Alphen aan den Rijn

GEMEENTEBLAD

Officiële uitgave van de gemeente Alphen aan den Rijn

Nr. 228688

25 mei

2023

Strategisch Gemeentelijk Informatiebeveiligingsbeleid Alphen aan den Rijn en Kaag en Braassem 2022 tot 2026

Inhoudsopgave

1. Inleiding

Deze beleidsnota beschrijft het gezamenlijk strategisch informatiebeveiligingsbeleid voor de jaren 2022 tot 2026 voor gemeente Alphen aan den Rijn en Kaag en Braassem, en vervangt hiermee het Strategisch Informatiebeveiligingsbeleid 2018-2022 voor Alphen aan den rijn, en het Informatiebeveiligingsbeleid 2019 voor gemeente Kaag en Braassem.
Deze nota is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleids-documenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Het operationele deel zal worden aangeboden als handboek informatiebeveiliging en zal op begrijpbare wijze per onderwerp ingaan op wat er wordt verwacht van de medewerkers.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2022 tot 2026' zetten de gemeenten Alphen aan den Rijn en Kaag en Braassem een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren, en door te ontwikkelen op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de Baseline Informatiebeveiliging

Overheid (BIO) zie bijlage B. De principes zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage A.

1.1 Leeswijzer
In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligings-jaarplan (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 lijnmanagers, de CISO, het dreigingsbeeld van de IBD, de uitkomsten van ENSIA, en de bevindingen van interne controles. 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. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de gemeente op het gebied van informatieveiligheid
Gemeente Alphen aan den Rijn heeft de missie en visie:
Wij leveren toonaangevende dienstverlening. Dit doen we voor mensen, door mensen, vanuit een organisatie waar het leuk werken is'.

Gemeente Kaag en Braassem heeft op dit onderwerp de visie:
De komende jaren zet de gemeente Kaag en Braassem in op het verhogen van informatieveiligheid en verdere professionalisering hiervan in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.
Informatieveiligheid faciliteert hierbij en zorgt ervoor dat onze dienstverlening op een veilige maar flexibele manier bijdraagt aan de kwaliteit zonder de beschikbaarheid, integriteit, en vertrouwelijkheid uit het oog te verliezen. Hiermee is de missie en visie op informatieveiligheid:
Onze dienstverlening is professioneel, toonaangevend, transparant, en veilig voor gegevens van mensen, door mensen, vanuit een gezamenlijke organisatie waar het leuk is veilig professioneel en verantwoord te werken.

2. Strategisch beleid

2.1 Doel
Het doel van deze beleidsnota is het presenteren van het gezamenlijke 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2022 tot 2026'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen jaarplan informatiebeveiliging.

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 gericht op risicomanagement. Dat wil zeggen dat de lijnmanagers 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 A)
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.

2.2.3 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 en dus de implementatie van de BIO is de NEN-ISO/IEC 27001. De maatregelen worden op basis van ‘best practices‘ bij (lokale) overheden en NEN-ISO/IEC 27002 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek 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 ISO en de BIO.
Ook het Informatiebeveiligingsplan zal deze structuur volgen.
Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet, hiermee worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA), binnen het beveiligingsbeleid van de gemeente is ook ruimte voor de bescherming van PA en dit beleid betreft dan ook beleidsteams die zich met PA bezighouden.

2.3.1 Wettelijke basis
De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):
- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet 2017;
- Wet computercriminaliteit;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet / Archiefregeling;
- Databankenwet;
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer;
- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet openbaarheid bestuur (WOB) en opvolger Wet Openbare Overheid (WOO);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Basisregistratie grootschalige topografie (BGT);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet ruimtelijke ordening (WRO).

• NIS2

Op grond van bovenstaande wet- en regelgeving worden er eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) hierop.

2.4 Plaats van het strategisch beleid
Het strategisch beleid 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 'Gemeentelijk Informatiebeveiligingsjaarplan'.

2.5 Scope informatiebeveiliging
De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen (zowel in huis als SaaS (online) varianten), procesautomatisering, 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 BRP, PNIK en 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 het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd. Ondanks dat informatiebeveiliging nauw samenhangt met privacy en privacywetgeving, is dit niet opgenomen in dit strategisch informatiebeveiligingsbeleid. Voor privacy is een separaat strategisch beleid opgesteld. Het strategisch informatiebeveiligingsbeleid en het strategisch privacybeleid hebben als deelgebied relatie met het informatiebeleid.

2.6 De basis
Het bestuur, de directie, leidinggevenden (lijnmanagement) 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, of juist te accepteren 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, procesautomatisering en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene informatiebeleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

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 dit beleid zijn:
• Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college is eindverantwoordelijke voor de informatiebeveiliging.
• Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen ; sluizen ; en gemalen.
• De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en systemen die gebruikt worden door de gemeente hebben een interne (gege-

vens)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 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' 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 stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
• De directie / het management team stelt jaarlijks het informatiebeveiligingsplan vast.
• De directie / het management team is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
• De directie / het management team is verantwoordelijk voor het vragen om informatie bij de lijnmanagers en ziet erop toe dat de lijnmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie, informatiesystemen en procesautomatiseringsystemen 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 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 tevens worden opgenomen in de auditplannen.
• De lijnmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
• De lijnmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
• Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT, WOZ) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet méér 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.
• Lijnmanagers 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. Lijnmanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken, ondersteund door een ISO of de CISO.
• Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de lijnmanager en de betreffende medewerker in functionerings– en beoordelingsgesprekken.
• De BVO Rijn en Braassem is verantwoordelijk voor het aansturen van ketenpartners waar genomen beveiligingsmaatregelen worden beheerd (regievoering)
• De BVO Rijn en Braassem coördineert het gecontroleerd doorvoeren van wijzigingen op het gebied van informatiebeveiliging nadat deze zijn goedgekeurd door de CISO.
• De BVO Rijn en Braassem registreert en verwerkt de binnengekomen meldingen op het gebied van informatiebeveiliging en rapporteert periodiek naast reguliere incidenten ook de beveiligingsincidenten.
• De BVO Rijn en Braassem vormt samen met de CISO en ISO's de beveiligingsorganisatie voor gemeente Alphen aan den Rijn en Kaag en Braassem.
• De BVO Rijn en Braassem is verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk is.
• Het CISO zorgt in overleg met het bestuur en BVO voor de prioritering en aanpak van (beveiligingsgerelaterde) projecten via het projectportfolio en ziet toe op de juiste procesgang.

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 de CISO, gebaseerd op:
• de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
• het dreigingsbeeld gemeenten van de IBD;
• de door de lijnmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse.

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, en Information security officers (ISO)) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (in- of externe) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een lijnmanager. De directie zorgt dat de lijnmanagers 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 continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO en ISO's van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: lijnmanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle lijnmanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn (CISO en ISO's). 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. Lijnmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams /afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van de lijnmanagers in het kader van informatiebeveiliging zijn:
• Het leveren van input voor wijzigingen op maatregelen en procedures.
• Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
• Het binnen het eigen team bespreken van het beveiligingsbeleid, procedures, en incidenten
• Het periodiek controleren op correctheid van autorisaties
• Het registreren en periodiek rapporteren van beveiligingsincidenten aan de CISO (direct of indirect)
• 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 met CISO of ISO's.
• Het bepalen van de dataclassificatie en risico's van de bedrijfsinformatie waarvoor verantwoording wordt gedragen in overleg en met behulp van CISO, ISO's, en privacy officers.

3.3 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente. De bestuurders en directeuren van de gemeente 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.

3.3.1 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat een ENSIA-coördinator wordt benoemd. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke lijnmanagers. De lijnmanagers leveren tijdig alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten, waarbij zij de operationele werkzaamheden delegeren aan de betreffende medewerkers. Zij zorgen ervoor dat de betreffende medewerkers voldoende tijd krijgen om deze werkzaamheden te kunnen uitvoeren, en zijn aanspreekpunt voor de uiteindelijke resultaten in de verantwoording. Bij onvoldoende resultaten stemmen zij met de ENSIA coördinator af hoe de onvolkomenheden kunnen worden opgelost en leggen dit vast in een verbeterplan.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college 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 en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Vastgesteld op 25 april 2023 door het college van Alphen aan den Rijn,
De secretaris, de burgemeester.

Vastgesteld op 9 mei 2023 door het college van Kaag en Braassem,
De secretaris, de burgemeester.