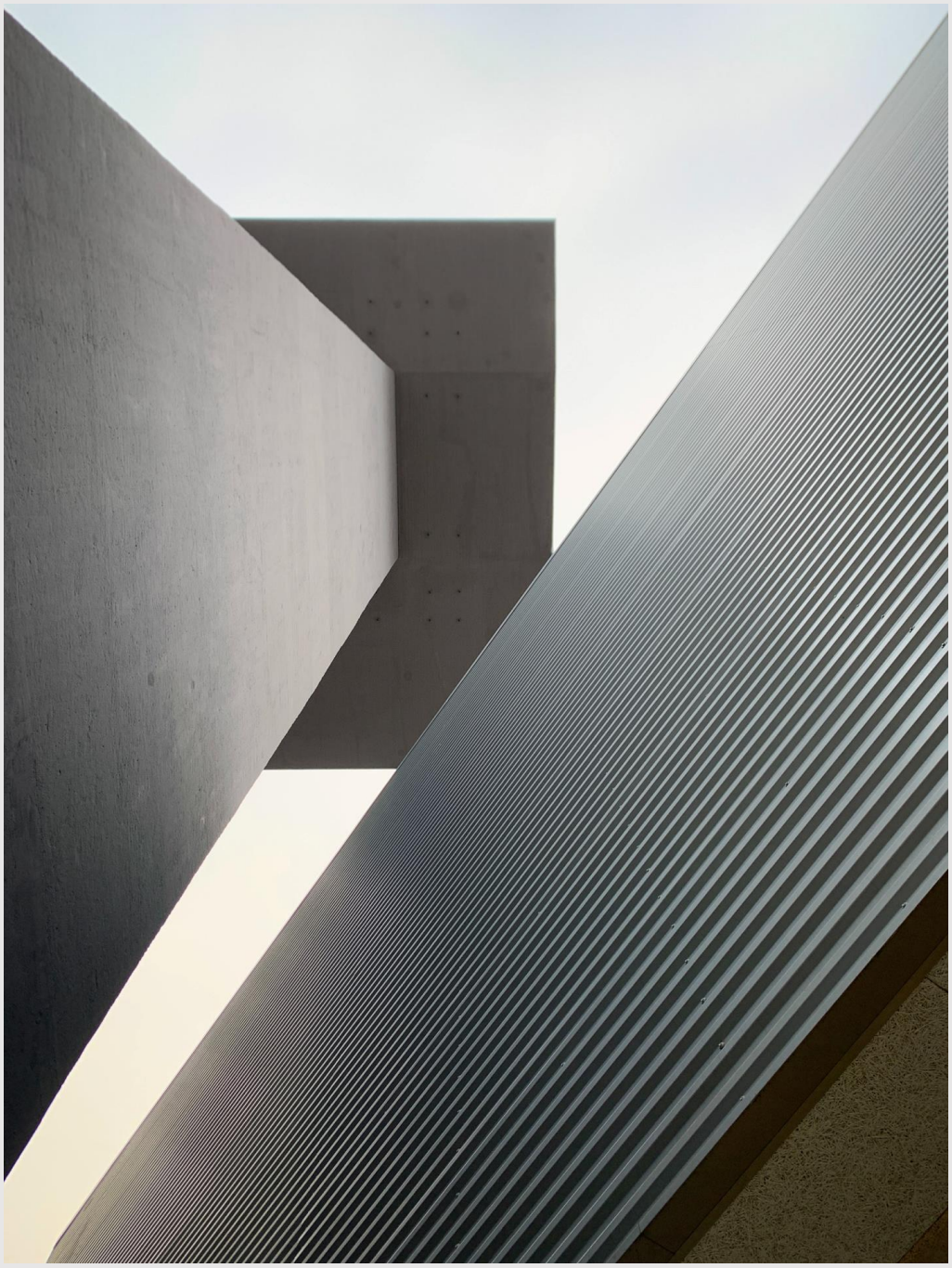

Strategisch Informatiebeveiligingsbeleid 2023-2026

Digitaal droge voeten in de Haarlemmermeer

gemeente Haarlemmermeer

Colofon

Tekst, vormgeving en drukwerk
Gemeente Haarlemmermeer
Postbus 250
2130 AG Hoofddorp
Telefoon 0900 1852
E-mail info@haarlemmermeer.nl
Internet www.haarlemmermeer.nl

Fotografie
Coverfoto – Unsplash - David Underland

december 2023

Versiebeheer

Versie	Datum	Verklaring
0.8	22-08-2023	Aanpassing aan conceptbeleid
0.9	19-09-2023	Verwerking commentaar
1.0	28-09-2023	Verwerking van de laatste notities
1.1	20-10-2023	Verwerking besluiten directieoverleg

Inhoudsopgave

Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid van de gemeente Haarlemmermeer voor de jaren 2023 tot 2026, en vervangt het door het college vastgestelde informatiebeveiligingsbeleid uit 2018. Dit beleid is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten (richtlijnen) voor informatiebeveiliging op tactisch niveau en daar waar gewenst werkinstructies op operationeel niveau.

Met dit Informatiebeveiligingsbeleid 2023-2026 zet de gemeente een volgende stap om de beveiliging van informatie binnen de gemeentelijke organisatie te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO 27001 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De 10 principes (zie par. 2.2.2) zoals deze binnen de gemeente Haarlemmermeer op het gebied van informatiebeveiliging worden gehanteerd zijn afgeleid van de principes welke zijn gedefinieerd in het kader van de Baseline Informatiebeveiliging Overheid (BIO).

1.1 Leeswijzer

In hoofdstuk 3 van dit document wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke beleidsdocumenten (richtlijnen) die aanvullend zijn op dit strategisch beleid. In het jaarlijks opgestelde jaarplan informatiebeveiliging dat wordt vastgesteld door de algemeen directeur/gemeentesecretaris van de gemeente Haarlemmermeer, worden de tactische en operationele aspecten van informatiebeveiliging binnen de gemeentelijke organisatie verder uitgewerkt en geconcretiseerd.

Deze verdere uitwerking wordt gedaan in samenwerking met de lijnorganisatie en op basis van input van de verschillende risicoanalyses, het dreigingsbeeld van Nederlandse gemeenten, de CISO en de uitkomsten van de jaarlijkse BIO audit. In het betreffende jaarplan informatiebeveiliging zijn de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is vastgesteld. Het document IB-rollen en verantwoordelijkheden beschrijft hoe de taken en verantwoordelijkheden op het gebied van informatiebeveiliging binnen de gemeentelijke organisatie zijn belegd.

1.2 Wat is informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en het continue onderhouden van een samenhangend geheel van het beheren van de processen tot en met de maatregelen om de betrouwbaarheid van de informatievoorziening van de gemeente Haarlemmermeer aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van de informatie waar de gemeente Haarlemmermeer verantwoordelijk voor is.

- Beschikbaarheid: het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente Haarlemmermeer en borgt dat de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op alle medewerkers, burgers, gasten, bezoekers en externe relaties van de gemeente Haarlemmermeer.

1.3 Visie van de gemeente Haarlemmermeer

De gemeente Haarlemmermeer is voor een correcte uitvoering van haar taken in sterke mate afhankelijk van een goed functionerende informatievoorziening. Het uitvallen van informatiesystemen of het door onbevoegden kennisnemen, wijzigen en/of verwijderen van informatie kunnen verstrekkende gevolgen hebben voor:

- De maatschappelijke doelstellingen van de gemeente Haarlemmermeer;
- Het imago van de gemeente Haarlemmermeer;
- De uitvoering van processen en financiën van de gemeente Haarlemmermeer.

Met informatiebeveiliging streeft de gemeente Haarlemmermeer naar beveiliging van haar informatie en alle daaraan gerelateerde aspecten die aansluiten bij het ambitieniveau van haar organisatie met een acceptabel balans tussen kosten en baten, lusten en lasten.

Strategisch beleid

2.1 Doel

Het doel van dit informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente Haarlemmermeer voor de jaren 2023 tot 2026.

Het informatiebeleid is gebaseerd op het normenkader de Baseline Informatiebeveiliging Overheid (BIO).
De operationele en tactische aspecten van dit beleid worden verder uitgewerkt en geconcretiseerd in het jaarlijks op te stellen jaarplan informatiebeveiliging en de richtlijnen. Dit informatiebeveiligingsbeleid wordt vastgesteld door de algemeen directeur van de gemeente Haarlemmermeer.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering en aanpassing van dit informatiebeveiligingsbeleid zijn de volgende:

De BIO heeft een werkwijze die gericht is op risicomanagement. Er dient gewerkt te worden volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt in dat men op voorhand keuzes en afwegingen maakt of informatie in bestaande en nieuwe processen voldoende beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Aan de hand van deze classificatie wordt het basisbeveiligingsniveau (BBN) bepaald. Is het beveiligingsniveau hoog dan wordt geadviseerd een diepgaande risicoanalyse uit te voeren.

2.2.1 Baseline Informatiebeveiliging Overheid

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele Nederlandse overheid.
De werkwijze van de Baseline Informatiebeveiliging is gericht op risicomanagement. Dit houdt in dat het management op basis van risicoanalyses keuzes en afwegingen maakt, om op deze wijze te borgen dat de informatie die verwerkt wordt binnen de verschillende gemeentelijke (bedrijfs-) processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een aanvulling op de Baseline Informatiebeveiliging (BIO) en gaan over de waarden die de organisatie zichzelf oplegt.

De onderstaande principes gaan met name over de rol van de directie bij het borgen van informatiebeveiliging binnen de gemeente. De principes ondersteunt de directie bij het inrichten en uitvoeren van goed risicomanagement. Immers als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijk processen, kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente Haarlemmermeer. De principes zijn als volgt:

- Bestuurders bevorderen een veilige cultuur
  Toelichting: gemeente Haarlemmermeer bevordert een veilige cultuur waarin medewerkers zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kan adequaat worden gereageerd op dreigingen en samenhangende risico's.
- Informatiebeveiliging is van iedereen.
  Toelichting: iedereen is betrokken bij informatiebeveiliging in alle lagen binnen de gemeente
- Informatiebeveiliging is gebaseerd op risicomanagement
  Toelichting: risicomanagement wordt bewust toegepast en werkt alleen als het geïntegreerd is in alle processen binnen de gemeente
- Risicomanagement is onderdeel van de besluitvorming
  Toelichting: medewerkers van de gemeente nemen deel aan het risicoproces op het vlak van informatiebeveiliging en nemen besluiten op basis van de risicorapportage.
- Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
  Toelichting: Het risicomanagementproces moet passen bij de gemeente en ondersteunen aan de organisatiedoelstellingen. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

• Informatiebeveiliging is een proces
Toelichting: risicomanagement moet een cyclisch en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien binnen risicomanagement geen rekening wordt gehouden met een veranderende omgeving, dan zijn maatregelen op termijn wellicht niet doelmatig.
• Informatiebeveiliging kost geld
Toelichting: risico's kunnen vermeden, gemitigeerd, overdragen of geaccepteerd worden door het nemen van maatregelen. Voor welke strategie is gekozen, het kost altijd middelen in termen van tijd en geld.
• Onzekerheid dient te worden ingecalculeerd
Toelichting: zonder goede informatie kunnen geen goede risico-inschattingen en besluiten worden genomen.
• Verbetering komt voort uit leren en ervaring
Toelichting: risicobeheer wordt voortdurend verbeterd door leren en ervaring.
• Het bestuur controleert en evalueert
Toelichting: controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement zij ingebed binnen de gemeente.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten (IBD, VNG) 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

Naast het hierboven genoemde dreigingsbeeld, heeft de gemeente Haarlemmermeer ook een eigen systeem waarin incidenten worden vastgelegd. Dit systeem bevat ook waardevolle informatie, welke als input kan dienen bij het actualiseren van het informatiebeveiligingsbeleid.

2.3 Standaarden Informatiebeveiliging

De basis voor de inrichting van informatiebeveiliging binnen de gemeente Haarlemmermeer is de NEN-ISO 27001. De te selecteren maatregelen worden op basis van best-practices en de NEN-ISO 27002 op basis van uitgevoerde risicoanalyses geselecteerd. Om informatiebeveiliging bij de Nederlandse overheidsinstellingen verder te vergroten heeft de interbestuurlijke werkgroep normatiek in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht welke is afgeleid van de beide Nen-normen. De Baseline Informatiebeveiliging Overheid (BIO) is verplicht voor alle Nederlandse overheidsinstellingen en daaraan gelieerde instellingen.

2.4 Plaats van het strategisch beleid

Het informatiebeveiligingsbeleid wordt gebruikt als uitgangspunt om richting te geven voor de verdere invulling van informatiebeveiliging binnen de gemeente Haarlemmermeer op tactisch en operationeel niveau. Dit beleid beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald naar tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks op te stellen 'Informatiebeveiligingsplan'.

2.5 Scope informatiebeveiliging

De scope van het informatiebeveiligingsbeleid omvat alle (bedrijfs-)processen, informatiesystemen en bijbehorende informatie van de gemeente Haarlemmermeer en het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht de locatie, het tijdstip en de gebruikte apparatuur. Dit informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving en regelgeving af.

2.6 Uitgangspunten informatiebeveiliging

De directie, de clustermanagers en teammanagers spelen een cruciale rol bij het uitvoeren van informatiebeveiliging binnen de gemeentelijke organisatie. Vanuit de informatie en het (in)zicht dat met name teammanagers hebben van de operationele praktijk krijgen clustermanagers en directie de voeding om een inschatting te maken van het belang dat de verschillende delen van de informatievoorziening voor de gemeentelijke organisatie hebben, welke risico's de gemeentelijke organisatie hiermee loopt en welke van de risico's onacceptabel hoog zijn. Op basis hiervan wordt met ondersteuning van Corporate Control het beleid voor informatiebeveiliging opgezet, uitgewerkt en door de directie

vastgesteld. Directie en management dragen het beleid uit naar de organisatie en zorgen voor -, ondersteunen en bewaken de uitvoering ervan. De directie gaat voorop in het uitdragen van het belang en de urgentie van informatiebeveiliging binnen de gemeentelijke organisatie, stuurt, samen met het management, proactief en spreekt aan en/of handhaaft waar nodig. De directie 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. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente Haarlemmermeer en de relevante landelijke en Europese wet- en regelgeving".

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid voor de gemeente Haarlemmermeer zijn:

- Het managen van de informatiebeveiliging binnen de gemeente Haarlemmermeer.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's die menselijk gedrag met zich meebrengen.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van beveiligde informatiesystemen.
- Het adequaat reageren op incidenten op het gebied van informatiebeveiliging.
- Het beschermen van kritieke (bedrijfs-) processen.
- Het waarborgen van de naleving van dit informatiebeveiligingsbeleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het informatiebeveiligingsbeleid zijn:

- Alle informatie en informatievoorzieningen zijn van belang voor een goed werkende bedrijfsvoering van de gemeente Haarlemmermeer.
- De uitvoering van informatiebeveiliging is een verantwoordelijkheid van de clustermanagers.
Alle informatie en -systemen die in gebruik zijn en onder de verantwoordelijkheid van de gemeente Haarlemmermeer vallen, hebben een eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die deze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie is dan ook belegd bij de eigenaar van de informatie;
- Door periodieke controle, organisatie, planning én coördinatie wordt de kwaliteit van de informatievoorzieningen verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament voor een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed 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' (PDCA) vormen samen het Information Security Management System (ISMS) van informatiebeveiliging;
- De gemeente Haarlemmermeer stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en (bedrijfs-) processen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Maatregelen 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 hierboven beschreven uitgangspunten:

- Het college van B&W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast;
- De directie stelt jaarlijks het informatiebeveiligingsplan vast;
- De algemeen directeur is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid;
- De CIO is verantwoordelijk om te borgen dat de clustermanagers erop toe zien dat er adequate maatregelen worden genomen om de informatie die onder hun verantwoordelijkheid valt adequaat te beveiligen;
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de directie en

organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie;
• De CIO heeft een belangrijke rol bij het waarborgen van informatiebeveiliging binnen de organisatie door actief betrokken te zijn bij de planning en uitvoering van informatiebeveiliging binnen de lijnorganisatie.
• Op basis van reguliere overleggen met de directie dient er aandacht te zijn voor de informatiebeveiliging;
• De clustermanagers zijn verantwoordelijk voor de uitvoering van informatiebeveiliging voor de (bedrijfs-) processen waarvoor zij verantwoordelijk zijn;
• Alle medewerkers van de gemeente Haarlemmermeer worden op verschillende manieren getraind op het gebied van informatiebeveiliging;
• Van medewerkers van de gemeente Haarlemmermeer wordt verwacht dat zij bewust om gaan met persoonsgegevens en andere informatie binnen de gemeente;
• De maatregelen op het gebied van informatiebeveiliging worden bepaald op basis van risicomanagement. Clustermanagers laten vaststellen welke maatregelen noodzakelijk zijn voor een adequate beveiliging van de informatie waar zij verantwoordelijk voor zijn middels de uitvoering van risicoanalyses.

2.6.4 Randvoorwaarden

De belangrijke randvoorwaarden zijn:

• Informatiebeveiliging maakt ook deel uit van afspraken met ketenpartners;
• Kennis en bewustzijn op het gebied van informatiebeveiliging dienen actief bevorderd en geborgd te worden;
• Jaarlijks stelt de CISO in samenspraak met de betrokken clustermanagers een informatiebeveiligingsplan op.

2.6.5 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsuitwerking en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Het legt de relatie tussen de ambitie, wet- en regelgeving en de dagelijkse operatie.

Organisatie, taken en verantwoordelijkheden

3.1 Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk van dit beleid is uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging er op welke plaats belegd zijn binnen de gemeentelijke organisatie. De gebruikte methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement (clustermanager) verantwoordelijk voor de (bedrijfs-)processen waar hij/zij verantwoordelijk voor is. De tweede lijn betreft de Chief Information Security Officer (CISO) en de Information Security Officer (ISO) deze ondersteunen, adviseren, coördineren of de clustermanagers ook daadwerkelijk de aan hen toegekende verantwoordelijkheden uitvoeren. In de derde lijn wordt het geheel door een interne of externe auditor van een objectief oordeel voorzien met eventuele mogelijkheden tot verbetering, hier zit ook de CISO in de rol van ENSIA coördinator.

3.2 Aansturing: Directie

De directie borgt dat alle (bedrijfs-) processen, informatiesystemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een clustermanager. De directie zorgt dat de clustermanagers zich verantwoorden over de beveiliging van de informatie waar zij verantwoordelijk voor zijn. De directie stelt het gewenste beveiligingsniveau vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiliging beleidsonderwerpen. De CIO is eindverantwoordelijk voor de generieke informatievoorziening van de gemeente. Binnen die scope is de CIO verantwoordelijk voor de implementatie van adequate informatiebeveiligingsmaatregelen die voldoen aan het beleid en normenkaders voor informatiebeveiliging. Binnen de gemeente Haarlemmermeer is de CIO rol toebedeeld aan de directeur Bedrijfsvoering. De CISO heeft een adviserende, ondersteunende en voorbereidende rol. De voorbereidende rol heeft zowel betrekking op de documenten voor besluitvorming als ook op de begeleiding van het proces in de organisatie voor het juiste zicht op het gewenste beveiligingsniveau en ten behoeve van de kwaliteit van de uitwerking van de tactische aspecten van informatiebeveiliging.

3.3 Uitvoering: Clustermanagers

Informatiebeveiliging is een van de verantwoordelijkheden van een clustermanager. Om deze verantwoordelijkheid waar te kunnen maken dienen zij ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, informatie en applicaties altijd een eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Clustermanagers informeren periodiek de CISO over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten.

Taken van de clustermanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen en uitzonderingen op maatregelen en procedures;
- Het binnen de eigen cluster uitdragen van het beveiligingsbeleid met de daaraan gerelateerde richtlijnen en procedures;
- Het signaleren van eventuele bedreigingen waaraan de informatie is blootgesteld.

3.4 Controle en verantwoording

Dit informatiebeveiligingsbeleid is een verantwoordelijkheid van de directie van de gemeente Haarlemmermeer. De algemeen directeur van de gemeente Haarlemmermeer, zal op basis van de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging.

De Chief Information Security Officer (CISO) heeft ook een toetsende en controlerende rol ten aanzien van het gehele systeem van informatiebeveiliging en het realiseren van organisatiedoelen, en brengt voor de directie periodiek (en wanneer nodig) de actuele stand van de informatiebeveiliging van de gehele organisatie in beeld inclusief een overzicht van de uitvoering van tactische en operationele informatiebeveiligingsactiviteiten in de clusters. Dit wordt opgesteld op basis van de voeding vanuit de samenwerking tussen de clusters en de CISO/ ISO en de informatie / rapportages die de clusters hierbij aan de CISO leveren (onder de verantwoordelijkheid van de clustermanagers). De

rapportages hebben betrekking op de stand van de informatiebeveiliging en de uitvoering van gerelateerde activiteiten

3.4.1 BIO audit

De gemeente Haarlemmermeer verantwoordt zich over informatiebeveiliging door middel van het BIO normenkader. Dit betekent dat er jaarlijks door een audit wordt gedaan door de opzet, bestaan en werking van informatiebeveiliging binnen de gemeentelijke organisatie te toetsen.

De verantwoording over de informatiebeveiliging binnen de gemeentelijke organisatie komt in het jaarverslag tot uitdrukking, en wordt vastgesteld door de directie. Door middel van dit jaarverslag, geeft de directie van de gemeente Haarlemmermeer aan in hoeverre de gemeente Haarlemmermeer voldoet aan de wet en regelgeving die voor haar van toepassing is, en laat de gemeente Haarlemmermeer zien dat zij informatiebeveiliging serieus neemt om zodoende de informatie waar zij eigenaar van is en of de verantwoordelijkheid voor draagt adequaat te beschermen.

3.4.2 ENSIA verantwoording

De gemeente verantwoordt zich jaarlijks over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat een ENSIA-coördinator wordt aangewezen door de algemeen directeur. De ENSIA-coördinator is een projectmanager / procesbegeleider die zorgt dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA tijdig beschikbaar wordt gesteld namens de verantwoordelijke clustermanagers. Zij leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

Middels deze verantwoording worden het bestuur en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat het informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen. 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 Haarlemmermeer voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging.

Relatie van het beleid met andere documenten en verschillende wet- en regelgeving

4.1 Relatie van het beleid met andere documenten

Wet- en Regelgeving: Verwijzing	Verwijzing
NEN-ISO 27001	Kader stellend
NEN-ISO 27002	Kader stellend
BIO versie 1.04	Kader stellend

4.2 4.2 Relatie van het beleid met verschillende wet- en regelgeving

Wet- en Regelgeving: Verwijzing	Verwijzing
de RODIN-richtlijnen voor digitale archivering en volledige substitutie.	Verschillende hoofstukken uit het Referentiekader Opbouw Digitaal Informatiebeheer (RODIN)
Algemene Verordening Gegevensbescherming (AVG)	Avg: artikel 5, Beginselen inzake verwerking van persoonsgegevens
Archiefwet	De verschillende hoofdstukken uit de archiefwet 1995
Basisadministratie Persoonsgegevens en Reisdocumenten (BRP)	De verschillende hoofdstukken uit de Basisadministratie Persoonsgegevens en Reisdocumenten (BRP).
Basisregistraties Adressen en Gebouwen (BAG)	De verschillende hoofdstukken uit de Basisregistraties Adressen en Gebouwen (BAG)
Basisregistraties Grootschalige Topografie (BGT)	De basisregistraties BGT kunnen toetsen met verbetermaatregelen
Basisregistratie Ondergrond (BRO) De basisregistraties BRO kunnen toetsen met verbetermaatregelen	De basisregistraties BRO kunnen toetsen met verbetermaatregelen
Basisregistratie personen (BRP)	Het beveiligen van basisregistratie personen door het toepassen van de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid)
ICT-beveiligingsrichtlijnen voor webapplicaties (DigiD)	Beveiligen van websites door gebruik te maken van richtlijnen zoals ncsc.nl: ICT richtlijnen voor applicaties
Paspoorten en Nederlandse Identiteitskaarten (PNIK)	Jaarlijks onderzoek naar de toepassing van de beveiligingsmaatregelen van de aanvraag en het uitgifte proces

Paspoort Uitvoeringsregeling Nederland (PUN)	De verschillende hoofdstukken uit de paspoortuitvoeringsregeling Nederland.
Regelement rijbewijzen	De verschillende hoofdstukken uit het reglement rijbewijzen
Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI)	De hoofdstukken uit de wet rekening houdende met de regels tot vaststelling van een structuur voor de uitvoering van taken met betrekking tot de arbeidsvoorziening en sociale-verzekeringswetten
NEN-ISO 27001	De verschillende hoofdstukken uit de NEN-ISO 27001
NEN-ISO 27002	De verschillende hoofdstukken uit de NEN-ISO 27002
BIO versie 1.04	De verschillende hoofdstukken uit de BIO
DOC-B-01 Beleid	Register verplichte standaarden

Bijlage 1 Termen definities en afkortingen

In de onderstaande paragrafen zijn de voor dit document relevante termen, definities en afkortingen opgesomd.

Termen en Definities

Baseline Informatiebeveiliging Overheid (BIO)
De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is geheel gestructureerd volgens NEN-ISO/IEC 27001, bijlage A en NEN-ISO/IEC 27002.

Beleid
De wijze waarop de organisatie zich voorstelt te werken aan de realisatie van de doelstellingen die gekoppeld zijn aan het gerelateerde beleidsveld. Beleid is een verdere verdieping van de strategie van de organisatie en bevat beleidsdoelstellingen, beleidsuitgangspunten, kaders, de middelen en het tijdspad voor doelrealisatie. Beleid heeft daarmee de functie om duiding en richting te geven aan het handelen en de besluiten in de organisatie.

Informatiebeveiliging
Is het geheel van preventieve en repressieve maatregelen met de bijbehorende procedures welke de beschikbaarheid, vertrouwelijkheid en de integriteit van de informatie garanderen. Het doel van deze maatregelen is de continuïteit van de informatievoorziening van de gemeente Haarlemmermeer te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel niveau te beperken.
Information Security Management System
Een Information Security Management System (ISMS) borgt een systematische aanpak van het beheer van bedrijfsinformatie, zodat deze veilig blijft. Het omvat: organisatie, mensen, processen en IT-systemen door het toepassen van een riskmanagementproces.

Informatiesysteem
Toepassingen, diensten, informatietechnologische bedrijfsmiddelen of andere gegevensverwerkende componenten.

Informatievoorziening
Is het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.

Informatiebeveiligingsplan
Het door de directie van de gemeente Haarlemmermeer vastgestelde jaarplan waarin is vastgelegd welke maatregelen en acties er in het betreffende jaar op het gebied van informatiebeveiliging geïnitieerd moeten worden.

ENSIA
ENSIA is een initiatief van de VNG en de ministeries van BZK. ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatiebeveiliging gebaseerd op de BIO.

NEN-ISO 27001
Specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

NEN-ISO 27002
Bevat richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie.

Plan Do Check Act
De PDCA-cyclus geeft het principe weer van continue verbetering en wordt gevormd door de facetten Plan-Do-Check-Act.

Proces
Een set van samenhangende activiteiten om de input om te zetten naar de output. Een proces wordt gestart door een duidelijke trigger en eindigt met een duidelijk resultaat.

Richtlijn
Een richtlijn is een specifieke uitwerking van het beleid en moeten de goede werking, vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatievoorzieningen garanderen. Bijv.: Incidentenbeheer, classificatie van informatie.

Risicoanalyse
Methode waarbij nader benoemde risico's worden gekwantificeerd door het bepalen van de kans dat een dreiging zich voordoet en de gevolgen daarvan: Risico = Kans x Gevolg. De risicoanalyse is de eerste stap binnen risicomanagement.

Gebruikte Afkortingen	Afkorting Beschrijving
IB	Informatiebeveiliging
3LOD	Three lines of Defense
BIO	Baseline Informatiebeveiliging Overheid
CISO	Chief Information Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
ISMS	Information Security Management System
ISO	Information Security Officer
NEN-ISO 27001	Internationale norm op het gebied van informatiebeveiliging
PDCA	Plan Do Check Act cyclus