RAADSMEMO

Aan
De gemeenteraad van Vlaardingen

Portefeuillehouder
K. Kegel

Onderwerp
Raadsmemo betreffende vaststelling Informatiebeveiligings- en Privacybeleid 2025-2028

Datum	Registratienummer	Aantal bijlagen
28 januari 2025	2014988	1

Geachte leden van de raad,

Dat we op een veilige en zorgvuldige manier moeten omgaan met informatie van onze inwoners, ondernemers en partners staat voor het college buiten kijf. Informatiebeveiliging gaat verder dan alleen maar regelgeving; het is het fundament van onze organisatie. Dat betekent dat wij moeten inspelen op toenemende cyberdreigingen en technologische ontwikkelingen die wij op ons af zien komen. Het college heeft daarom het nieuwe Informatiebeveiligings- en privacybeleid 2025 – 2028 vastgesteld.

Het geactualiseerde beleid biedt handvatten om in de periode 2025-2028 verder concrete invulling te geven aan het verbeteren van onze informatiebeveiliging. De ambitie van de gemeente Vlaardingen is om te zorgen dat de informatieveiligheid van haar informatievoorziening zodanig is ingericht dat de vertrouwelijkheid, integriteit en beschikbaarheid effectief en duurzaam gewaarborgd is. Hierdoor kan de dienstverlening aan onze inwoners, bedrijven, organisaties, ketenpartners ten allen tijde doorgaan en kunnen wij uitvoering blijven geven aan onze wettelijke taken.

In het nieuwe beleid geven we extra aandacht aan het borgen van bedrijfscontinuïteit, cybercrisisbeheersing en de beveiliging van informatieketens. We kiezen voor een risicogedreven aanpak waarbij we onze risico's goed in beeld hebben en daarop tijdig acteren. Met dit nieuwe beleid zijn we voorbereid op de eisen van de nieuwe Baseline Informatiebeveiliging Overheden (BIO 2.0) en Cybersecuritywet 2025. Ook is het beleid aangepast aan de onlangs ingevoerde Europese regelgeving, Network and Information security directive 2 (NIS2).

Door het geactualiseerde beleid zijn we goed voorbereid om de uitdagingen die op ons pad komen met vertrouwen aan te gaan.

Hoogachtend,

Burgemeester en wethouders van Vlaardingen,

de secretaris
drs. E. Stolk

de burgemeester
drs. B. Wijbenga - van Nieuwenhuizen

Informatiebeveiligings- en Privacybeleid gemeente Vlaardingen 2025 - 2028

Gemeente Vlaardingen

Status:

Openbaar

Gemeente Vlaardingen

Inhoud

Belangrijkste begrippen

AVG	– Algemene Verordening Gegevensbescherming – Privacywet
BIO	– Baseline Informatiebeveiliging Overheden
CIP	- Centrum Informatiebeveiliging en Privacybescherming
ENSIA	– Eenduidig Normenkader Single Information Audit
IBD	– Informatiebeveiligingsdienst VNG
ISMS	– Information System Security Management System
NCSC	– Nationaal Cybersecurity Centrum
NEN-ISO/IEC 27001/2	– Internationale norm voor informatiebeveiliging
NIS2	– Europese Network and Information Security richtlijn, uitvoeringswet Cybersecuritywet 2025 in NL
PDCA (-Cyclus)	– De controle cirkel van Deming: Plan Do Check Act
SaaS	– Software as a Service – “de cloud”
VNG	– Vereniging Nederlandse Gemeenten
WPG	– Wet Politiegegevens

Gemeente Vlaardingen

1. Inleiding

Deze beleidsnota beschrijft het Informatiebeveiligings- en privacy beleid (IB&P beleid) voor de jaren 2025 tot 2028 en vervangt het in 2020 vastgestelde 'Strategisch Informatiebeveiligingsbeleid 2020-2023'.

Dit beleid is richtinggevend en kaderstellend voor onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Informatiebeveiligings- en Privacybeleid 2025-2028' 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 dit beleid is de NEN-ISO/IEC 27002:2022 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO zie Bijlage 1) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens, zie hoofdstuk 2.

Wettelijke grondslag(en) of bevoegdheid waarop dit beleid is gebaseerd: https://bio-overheid.nl.

Tussentijdse evaluatie

Een tussentijdse evaluatie van dit beleid op hoofdlijnen zal plaatsvinden in het eerste kwartaal van 2027. Hierbij zal getoetst worden of het kader nog voldoende aansluit met de dan actuele ontwikkelingen en inzichten rondom de Cybersecuritywet 2025 en de BIO 2.0 en of aanpassing derhalve noodzakelijk is.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit beleid. Tactische en operationele aspecten van informatiebeveiliging en privacy worden verder uitgewerkt en geconcretiseerd in afzonderlijke informatiebeveiligings- en privacy plannen. Dit wordt gedaan op basis van input van de teammanagers uit het I-Domein, de Chief Information Security Officer (CISO), de Concern Controller en Functionaris Gegevensbescherming (FG)), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's.

Hoofdstuk 3 beschrijft 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 (persoons)gegevens 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.

Belangrijk om te noemen is dat de menselijke factor en hiermee het gedrag een steeds grotere en fundamentele rol speelt in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk.

Vier kernpunten van informatiebeveiliging zijn:

- **Beschikbaarheid (of continuïteit):** 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 (juistheid), volledigheid, tijdigheid van informatie en informatieverwerking, oftewel het in overeenstemming zijn van informatie met de werkelijkheid.
- **Vertrouwelijkheid:** het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe bevoegd en geautoriseerd zijn.
- **Controleerbaarheid:** waarborgen dat de beoogde toegang tot gegevens en de juiste werking van systemen continu alsook achteraf te controleren is.

Informatiebeveiliging beperkt zich niet alleen tot ICT of technische maatregelen. Het heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.4 Ambitie en visie

1.4.1 Visie

De gemeente Vlaardingen streeft naar een veilige en vertrouwelijke informatievoorziening waarin de bescherming van informatie en privacy centraal staat. De visie van de gemeente Vlaardingen is gebaseerd op het idee dat elke gebruiker van de informatievoorzieningen (intern en extern) moet kunnen rekenen op een robuuste, proactieve en betrouwbare bescherming. In het licht van toenemende cyberdreigingen en technologische ontwikkelingen erkent de gemeente Vlaardingen de noodzaak te streven naar continue verbetering van de informatiebeveiliging om te kunnen blijven anticiperen op nieuwe risico's en adequaat te kunnen reageren op incidenten. De betekenis van informatiebeveiliging gaat voor de gemeente Vlaardingen dan ook verder dan het naleven van regelgeving alleen; het behoort een fundament te zijn en daarmee een onlosmakelijk onderdeel van de organisatie.

1.4.2 Ambitie

De ambitie van de gemeente Vlaardingen is om te zorgen dat de informatieveiligheid van haar informatievoorziening zodanig is ingericht dat de vertrouwelijkheid, integriteit en beschikbaarheid effectief en duurzaam gewaarborgd is. Hierdoor kan de gemeente een ongestoorde dienstverlening verzorgen aan burgers, bedrijven, organisaties, ketenpartners en bezoekers en geeft daarmee tevens continuïteit aan de uitvoering aan haar wettelijke taken.

Om dit te bepalen maken we hierbij gebruik van het BIO-SA model van het Centrum Informatiebeveiliging en Privacybescherming (CIP)[1] dat vijf volwassenheidsniveaus uitdrukt en onderscheid. Op basis van dit model werken we stapsgewijs toe naar een hoger volwassenheidsniveau waarbij uiteindelijk het doel is dat we informatieveiligheid effectief en efficiënt hebben geborgd hebben binnen onze werkprocessen en dit meetbaar is. Het CIP vertaalt de wetgeving op het gebied van informatieveiligheid en privacy naar concrete, hanteerbare normen die duidelijk aangeven wat organisaties dienen te regelen in hun beveiligingsbeleid, de uitvoering en de controle erop.

Figuur 1 - BIO-SA onderscheidt vijf niveaus (levels) van volwassenheid

We ambiëren een volwassenheidsniveau van informatieveiligheid waarbij we volledig 'in control' zijn. Een organisatie is 'in control' als een organisatie zodanig is ingericht dat er wordt gestuurd op resultaten zodat (indien nodig) bijgestuurd kan worden om zo de doelstellingen te realiseren. Momenteel verschilt het volwassenheidsniveau van de gemeente Vlaardingen per proces, afdeling of systeem. Hierbij heeft de gemeente niet altijd de volledige controle en is zij afhankelijk van de medewerking van ketenpartners.

Door de complexiteit van sommige processen is hiervoor het uitgangspunt van de gemeente Vlaardingen om in 2026 van niveau 2.6 (meting juni 2024) naar minimaal niveau 3 gegroeid te zijn.

[1] https://www.cip-overheid.nl/media/o0bpu3x3/de-16-criteria-van-de-bio-sa-v10.pdf

Hiervoor is een gecoördineerde en gestructureerde aanpak noodzakelijk zodat we uiteindelijk proactief op ontwikkelingen kunnen anticiperen.

Getroffen maatregelen dienen daarbij continu te worden geëvalueerd en indien nodig geactualiseerd. De eerste evaluatie zal plaatsvinden in het eerste kwartaal van 2026. Afhankelijk van de herijking van onder andere de Cybersecuritywet 2025 en de BIO2.0 en de dan gestelde eisen zal het ambitieniveau worden bijgesteld om te kunnen komen tot volwassenheidsniveau 4.

Daarbij gaat het om intern beleid, normen en procedures, en anderzijds om de technische en organisatorische maatregelen, zoals heldere verantwoordelijkheden en bewustwording van medewerkers. Hierbij realiseren we ons dat 100% beveiliging tegen cybercriminaliteit altijd een onmogelijke opgave zal blijven. Met het treffen van gerichte maatregelen proberen we beveiligingsincidenten zoveel mogelijk te voorkomen en eventuele gevolgen te minimaliseren.

Gemeente Vlaardingen

2. Beleid

2.1 Strategische doelen

Het doel van deze beleidsnota is om op strategisch niveau richting te geven aan de ambtelijke organisatie en de onderliggende tactische plannen op het gebied van informatiebeveiliging- en privacy voor de jaren 2025 tot 2028.

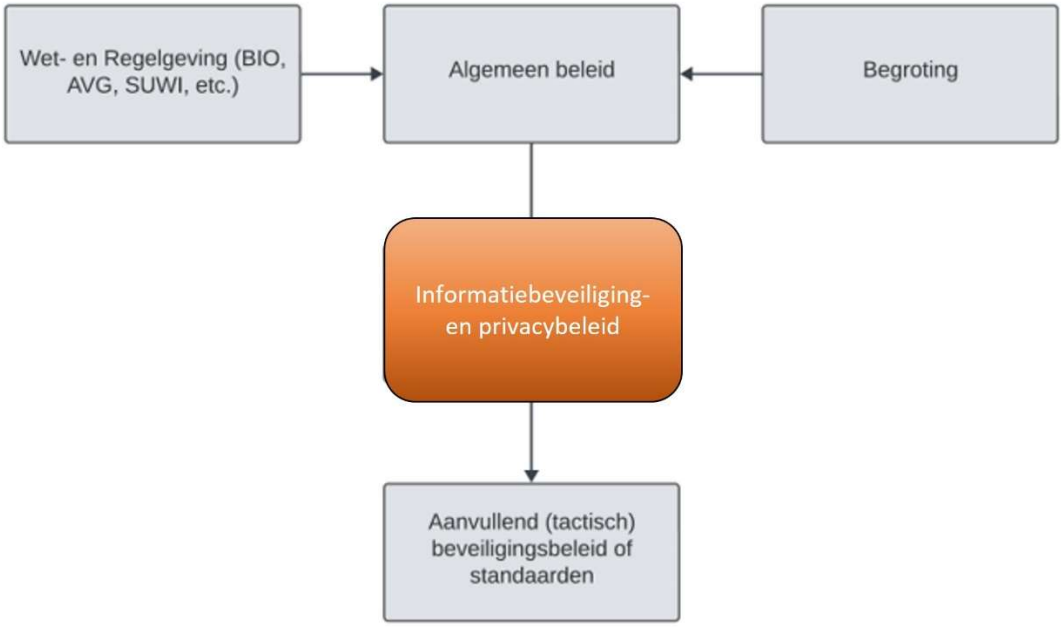
De strategische doelen van het IB&P beleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het sturen op en toepassen van dataminimalisatie.
- 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.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en andere relevante wetgeving en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in een jaarlijks bij te stellen informatiebeveiligings- en privacy plan. Het beleid op informatiebeveiliging en privacy biedt ondersteuning aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2 Plaats van het beleid

Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Het beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en geeft daarmee richting voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau.



Figuur 2 - Visualisering en indruk van de positie van het informatiebeveiliging- en privacy beleid

In een breder kader geeft dit informatiebeveiligingsbeleid sturing aan alle informatiebeveiligingsaspecten van het I-Beleid van de gemeente Vlaardingen.

2.3 Risico's

Onze gemeente digitaliseert net als de samenleving om ons heen. Zodoende is informatiebeveiliging een onderwerp dat steeds belangrijker wordt. Inwoners en partijen waar wij mee samenwerken willen snel en digitaal geholpen worden maar daarmee nemen moderne en digitale dreigingen alsmaar toe. Het IBD brengt periodiek in kaart wat de actuele, meest belangrijke risico's zijn op het gebied van gemeentelijke informatiebeveiliging. In het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023-2024[2] wordt ingegaan op deze risico's.

De belangrijkste risico's zijn volgens het IBD als volgt:

- **Uitval van dienstverlening en bedrijfsvoering:** als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering.
- **Vertrouwelijke informatie in verkeerde handen:** onterechte toegang tot gevoelige informatie kan uiterst nadelig uitvallen voor inwoners en ondernemers
- **Fouten in de dienstverlening:** informatiebeveiligingsincidenten kunnen leiden tot fouten in dienstverlening. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

[2] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

Aanvullend op de genoemde risico's valt het IBD in het bijzonder drie soorten dreigingen op:

- **Meer Ransomware, met destructievere gevolgen:** aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger.
- **Steeds meer en ernstiger kwetsbaarheden in software:** kwetsbaarheden met een hoge kans op misbruik en ernstige gevolgen komen in de afgelopen jaren relatief steeds vaker voor.
- **Gevaren in ketens uit het zicht:** als gemeente neem je deel aan veel samenwerkingsverbanden. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico's als taken zijn uitbesteed.

Aanvullend op bovengenoemde bekende risico's voeren we als gemeente een eigen registratie waarin incidenten worden vastgelegd. Deze registratie geeft waardevolle informatie om van te leren en zodoende zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van beleid en procedures.

Als gemeente verhogen we onze weerbaarheid door ons te wapenen tegen de toenemende geprofessionaliseerde dreiging. Waarbij ook het softwarelandschap en hiermee onze ICT-infrastructuur aan verandering onderhevig is. Steeds meer applicaties verhuizen van een in huis geïnstalleerde applicatie naar extern gehoste Software as a Service (SaaS) oplossingen. Dataverwerking is meer en meer in de Cloud, wat wil zeggen dat applicaties extern bij andere organisaties op de servers staan. Voor ons als gemeente is het belangrijk hier regie op te houden en ervoor te zorgen dat informatieveiligheid altijd vanaf het begin bij vernieuwingen en veranderingen, zowel bij systemen als beleid en processen, meegenomen wordt (security by design). Daarnaast controleren en beoordelen we partners actief. Dit geldt ook, zoals het IBD benadrukt, voor ketenpartners waar wij als gemeente mee samenwerken.

Ook de ontwikkeling van het tijd- en plaats onafhankelijk werken heeft voor nieuwe risico's gezorgd. Er worden steeds meer mobiele apparaten gebruikt met gevoelige data en er wordt op verschillende, soms openbare, plekken gewerkt. Dit vergt goede afspraken met onze medewerkers. Afhankelijk van de gevoeligheid van informatie wordt bepaald welke maatregelen moeten worden getroffen wanneer gegevens benaderbaar zijn vanaf een locatie buiten de gebouwen van de gemeente.

Tot slot zijn er meer maatschappelijke ontwikkelingen en innovaties binnen de gemeente en haar ketenpartners. Zo is er steeds meer aandacht voor data gedreven werken, het gebruikmaken van algoritmes en kunstmatige intelligentie. Voor dergelijke ontwikkelingen creëren we een visie om hier goed, efficiënt en veilig mee om te gaan.

De ontwikkelingen die van belang zijn voor de actualisering van het IB&P beleid zijn de volgende:

2.4 Ontwikkelingen

2.5.1 Regionale samenwerking

VeiligheidsAliantie Regio Rijnmond

De VAR kan door samenwerking haar weerbaarheid versterken met als doel te voorkomen dat er misbruik of oneigenlijk gebruik wordt gemaakt van de informatiestructuren in de Regio Rijnmond. De thema's en ambities die de VAR hiervoor nastreeft zijn te vinden op https://veiligheidsalliantie.nl/

Samenwerking binnen de VAR raakt niet alleen informatiebeveiliging, maar ook integrale veiligheid.

2.5.2 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het 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 leidend. 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.

Bij herziening of actualisatie van overheidswege van de BIO zal de meest recente versie onverkort van toepassing zijn en opgenomen worden in de Bijlage A waarbij de huidige versie zal vervallen.

2.5.2 De 10 principes voor informatiebeveiliging[3]

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.

2.5.3 Network and Information Security Directive (NIS2)

De Network and Information Security Directive (NIS2-richtlijn)[4] is gericht op versterking van de digitale en economische weerbaarheid van Europese lidstaten. Gemeenten gelden hierbij als 'essentiële entiteit'. De NIS2-richtlijn richt zich op digitale (cyber) risico's voor netwerk- en informatiesystemen. NIS2 kent een aantal verplichtingen: zorgplicht, meldplicht, registratieplicht en toezicht.

3 https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

4 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

2.5.4 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Vlaardingen is zich hiervan bewust en wil daarom met dit beleid aangeven hoe in algemene zin invulling wordt gegeven aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG)[5].

2.5.5 Kunstmatige Intelligentie (AI)

Artificial Intelligence wordt op steeds meer terreinen ingezet. Het kan bijdragen aan het oplossen van maatschappelijke vraagstukken, kan de productiviteit verhogen en de werkgelegenheid stimuleren. Tegelijkertijd zijn er ook risico's aan verbonden voor publieke waarden en mensenrechten. Om de kansen van AI te kunnen benutten en daarnaast goed voorbereid te zijn op de risico's van AI-toepassingen is kennisuitwisselingen en beleidsafstemming nodig. Het gemeentelijke beleid omtrent de inzet van AI is in een apart beleidsdocument uitgewerkt.

2.5.6 De WPG

De gemeente heeft buitengewoon opsporingsambtenaren (BOA's) in dienst. Zij verwerken naast gegevens die onder de AVG vallen ook gegevens die vallen onder de wet Politiegegevens (WPG)[6]. Hiervoor moet de gemeentebeleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

2.5.7 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[7] van de Informatiebeveiligingsdienst (IBD) geeft zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld wordt gebruikt om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging. Het dreigingsbeeld wordt jaarlijks geactualiseerd.

2.5.8 Beveiligingsadviezen Nationaal Cyber Security Centrum (NCSC)

Beveiligingsadviezen[8] die door het NCSC worden gepubliceerd naar aanleiding van een recent gevonden kwetsbaarheid of geconstateerde dreiging. Beveiligingsadviezen beschrijven de mogelijke gevolgen en mogelijke oplossingen van een kwetsbaarheid of dreiging.

2.5.9 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente gebruikt naast het hierboven genoemde dreigingsbeeld ook systemen waarin incidenten worden vastgelegd. Deze systemen geven ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

[5] https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort
[6] https://wetten.overheid.nl/BWBR0022463/2023-11-01
[7] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/
[8] https://advisories.ncsc.nl/advisories

2.6 Standaarden informatiebeveiliging

De BIO is gebaseerd op de recentst geldende versie van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002. 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. De inhoud en structuur van deze beleidsnota is afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen. Bij vernieuwing van de BIO zal telkens de meest recente versie worden aangehouden.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsteams die zich met PA bezighouden. Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn[9] (CSIR).

2.7 Scope informatiebeveiliging en privacy

De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, 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 gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Tevens wordt ingehaakt op de Nederlandse Cybersecuritywet welke in 2025 actief zal zijn. Hiermee is dit beleid toekomstgericht ook in lijn met de Europese NIS2 richtlijn. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld AVG, SUWI, gemeentelijke basisregistraties en DigiD met norm B.01 eisen). Deze worden in aanvullende beleidsdocumenten geformuleerd.

Bewust wordt in het beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het beleid gelegd.

2.8 Uitgangspunten

Het bestuur, het CDT en het teammanagement spelen een cruciale rol bij het uitvoeren van dit IB&P beleid. Het teammanagement maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de (privacy) risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Het gehele gemeentelijke management geeft richting aan informatiebeveiliging en privacy en laat zien dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt. Dit gebeurt door het actief uitdragen en handhaven van het IB&P beleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en

[9] https://www.cert-wm.nl/csir

(persoons)gegevens(verzamelingen). Dit beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.8.1 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Vlaardingen hebben een interne (proces)eigenaar die de vertrouwelijkheid, privacy eisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie en ketens van informatiesystemen ligt dan ook bij de eigenaar van de informatie;
- Door periodieke controle, planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met de tactische informatiebeveiliging- en privacy plannen het fundament onder een betrouwbare informatievoorziening en privacybescherming. In deze plannen wordt de betrouwbaarheid van de informatievoorziening en privacy organisatie breed benaderd. De plannen worden periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy;
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. '**Plan, do, check en act**' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming;
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid;
- Regels en verantwoordelijkheden voor het IB&P beleid dienen te worden vastgelegd en vastgesteld;
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken;
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, 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.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan

bij dat medewerkers hiertoe in staat zijn. Hiertoe worden onder meer E-learnings ter beschikking gesteld en trainingen gegeven welke jaarlijks verplicht worden gesteld.
- Informatiebeveiliging en privacybescherming maakt deel uit van de ontwikkelingsbeoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.8.2 Randvoorwaarden

Randvoorwaarden zijn de eisen waaraan moet worden voldaan om het IB&P beleid uit te kunnen voeren. Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek zowel technisch als organisatorisch geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt het informatiebeveiligings- en privacy plan opgesteld onder leiding van het hoofd informatiebeveiliging, gebaseerd op:
- Dit IB&P beleid;
- De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
- Andere audit resultaten van veiligheidsonderzoeken, penetratietests, kwetsbaarheidsanalyses;
- Het dreigingsbeeld gemeenten van de IBD;
- Uitkomsten risicoanalyse en DPIA's;
- De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).
- Om uitvoering te kunnen geven aan dit beleid en het IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

Gemeente Vlaardingen

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt op hooflijnen uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense').

1. In dit model is het lijnmanagement in de eerste lijn verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen;
2. In de tweede lijn bewaken de Security Officers en Privacy Officers, of het lijnmanagement zijn verantwoordelijkheden ook daadwerkelijk neemt. Zij adviseren en ondersteunen het lijnmanagement met het coördineren van maatregelen;
3. In de derde lijn wordt het geheel door een (interne) auditor, CISO en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier is ook de ENSIA-coördinator gepositioneerd.

3.1 College van B&W

De eindverantwoordelijkheid ten aanzien van alle informatie en informatiesystemen ligt bij het college van B&W, de Burgemeester (bij taken in het kader van handhaven Openbare Orde en Veiligheid) of de gemeenteraad. De eindverantwoordelijkheden zijn benoemd in het register van verwerkingen. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.

3.2 Aansturing: Concern Directieteam (CDT)

Het CDT zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. Het CDT zorgt dat de teammanagers zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het CDT zorgt dat de eindverantwoordelijke portefeuillehouder(s) binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het CDT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het CDT draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacy beleidsonderwerpen en laat zich hierin bijstaan door de CISO en FG/privacy officer van de gemeente. Het CDT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de gemeente Vlaardingen gezien als een integraal onderdeel van risicomanagement.

3.2.1 Taken en Verantwoordelijkheden van het CDT

- Het CDT stelt jaarlijks de tactische informatiebeveiligings- en privacy plannen vast.
- Het CDT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit beleid.
- Het CDT is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.

3.3 Uitvoering: Teammanagers

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. De verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, (persoons)gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teamleiders rapporteren aan het CDT over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal jaarlijks het onderwerp informatiebeveiliging en privacy te bespreken in het bedrijfsvoeringsoverleg.

3.4 Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het CDT, voorafgaand aan de P&C-gesprekken.

3.5 Functionaris Gegevensbescherming (FG)

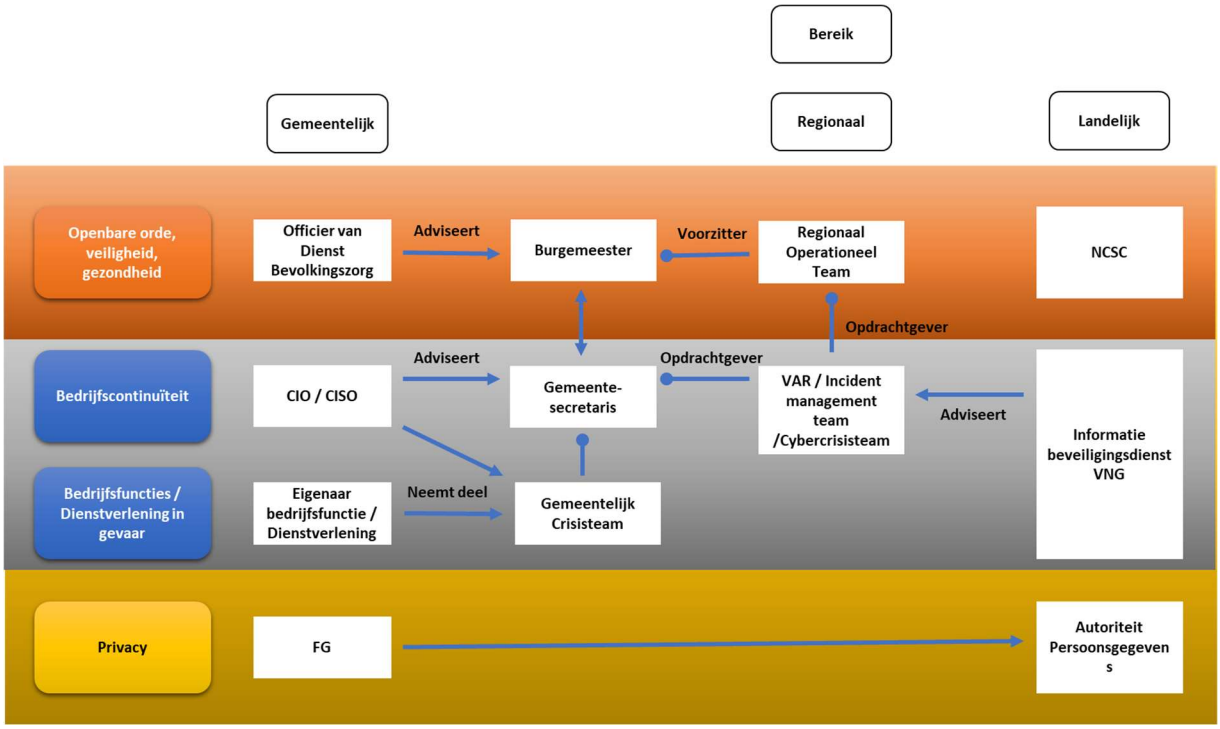
De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.

Het CDT en de teammanagers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de Functionaris Gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de Functionaris Gegevensbescherming.

3.6 ICT-crisisbeheersing en samenwerking

Voor interne crisisbeheersing is er een crisisteam geïnstalleerd. Dit crisisteam bestaat in ieder geval uit: de gemeentesecretaris of gedelegeerde functionaris (CIO/CTO), de CISO en proceseigena(a)r(en) of teammanager(s). Op basis van de aard van het incident wordt het crisisteam uitgebreid met de PFO/Burgermeester, teammanagers uit het I-Domein, communicatie, personen met relevante expertise en/of de CISO’s van de andere mogelijk betrokken deelnemende gemeenten uit de regio. Bij afwezigheid wordt er een plaatsvervanger aangesteld binnen de eigen organisatie en/of kan er een beroep worden gedaan op de expertise vanuit de regio.

In het geval van regionale crisisbeheersing borgt de gemeente Vlaardingen zich middels een mandaatbesluit als deelnemende organisatie binnen de regionale samenwerking tot de afbakening van taken en bevoegdheden van de voorzitter van het regionaal incidentbestrijdingsteam. Dit is vastgelegd in een lokale en regionale ICT-crisis procedure.



Figuur 3 - Regionale verdeling verantwoordelijkheden op basis van classificatie en bereik naar interne organisatie

3.7 Controle en verantwoording

Dit Informatiebeveiligings- en Privacybeleid is een verantwoordelijkheid van het bestuur van de gemeente Vlaardingen. De bestuurders en directie van de gemeente Vlaardingen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van (persoons-)gegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie. Het CDT is, al dan niet bij monde van de CISO, verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. Het CDT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit beleid.

3.7.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dit betekent dat er een ENSIA-coördinator is 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. Via ENSIA verantwoordt de gemeente zich ook aan de toezichthouders van de stelsels waaronder DIGID/BAG/BGT/BRO/SUWI.

Om te beoordelen of de organisatie zijn informatiebeveiligingsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke audits en controles uitgevoerd. Bij een audit toetst een onafhankelijke deskundige partij op de opzet, bestaan en werking van beheersmaatregelen. Hiervoor wordt doorgaans een externe partij ingeschakeld. Deze diverse interne en externe audits uitgevoerd bieden input voor het actieplan zoals genoemd onder stap twee van de PDCA-cyclus. Als resultaat van de audit kunnen eventuele zwakheden in de beveiliging ontdekt worden en dit kan tot gevolg hebben dat er aanpassingen noodzakelijk zijn in het beveiligingsbeleid.

3.7.2 Overige audits en controles

Naast de ENSIA en overige audits zijn er meer controles. Zo wordt informatiebeveiliging als onderdeel van de accountantscontrole meegenomen, maar kan er ook sprake zijn van een Rekenkameronderzoek. Als onderdeel van de informatiebeveiliging jaarplan worden verschillende controles of onderzoeken uitgevoerd op onderwerpen als autorisatiebeheer en toegangscontrole. Ook controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel en input voor het actieplan. Ten slotte leren we van incidenten door deze zorgvuldig te registreren en te evalueren.

3.7.3 AVG

Burgemeesters en wethouders leggen verantwoording af aan de gemeenteraad over het naleven van de privacywet (AVG).

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

Ondertekening

Vastgesteld op d.d.

Burgemeester en wethouders van de gemeente Vlaardingen,

Gemeente Vlaardingen

BIJLAGE 1 - Overzicht tactische uitwerking BIO maatregelen

BIJLAGE 2 - Lokale Governance

BIJLAGE 3 - Overige Governance