gemeente Wijk bij Duurstede

GEMEENTEBLAD

Officiële uitgave van de gemeente Wijk bij Duurstede

Nr. 302124

4 juli

2022

Strategisch Informatiebeveiligingsbeleid Gemeente Wijk bij Duurstede 2021

1 Inleiding

Deze nota beschrijft het strategisch informatiebeveiligingsbeleid van de gemeente Wijk bij Duurstede vanaf 2021 en vervangt het vastgestelde informatiebeveiligingsbeleid van voorgaande jaren.
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 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). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG (zie www.informatiebeveiligingsdienst.nl).

1.1 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan:
'Het proces van vaststellen van de vereiste beveiliging van informatiesystemen alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Kernpunten daarbij zijn de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons) informatie.'

Informatiebeveiliging heeft betrekking op:

> **Alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, etc.).**
> **Alle mogelijke informatiedragers (papier, CD, DVD, foto, film, etc.).**

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 de leden van de gemeenteraad, het College van B&W, alle medewerkers van de gemeente, inwoners, gasten, bezoekers en externe relaties.

1.2 Ambitie en visie op het gebied van informatieveiligheid

De gemeente Wijk bij Duurstede 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 dienstverlening 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 directieteam) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teamleiders, 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 het strategisch informatiebeveiligingsbeleid vanaf 2021. Dit beleid wordt periodiek en in aansluiting bij de (bestaande) P&C-cycli en (externe) ontwikkelingen beoordeeld en zo nodig bijgesteld. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan.

2.2 Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid van de gemeente Wijk bij Duurstede zijn in onderstaande paragrafen beschreven.

2.2.1 De BIO
De Baseline Informatiebeveiliging Overheid (BIO) is vanaf 1-1-2020 het nieuwe normenkader voor de gehele overheid. De werkwijze van de BIO is gericht op risicomanagement, waarbij de voorgaande Baseline Informatiebeveiliging voor Gemeenten (BIG) gericht was op compliance. Risicomanagement is voor leidinggevenden dus leidend. Dit houdt in dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe 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 bestuurlijke aanvulling op het normenkader BIO. Deze principes helpen bestuurders om de juiste dingen te doen en gaan over waarden die de bestuurder zichzelf oplegt.

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

De principes gaan vooral over de rol van de bestuurder 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, partners van de gemeente en de dienstverlening aan deze partijen. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten (IBD)
Het dreigingsbeeld geeft een actueel zicht op dreigingen, risico's op het gebied van politiek & bestuur / inwoners & ondernemers / ambtelijk terrein en biedt een handelingsperspectief voor management en directie. 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 lokale incidenten en inbreuken op de beveiliging
De gemeente kent naast het hierboven genoemde dreigingsbeeld een 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 en voor het treffen van beveiligingsmaatregelen.

2.3 Standaarden informatiebeveiliging
De basis voor de inrichting van het strategische informatiebeveiligingsbeleid is de ISO27001/2. Beveiligingsmaatregelen worden genomen op basis van "best practices" bij (lokale) overheden en deze ISO-normen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek2 in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide ISO-normen. Deze BIO bestaat uit een baseline met verschillende niveaus voor het beveiligen van informatie.
Door de Informatiebeveiligingsdienst (IBD) worden er praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van risicoanalyses, voor het opstellen van een beveiligingsplan en diverse soorten beleidsstukken.

Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente Wijk bij Duurstede en de relevante landelijke en Europese wet- en regelgeving.

2.4 Plaats van strategische 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 de uitwisseling van gegeven met 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. Met verbonden partijen maken de samenwerkende gemeenten afspraken over maatregelen op het gebied van informatiebeveiliging en afstemming hierover met de gemeenten.

Dit strategisch gemeentelijke informatiebeveiligingsbeleid is een algemene basis en dekt ook de beveiligingseisen uit wetgeving af zoals voor de BRP, Reisdocumenten (PUN en PNIK), SUWI en DigiD. 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.

2.6 Uitgangspunten
Het bestuur, de gemeentesecretaris en lijnmanagement van de gemeente 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 Informatiebeveilgiing 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 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 tot systemen en/of gebouwen.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op informatiebeveiligingsincidenten.
- 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 de directie en de onderliggende lijn. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente

Wijk bij Duurstede 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.
- ✔ 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 de strategie.
- ✔ De directie 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 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 teamleiders 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.
- ✔ Teamleiders 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. Teamleiders 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 Teamleider Informatievoorziening, gebaseerd op:
  - ° de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - ° het dreigingsbeeld gemeenten van de IBD;

- ° de door de teamleiders 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 en 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)(zie figuur 1). 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: directieteam

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

3.2 Uitvoering: teamleiders

Informatiebeveiliging valt onder de verantwoordelijkheden van alle teamleiders. 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. Teamleiders rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams 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 teamleiders in het kader van informatiebeveiliging zijn:
- ✔ Het leveren van input voor wijzigingen op maatregelen en procedures.
- ✔ Het binnen het eigen thema 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.

Figuur 1
Toegepast wordt het principe van het '3-Lines of Defence' model. In dit 3LoD model hebben de verschillende spelers specifieke rollen en taken met betrekking tot informatiebeveiliging.

Rollen en Taken binnen het 3-Lines of Defence model		
1e lijn >> Directie, lijnmanagement, medewerkers	**2e lijn >> CISO en TISO [1], samenwerkend in een Information Securityteam**	**3e lijn >> Controller, auditor, FG**
Dagelijkse operatie • Voldoen aan beleid • Implementatie beleid • Inrichting processen • Maken werkbeschrijvingen • Inrichting techniek • Risico eigenaar **Borging** • Borging kennis • 1e lijn controles (controles eigen werk) • Inrichten functiescheiding	**Kader stellend** • Definiëren kader stellend beleid **Adviserend** • Ondersteunen 1e lijn **Toetsend** • Dagelijkse operatie toetsen aan beleid • Review operationeel beleid **Monitorend** • Control review • Risico assessments • Risico monitoring	**Onafhankelijke toetsing van 1e en 2e lijn m.b.t.** • Naleving beleid • Uitvoer processen • De realisatie van de maatregelen • De afhandeling van beveiligingsincidenten. **Onafhankelijk betekent** • Geen operationele verantwoordelijkheid • Geen beleidsmatige verantwoordelijkheid

3.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente. De bestuurders van de gemeente Wijk bij Duurstede 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 ENSIA

De gemeente Wijk bij Duurstede verantwoordt zich over informatiebeveiliging door middel van de ENSIA-systematiek. Het MT wijst een (regionale) ENSIA-coördinator aan. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teamleiders. De teamleiders 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. Door middel van 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 Wijk bij Duurstede informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

1) Technisch information security officer, ondergebracht bij de GR RID