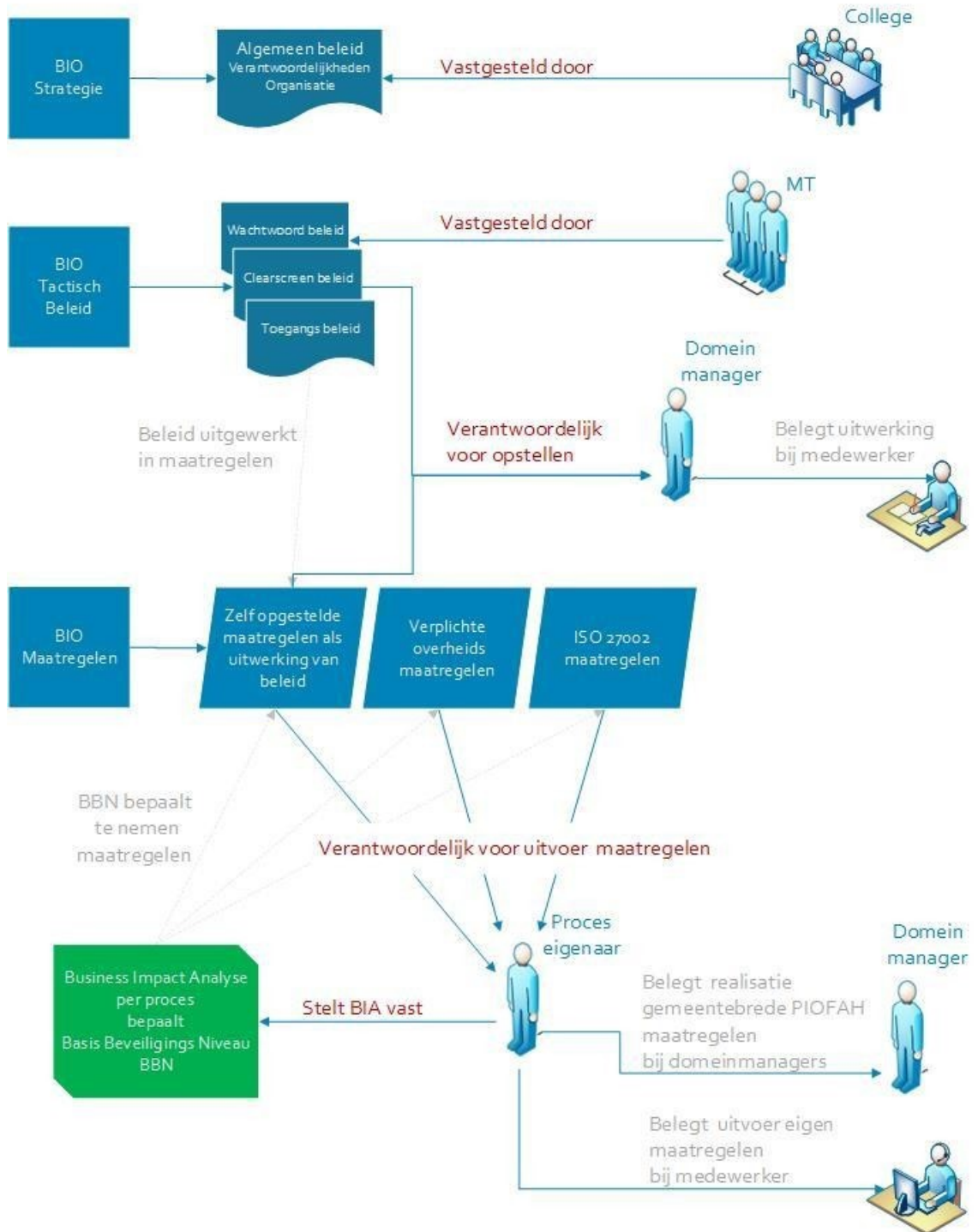
Informatiebeveiliging valt onder de verantwoordelijkheden van alle domeinmanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn (CISO, security officers). Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden kunnen zij wel delegeren naar de onderliggende lijn. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Domeinmanagers rapporteren aan het managementteam over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg. Voorbereiding en coördinatie van dit overleg ligt bij de CISO.

Taken van de domeinmanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Schematisch overzicht van de organisatie en verantwoordelijkheden voor informatieveiligheid

Baseline Informatieveiligheid Overheid- BIO verantwoordelijkheden en organisatie Gemeente Bloemendaal – Gemeente Heemstede



3.3 Controle en verantwoording

De strategie Informatiebeveiliging is een verantwoordelijkheid van het bestuur van de gemeente Heemstede. De bestuurders van de gemeente Heemstede zullen volgens de 10 principes voor informa-

tiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het managementteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het managementteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.3.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Het MT wijst een ENSIA-coördinator aan. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke domeinmanagers. De domeinmanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording worden het bestuur van de gemeente Heemstede en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Heemstede informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Vastgesteld op 22 september 2020 door het college van de Gemeente Heemstede



Bijlage A – De Baseline Informatiebeveiliging Overheid versie 1.04

Zie voor originele pdf de externe bijlage

Bijlage B – De 10 bestuurlijke principes voor informatiebeveiliging door de VNG

Zie voor originele pdf de externe bijlage