gemeente Halderberge

GEMEENTEBLAD

Officiële uitgave van de gemeente Halderberge

Nr. 272218

21 juni

2024

Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente Halderberge 2024 t/m 2028

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2024 tot en met 2028 en vervangt het in 2019 vastgestelde 'Informatiebeveiligingsbeleid 2019 - 2023 Halderberge met addendum'.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.
Met dit 'Informatiebeveiligingsbeleid 2024-2028' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te verbeteren en verder te gaan met de stappen die in de voorgaande jaren gezet zijn.
De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017, de daarvan afgeleide Baseline Informatiebeveiliging Overheid (vanaf nu BIO) (zie bijlage 3) en Wet- en regelgeving (zie bijlage 2). Hieronder valt ook de nog vast te stellen nieuwe wet NIB2 die gebaseerd is op de Europese directieve NIS2 welke eind 2022 is vastgesteld.
De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG (zie bijlage 4).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch en operationeel niveau aangevuld met onderwerpspecifieke, tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teammanagers, de Chief Information Security Officer (CISO), het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het informatiebeveiligingsbeleid 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. Naast ICT heeft informatiebeveiliging ook betrekking op onder andere de BRP, Waardedocumenten, SUWI, facilitaire zaken, gebouwbeheer, informatievoorziening, OT (operationele techniek), privacy en personeelszaken en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de gemeente

De ambitie van de gemeente Halderberge wordt als volgt beschreven:
'Realisatie van de BIO en in de toekomst aan de NIB2 met daarbij het mitigeren van de risico's welke door de eindverantwoordelijke worden bepaald'.
Waarbij de ondergrens bepaald wordt door wet- en regelgeving, beleidskaders, de BIO2 en NIB2.

Het resultaat hiervan is dat de informatiebeveiliging jaarlijks worden verbeterd waarbij de grootste risico's het eerst worden aangepakt.

1.4 NIS2, WBNI en BIO 2.0

Eind 2022 heeft de Europese Unie de directive NIS2 vastgesteld. Elke lidstaat dient uiterlijk oktober 2024 deze directive vertaald te hebben naar eigen wetgeving. De nieuwe wet zal worden ondergebracht onder de bestaande wet WBNI, en gaat ook gelden voor een gemeente. Een gemeente wordt gekenmerkt als een essentiële entiteit, wat betekent dat zij moet voldoen aan het zware regime. Hieronder worden de belangrijkste wijzigingen waaraan wij als gemeente moeten voldoen kort benoemd.

1.4.1 Zorgplicht
De NIS2-richtlijn vereist dat organisaties een zorgplicht hebben om hun netwerk- en informatiesystemen te beveiligen. Dit betekent dat je beleid moet aangeven hoe je organisatie deze verantwoordelijkheid zal nakomen.

1.4.2 Meldplicht
De NIS2-richtlijn introduceert een meldplicht voor incidenten met aanzienlijke impact op de dienstverlening. Je beleid moet dus procedures bevatten voor het identificeren, rapporteren en opvolgen van dergelijke incidenten.

1.4.3 Beheer van beveiligingsrisico's
De NIS2-richtlijn vereist dat organisaties maatregelen nemen om beveiligingsrisico's te beheren. Dit omvat het maken van back-ups, het uitvoeren van risicoanalyses en het nemen van passende beveiligingsmaatregelen. Het beleid moet dus aangeven hoe de organisatie deze taken zal uitvoeren.

1.4.4 Verantwoordelijkheid van het management
Om de administratieve druk laag te houden, zal het management van een organisatie verantwoordelijk worden voor de naleving van de bepalingen uit de NIS2-richtlijn. Het beleid moet dus duidelijk maken wie binnen de organisatie verantwoordelijk is voor welke aspecten van de naleving van de NIS2-richtlijn.

2. Strategisch beleid
2.1 Doel
Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2024 - 2028'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het, jaarlijks bij te stellen, informatiebeveiligingsplan (IBP).
2.2 Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 DE WBNI/ NIB2
Voor deze nieuwe wet is onder andere essentieel om 'opzet, bestaan en werking' goed aantoonbaar te maken, omdat wij aan dit strengere regime moeten gaan voldoen. Omdat deze nieuwe wet de verantwoording expliciet legt bij bestuur, directie en management is het van belang dat hier eisen aan worden gesteld en dat er controle op wordt uitgevoerd.

2.2.2 De BIO
De BIO2 is het nieuwe (verplichte) normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teammanagers 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. Vervolgens moeten deze keuzes goed worden vastgelegd.

2.2.3 DigiD normen
Elke organisatie welke één of meerdere DigiD aansluitingen heeft, dient te voldoen aan de DigiD normen. Sinds 2022 is hier een nieuwe norm, de norm B.01, aan toegevoegd waaraan gemeentes dienen te voldoen. De norm stelt het volgende:
"De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer"

2.2.4 Forum voor standaardisatie
De normen ISO 27001 en ISO 27002 zijn opgenomen in de lijst van het forum voor standaardisatie waardoor het 'Pas toe of leg uit' principe geldt.

2.2.5 De 10 principes voor informatiebeveiliging (zie bijlage 4)

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 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.

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.

2.2.6 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.

2.2.7 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 in 2018 de BIO uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen en wordt eind 2023 vervangen door de BIO 2.0. 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 ISO, de BIO 2.0 en de NIB2. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen om daarmee richting te geven aan 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. Jaarlijks voert de CISO een gap- impactanalyse en een risicoanalyse uit welke samen met de verantwoordelijke worden besproken. Vervolgens worden door de verantwoordelijke de daaruit voorkomende werkzaamheden bepaald die 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 (zoals de politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Zowel externe partijen als ketenpartners moeten aantoonbaar aan dit beleid voldoen.
Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt ook aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligings-

eisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten
Het bestuur, de directie en het management 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. Vervolgens laat het management deze overwegingen inclusief besluiten goed vastleggen.

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). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving (zie bijlage 4).

2.6.1 Strategische doelen
De strategische doelen van het informatiebeveiligingsbeleid 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 van het beleid zijn:
- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging;
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Halderberge 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. Het informatiebeveiligingsbeleid 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 vastgesteld en vastgelegd;
- 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

Op operationeel niveau wordt als volgt invulling gegeven aan de uitgangspunten:
• Het college van B en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast;
• De directie stelt jaarlijks het informatiebeveiligingsplan vast;
• De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid;
• De directie is verantwoordelijk voor het vragen om informatie aan de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt;
• De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-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 ook worden opgenomen in de auditplannen;
• De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn. Het aantoonbaar maken van 'Opzet, bestaan en werking' is hierbij een essentieel onderdeel van deze verantwoordelijkheid;
• Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT en BRO) 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;
• Teammanagers 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. Teammanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:
• 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 de CISO, gebaseerd op:
• De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
• Het dreigingsbeeld gemeenten van de IBD;
• De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

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 management verantwoordelijk voor de eigen processen. De tweede lijn (CISO en beveiligingsbeheerders) 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 Kaderstellend: het bestuur

Bij de implementatie van het informatiebeveiligingsbeleid heeft het bestuur van de gemeente Halderberge belangrijke verantwoordelijkheden om ervoor te zorgen dat de organisatie voldoet aan het beleid. Enkele van deze verantwoordelijkheden zijn:
1. Leiderschap en betrokkenheid: Het bestuur moet leiderschap tonen en betrokken zijn bij het ontwikkelen en implementeren van het beleid;
2. Risicobeheer: Het bestuur is verantwoordelijk voor het waarborgen van een effectief risicobeheerproces, inclusief informatiebeveiliging;

3. Toewijzing van middelen: Het bestuur moet voldoende financiële, personele en technische middelen toewijzen om het beleid voldoende te kunnen implementeren;
4. Naleving van wet- en regelgeving: Het bestuur moet toezicht houden op de naleving van wet- en regelgeving met betrekking tot informatiebeveiliging, zoals de BIO 2.0, NIS2-richtlijn en andere relevante wetgeving (bijvoorbeeld AVG);
5. Cultuur van informatiebeveiliging: Het bestuur moet een cultuur van informatiebeveiliging bevorderen binnen de organisatie en zorgen voor bewustwording en training van medewerkers op het gebied van cyberbeveiliging en de naleving van het informatiebeveiligingsbeleid;
6. Regelmatige evaluatie en verbetering: Het bestuur moet toezicht houden op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen en zorgen voor continue verbetering van de informatiebeveiliging in overeenstemming met de vereisten van het informatiebeveiligingsbeleid.

3.2 Aansturing: directieteam
De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. De directie zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. 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. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie stelt het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Halderberge gezien als een integraal onderdeel van risicomanagement.

3.3 Uitvoering: teammanagers
Informatiebeveiliging valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan de directie 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.

Taken van de teammanagers 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;
• Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.4 Controle en verantwoording
Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Halderberge. De bestuurders en directeur van de gemeente Halderberge zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4.1 Controle door de raad
De raad controleert het college, dus ook op het gebied van de informatiebeveiliging. Jaarlijks zal hiervoor het college van B en W een collegeverklaring samen met een rapportage informatiebeveiliging aan de raad aanbieden. Door uitvoering te geven aan dit beleid is de raad in de gelegenheid gebracht om het college te kunnen controleren.

3.4.2 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging via de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teammanagers. De teammanagers 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.

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

3.4.3 I.S.M.S.

In het I.S.M.S. (Information Security Management System) worden alle werkzaamheden, besluiten, risico's en maatregelen beschreven. Als dit niet mogelijk is wordt er verwezen naar de bron waarin dit wordt bijgehouden.
Het I.S.M.S. is dus niet alleen een middel om de stand van zaken in bij te houden maar ook het proces dat jaarlijks wordt doorlopen om de informatieveiligheid binnen de gemeente te verbeteren.
Het I.S.M.S. wordt door iedereen gevoed die werkt aan de informatiebeveiliging en voor de CISO en management is het ook een middel om sturing te geven aan het continue verbeteren van de informatiebeveiliging.

4. Bijlagen

Bijlage 1: Begrippenlijst
Bijlage 2: Wet- en regelgeving
Bijlage 3: Baseline Informatiebeveiliging Overheid (BIO) versie 1.04
Bijlage 4: 10 principes voor informatiebeveiliging

4.1 Bijlage 1: Begrippenlijst

BAG De BAG (Basisregistratie Adressen en Gebouwen) bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente.
BRO De Basisregistratie Ondergrond (BRO) bevat gegevens over geologische en bodemkundige opbouw en, voor zover van belang voor het benutten van natuurlijke hulpbronnen in de ondergrond, ondergrondse constructies en gebruiksrechten.
BRP De Basisregistratie Personen (BRP) bevat persoonsgegevens van inwoners van Nederland (ingezetenen) en van personen die Nederland hebben verlaten (niet ingezetenen).
IBD De IBD is de sectorale CERT/ CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging.
Dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten Het dreigingsbeeld heeft als doel gemeenten weerbaarder te maken op het gebied van informatiebeveiliging door inzicht te geven in de belangrijkste risico's voor de eigen organisatie.
ENSIA ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de BIG/ BIO
Mitigeren Onder mitigatie wordt verstaan het voorkomen of reduceren van de negatieve effecten.
NEN NEN ondersteunt in Nederland het normalisatieproces.
OT Operationele Technologie (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld zoals het aansturen en monitoren van (industriële) apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie.
Pas toe, leg uit Voor alle organisaties binnen de publieke sector geldt een 'pas-toe-of-leg-uit' verplichting. Dit betekent dat organisaties bij inkoop van ICT-systemen en -diensten boven € 50.000 moeten vragen naar de relevante open standaarden op de 'pas-toe-of-leg-uit' lijst van het Forum Standaardisatie.
PDCA De PDCA-cyclus bestaat uit de onderdelen Plan-Do-Check-Act en is gericht op het proces van continue verbetering.

PNIK Gemeenten, aangewezen gemeenten en de openbare lichamen voeren ieder jaar de verplichte zelfevaluatie paspoorten en Nederlandse identiteitskaarten (PNIK) uit.
PUN Paspoort Uitvoeringsregeling Nederland
SUWI Structuur uitvoeringsorganisatie werk en inkomen; regelt de structuur, taken en verantwoordelijkheden voor de sociale zekerheid

4.2 Bijlage 2: Wet- en regelgeving
In de BIO zijn verwijzingen opgenomen naar de volgende wet- en regelgeving:

- Ades baseline profile standard;
- Algemeen Rijksambtenarenreglement (ARAR);
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016);
- AVG;
- Beveiligingsvoorschrift 2013 (BVR 2013), Stcrt. 2013, 15496;
- CM (2002)49;
- Gedragsregeling voor de digitale werkomgeving (1 juli 2016; SGO besluit);
- Het NKBR (Normenkader beveiliging Rijkskantoren) 2015;
- Interne klokkenluidersregeling;
- ITIL, ASL of BISL framework;
- Kader Rijkstoegangsbeleid;
- NCSC-classificatie;
- NIB2 (treedt oktober 2024 in werking);
- 'Pas toe of leg uit'-lijst van het Forum Standaardisatie;
- Programma van Eisen PKI Overheid;
- Responsible disclosure procedure;
- Voorschrift Informatiebeveiliging Rijksdienst (VIR2007), Stcrt. 2007, 122/11;
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI 2013);
- Wet veiligheidsonderzoeken (WVO);
- Archiefwet;
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI);
- Wet basisregistratie personen (Wet BRP);
- Telecommunication Infrastructure Standard for Data Centers (TIA-942).