GEMEENTE ZUNDERT

GEMEENTEBLAD

Officiële uitgave van de gemeente Zundert

Nr. 23103

18 januari 2023

Strategische informatiebeveiligingsbeleid

Het college van burgemeester en wethouders van de gemeente Zundert;

gelezen het bepaalde in:
- artikel 4:81 van Algemene wet bestuursrecht;
- artikel 1.11,eerste lid, van de Wet Basisregistratie Personen;
- artikel 6 van het Besluit Basisregistratie Personen;
- artikel 90 van de Paspoortuitvoeringsregeling Nederland;
- artikel 62 van de Wet structuur uitvoeringsorganisatie werk en inkomen;
- control 5.1.1 van de Baseline Informatiebeveiliging Overheid;

besluit:

1. Vast te stellen de beleidsregels "strategische informatiebeveiligingsbeleid".

Inleiding

We leven in een samenleving waarin informatie door alle technologische ontwikkelingen steeds vaker digitaal wordt vastgelegd en gedeeld. De gemeente werkt vaak en veelvuldig met waardevolle en privacygevoelige (digitale) informatie. Informatie is nooit 100% veilig, er is altijd risico. Er zijn verschillende invloeden en factoren die de informatieveiligheid kunnen beïnvloeden. Het is dus heel belangrijk om te sturen op een zo veilig mogelijk informatiegebruik binnen onze organisatie en informatie niet zomaar te delen met externe partijen. Informatiebeveiliging (IB) en het nemen van beheersmaatregelen om de risico's te beperken zijn daarbij leidend.

De gemeente Zundert wil een betrouwbare organisatie zijn voor haar inwoners, ondernemers, partners en medewerkers. Zorgvuldig omgaan met (persoons) gegevens staat bij ons om die reden hoog in het vaandel. Voorheen werden (persoons)gegevensbescherming en IB los van elkaar georganiseerd. Maar er zijn veel raakvlakken tussen beiden; we kunnen gegevens alleen beschermen wanneer IB op orde is. Daarom werken we vanuit een integraal beveiligingsbeleid. We dragen zorg voor een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening en -bescherming aantoonbaar te waarborgen. Het integrale IB-beleid geldt voor de gehele informatievoorziening; op de gehele organisatie, alle processen, objecten, informatiesystemen, procesautomatisering en gegevens(verzamelingen) van de gemeente. Ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Informatiebeveiliging beperkt zich niet tot ICT. Het is ook van toepassing op de op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

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 [1] (juistheid) en vertrouwelijkheid van persoonsgegevens en andere organisatie essentiële- kritische en strategische informatie.
Het IB-beleid 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.

Strategisch informatiebeveiligingsbeleid

Visie
Zundert is een betrouwbare klantgerichte en dienstverlenende gemeente. Onze organisatie verwerkt gegevens en informatie van inwoners, ondernemers, medewerkers, partners en andere betrokkenen veilig, vertrouwelijk en daarmee zorgvuldig. Privacy wordt te allen tijde beschermd. Door het borgen van IB toont de gemeente haar betrouwbaarheid.

Deze betrouwbaarheid maken we concreet door de volgende uitgangspunten:
- De gemeente leeft wet- en regelgeving na.
- De gemeente levert continuïteit in dienstverlening en bedrijfsvoering.

1) Juistheid, volledigheid en tijdigheid

- De gemeente zorgt voor effectief risicobeheer.
- De gemeente blijft leren en verbetert continu haar processen.
- De gemeente genereert vertrouwen in haar informatieverwerking- en deling.
- De gemeente leidt haar medewerkers op om zorgvuldig met gegevens om te gaan.

Strategie
We verbinden verschillende aandachtsgebieden op het gebied van beveiliging, vanuit één strategische visie. Dit integrale beleid maakt dat we efficiënt en eensluidend jaarplannen kunnen formuleren en verantwoorden. Door dit jaarlijks te doen, blijven we flexibel en kunnen we inspelen op actuele situaties en ontwikkelingen. Het werken in overeenstemming met de geldende wet- en regelgeving (compliance) blijft belangrijk, maar wordt voorzien van een 'blik vooruit'. Het beleid legt meer dan voorheen de nadruk op het uitvoeren van risicoanalyse.

Om de betrouwbare gemeente uit de visie te worden, werken we vanuit een strategie die is geënt op twee pijlers. De eerste pijler is het kiezen voor een beleid van 'bewust risico nemen' in plaats van 'onbewust risico lopen'. Dat uit zich in een verschuiving van reactief naar preventief beleid. Tot waar zijn de risico's acceptabel en beheersbaar? Het uitvoeren van risicoanalyses vindt plaats op basis van proportionaliteit; in eerste instantie wordt een quickscan (pre-DPIA) uitgevoerd. Als uit deze quickscan blijkt, dat een verwerking een hoog risico voor de betrokken heeft, wordt een Data Protection Impact Assessments (DPIA's) uitgevoerd. Het beschrijven en bepalen van de informatiebeveiligingsrisico's en maatregelen vormen hiervan een onderdeel.

De tweede pijler wordt vormgegeven door onze ambities omtrent de volwassenheidsladder van betrouwbaarheid, zoals deze is vastgesteld door de Vereniging Nederlandse Gemeenten (VNG) voor privacy en informatiebeveiliging. Het zogenaamde 'Capability Maturity Model' (CMM) – oftewel het Volwassenheidsniveau-model – is een algemeen gebruikt model dat aangeeft op welk niveau de ontwikkeling van een organisatie zit.

Volwassenheidsniveau (CMM)		
Geoptimaliseerd	5	Beleid wordt tot op het laagste niveau correct geïnterpreteerd en uitgevoerd. Systematische procesverbetering o.b.v. metingen is onderdeel geworden van de bedrijfsvoering.
Beheerst en meetbaar	4	Het beleid wordt gedragen door de organisatie en de bevoegdheden zijn belegd. Hoge awareness en bijsturing van beheersmaatregelen o.b.v. periodieke kwantitatieve analyse en evaluaties
Gedefinieerd proces	3	De belangrijkste processen zijn gestandaardiseerd, gedefinieerd en voorzien van bijpassende beheersmaatregelen. Procesverbetering vindt plaats o.b.v. een kwalitatieve analyse.
Herhaalbaar, maar intuïtief	2	Er is algemeen beleid of beleid voor belangrijke delen, maar niet noodzakelijk formeel vastgelegd. Er zijn beheersmaatregelen, maar risico's zijn niet overal afgedekt en gedocumenteerd.
Ad hoc / initieel	1	Processen en verantwoordelijkheden zijn niet gedefinieerd en slecht beheersbaar. Problemen worden pas opgelost als ze zich voordoen.

Vanuit de Equalit-share geldt de gezamenlijke ambitie om alle deelnemende gemeenten voor wat betreft de borging van informatiebeveiliging per eind 2024 op volwassenheidsniveau 3 te hebben. Op volwassenheidsniveau 3 vinden de werkzaamheden in herhaalbare en beheerste processen plaats, nemen de processen de inwoner (klant) als uitgangspunt en zijn deze processen gebaseerd op een organisatie breed formeel vastgestelde werkwijze (gestandaardiseerd). Dit sluit aan op het programma "Dienstverlenend en Betrokken Zundert".

Doelstelling
De gemeente Zundert heeft dienstverlening tot een speerpunt gemaakt en daarmee een klantgerichte focus op het leveren van producten, diensten en participatie in de samenleving. Om een dienstverlenende en klantgerichte organisatie te ondersteunen, sluit het doel van IB hierop aan door het waarborgen van de betrouwbaarheid van de informatie(systemen) van onze gemeente. Het normenkader waar de gemeente op het gebied van IB aan moet voldoen is de Baseline Informatiebeveiliging Overheid (BIO). De BIO helpt proceseigenaren in de organisatie bij het nemen van hun verantwoordelijkheid in IB. Vanuit de BIO is een aantal eisen opgelegd waar de gemeente zorg voor moet dragen, naast het opstellen van dit IB-beleid en de organisatie ervan. De norm vanuit de BIO is dat iedere gemeente maatregelen moet nemen om hieraan te voldoen.

Naast deze hoofddoelstelling zijn ook onderstaande nevendoelstellingen geformuleerd:
- Alle medewerkers zetten zich bewust in op het verzorgen van een betrouwbare informatievoorziening voor onze burgers, ondernemers, ketenpartners en onze eigen organisatie.
- Onze gemeentelijke processen zijn ingericht om de betrouwbaarheid van het leveren van producten en diensten te borgen.
- Onze informatiesystemen en fysieke werkruimten en de daarin aanwezige gegevens worden beschermd tegen het al dan niet opzettelijk aanrichten van schade.

Het doel van het strategisch informatie beveiligingsbeleid kan als volgt worden omschreven: "het borgen van de betrouwbaarheid van de informatievoorziening en voldoen aan de vigerende normen-, wettelijke- en beleidskaders."

Scope
De scope van het IB-beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen en het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Randvoorwaarden
Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is. Daarnaast is het streven om transparant en proactief verantwoording af te leggen aan burgers en raadsleden en met minimale middelen maximale resultaten te behalen. Een betrouwbare informatievoorziening is hierbij een kritische succesfactor voor de bedrijfsvoering en de dienstverlening van de gemeente en de basis voor het beschermen van de rechten van inwoners en ondernemingen. Hiervoor is borging van de volgende kwaliteitsaspecten noodzakelijk:

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname door onbevoegden, door deze alleen toegankelijk te maken voor degenen die hiertoe expliciet worden geautoriseerd.
- Integriteit: het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking, door mutaties van onbevoegden te voorkomen.

Net als alle gemeenten in Nederland zijn we als uitvoeringsorganisatie gebonden aan bepaalde (beleids-)kaders welke voortkomen uit wet- en regelgeving. De wettelijke kaders zijn onder andere:

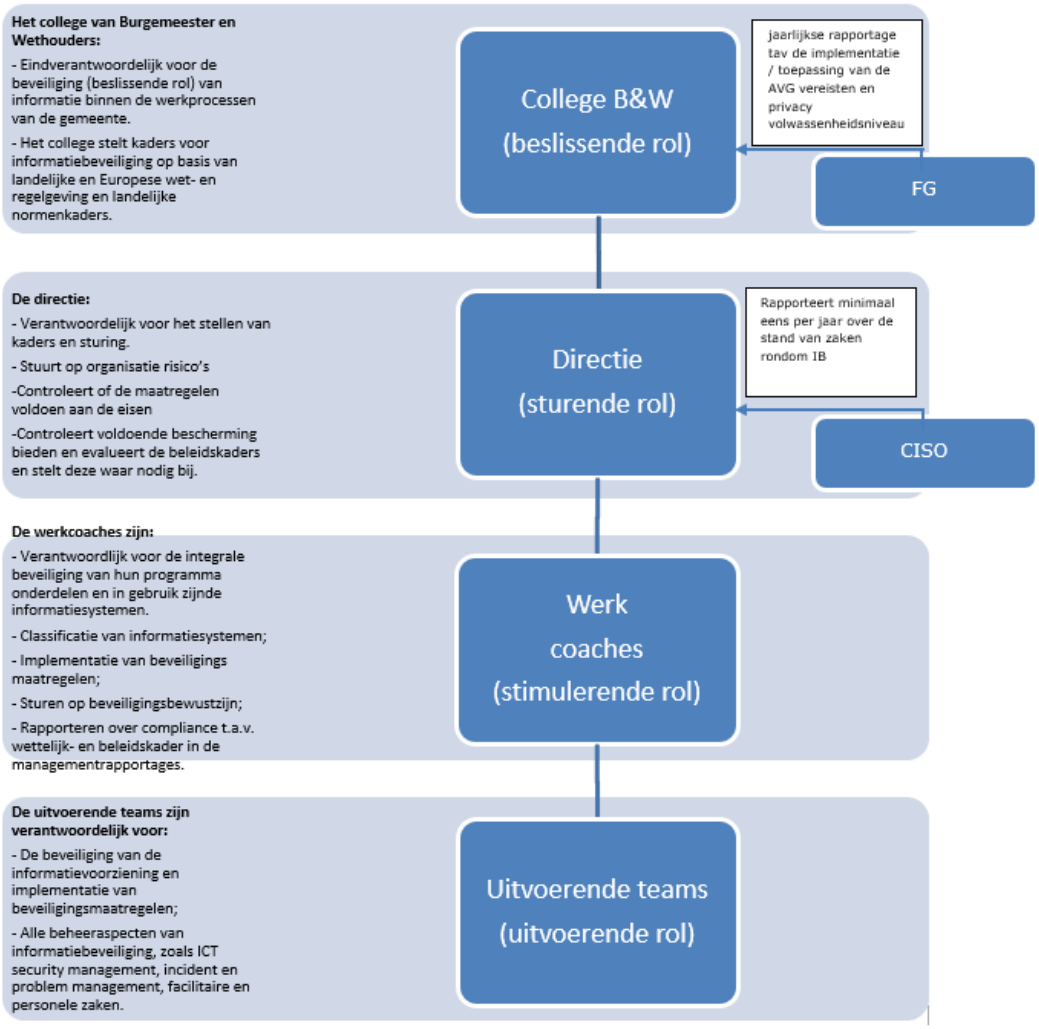
- Algemene Verordening Gegevensbescherming ((U)AVG)
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)
- Wet Basisregistratie Personen (BRP)
- Paspoorten en Nederlandse Identiteitskaarten (PNIK)
- Paspoortuitvoeringsregeling (PUN)
- Wet Basisregistratie Adressen en Gebouwen (BAG)
- Wet Basisregistratie Grootschalige Topografie (BGT)
- Wet Basisregistratie Ondergrond (BRO)
- Wet Politie Gegevens (WPG)

Daarnaast zijn er beleidskaders rondom het inrichten van IB zoals:

- ISO27001 & ISO27002
- Baseline Informatiebeveiliging Overheid (BIO), tactisch en operationeel niveau.
- DigiD

Organisatie, taken & verantwoordelijkheden

Vanuit een IB-perspectief en ook vanuit het wettelijke kader is het van belang om de verantwoordelijkheden en bijbehorende activiteiten met betrekking tot IB te beleggen. IB is een verantwoordelijkheid van alle medewerkers. Dit hoofdstuk beschrijft in grote lijnen welke rollen en verantwoordelijkheden er zijn met betrekking tot IB en is vertaald naar onderstaand overzicht:



Eindverantwoordelijk: B&W
Het college van B&W is eindverantwoordelijk voor informatiebeveiliging binnen onze gemeente. Zij stelt het strategisch informatiebeveiligingsbeleid vast en toont hiermee, dat zij betrokken is bij het uitdragen en handhaven van het IB-beleid van en voor de hele gemeente. Vanuit de VNG zijn de tien principes voor informatiebeveiliging vastgesteld. Deze tien principes zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurders zichzelf opleggen, te weten:

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.

Aansturing: Directieteam
De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van de programma coördinatoren/managers. De directie zorgt dat de programma coördinatoren/managers zich verantwoorden over de beveiliging van de informatie. De directie zorgt dat de verantwoordelijke portefeuillehouders binnen het College gevraagd en ongevraagd geïnformeerd worden over de mate waarin IB een onderdeel is van het handelen van de bedrijfsvoering.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische IB beleidsonderwerpen en laat zich hierin bijstaan door de CISO van

de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp IB wordt in de gemeente Zundert gezien als een integraal onderdeel van Risicomanagement dat betrekking heeft op alle programma's.

Stimulerend: Werkcoaches
De bedoeling is dat alle processen, systemen, data, applicaties altijd één eigenaar hebben, er moet dus altijd iemand binnen een programma verantwoordelijk zijn. De CISO rapporteert over de tactisch- en operationeel uitgevoerde IB activiteiten aan de directie. Afstemming met de programma's over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp IB te bespreken in individuele sessies of bijvoorbeeld tijdens het coördinatorenoverleg.

Taken van de programma werkcoaches in het kader van IB zijn:
- het binnen de eigen programma onderdelen uitdragen van het beveiligingsbeleid, en daaraan gerelateerde procedures, inclusief het bevorderen van de bewustwording door training en opleiding;
- het leveren van input voor wijzigingen op maatregelen en procedures;
- bespreken van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

En uiteraard eenzelfde houding en gedrag ten aanzien van informatiebeveiliging als vermeld bij de medewerkers.

Uitvoering: Medewerkers
De gemeente Zundert is een platte organisatie waarbij alle medewerkers eigenaarschap tonen. Iedere medewerker wordt geacht om op verantwoorde wijze om te gaan met IB.

Houding en gedrag van medewerkers speelt hierbij een cruciale rol, zoals:
- Het voorkomen van toegang tot gebouwen en informatie door onbevoegden in de gebouwen en op de werkplekken;
- Het veilig omgaan met data en bedrijfsmiddelen en hiermee voorkomen van misbruik en diefstal van informatie;
- Het vertrouwelijk omgaan met informatie;
- Het melden van incidenten.
- het leveren van input voor wijzigingen op procedures;
- het vroegtijdig signaleren van de bedreigingen waaraan de bedrijfsinformatie is blootgesteld;

Samenwerking met Equalit
De gemeente Zundert werkt samen met Equalit, op het terrein van hosten van de ICT infrastructuur. Door ver"saas"ing (het uit de cloud afnemen van informatiesystemen) groeit het aantal ICT-leveranciers en hosting partijen binnen en buiten de Equalit-samenwerking. De samenwerking met andere gemeentes of gemeentelijke instellingen gaat verder dan alleen het beheren van de ICT. Het betreft op onderdelen gezamenlijk keuzes maken rond de inzet van applicaties, beheer en de vereiste beveiligingsniveaus. De gemeente Zundert heeft als strategisch uitgangspunt dat de lijn en afspraken die gemaakt worden door de Deelnemersraad Equalit (waarin Zundert is vertegenwoordigd) bij ICT-gerelateerde vraagstukken prevaleren boven keuzes van andere samenwerkingsverbanden of programma's. Het kunnen samenwerken met en eventueel koppelen met systemen van samenwerkingspartners moet uiteraard wel altijd mogelijk zijn, mits voldaan wordt aan de IB-eisen vanuit de BIO.

Deze uitgangspunten maken dat de gemeente Zundert een duidelijke richting kiest rond de verdere optimalisatie van de ICT-voorzieningen en zeker ook de weg naar een netwerkorganisatie open blijft houden.

Specifieke rollen en verantwoordelijkheden

Rol	Verantwoordelijkheden
CISO	- Algemene en dagelijkse coördinatie van de informatiebeveiliging, adviseren over de implementatie van het informatiebeveiligingsbeleid - Bevordert en adviseert gevraagd en ongevraagd over IB - Rapporteert minimaal eens per jaar aan de directie over de stand van zaken.

Kernteam	- Overleggen ieder kwartaal over relevante, actuele onderwerpen rondom IB - Signaleren nieuwe ontwikkelingen, knelpunten en incidenten op het gebied van IB
Functionaris Gegevensbescherming	- Onafhankelijk toezichthouder op de naleving van de (U)AVG en de WPG. Daarnaast gevraagd en ongevraagd adviserend over privacy vraagstukken en toepassing van relevante privacy wetgeving.
Facilitaire zaken	- Fysieke beveiliging van de informatievoorziening - Implementatie van beveiligingsmaatregelen die voortvloeien uit betrouwbaarheidseisen
Equalit	- Technische beveiliging
Controller	- Verbeteren van systemen, werkwijzen en procedures. - Interne en externe informatievoorziening - Interne beheersing
Informatiemanager	- Vertalen van de informatiebehoefte die vanuit verschillende werk- en bedrijfsprocessen van een organisatie ontstaan in informatievoorziening.
Personeelszaken/HRM	- Arbeidsvoorwaardelijke zaken
Functioneel beheerders	- Beheert de informatievoorziening ten aanzien van applicaties welke intern in beheer zijn
Proces en gegevenseigenaren	- Bepalen van beschermingseisen van informatie
Auditors	- Onafhankelijke toetsing van het beleid
Leveranciers en ketenpartners	- Compliance aan het beleid
Alle medewerkers & externe gebruikers van onze systemen	- Gedrag conform afspraken m.b.t. IB-beleid alsook de naleving hiervan

ENSIA verantwoording
De gemeente verantwoordt zich over IB middels de ENSIA systematiek. Hiermee kan de gemeente in één keer verantwoording afleggen over informatieveiligheid gebaseerd op de BIO (Baseline Informatiebeveiliging Nederlandse Overheid). Binnen de ENSIA verantwoordingssystematiek vallen de Basisregistratie Personen (BRP), de verantwoordingssystematiek over de Paspoorten en Nederlandse Identiteitskaarten(PNIK) Paspoortuitvoerings-regeling Nederland (PUN), Zelfevaluatie PNIK, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) en Waardering Onroerende Zaken (WOZ).

De Suwinet aansluiting is voor de gemeente Zundert geregeld via het Werkplein Hart van West-Brabant. Het Werkplein Hart van West-Brabant legt verantwoording af aan de gemeente Zundert over de wijze waarop voldaan wordt aan de eisen met betrekking tot IB voor dit specifieke onderdeel.

De gemeente Zundert heeft een eigen DigiD aansluiting, hiervoor ontvangt zij vanuit de leverancier een assurance rapportage (TPM). Op de eigen procedures en beheersmaatregelen vindt jaarlijks een onafhankelijke audit plaats door een IT-auditor.

Voor BRP/PUN/PNIK ligt de controle bij de beveiligingsfunctionaris reisdocumenten en rijbewijzen binnen de gemeente Zundert zelf.

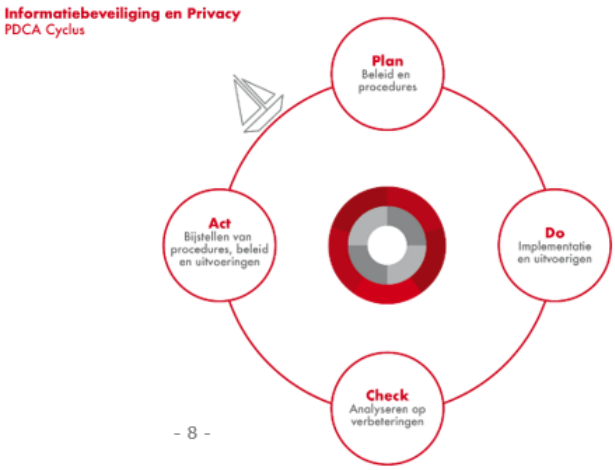
Binnen de gemeente Zundert is een ENSIA coördinator aangewezen, deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke werkcoaches.

De verantwoording over de IB komt in de collegeverklaring tot uitdrukking. De ingevulde ENSIA-zelfevaluatievragenlijst vormt de basis voor het opstellen van de Collegeverklaring aan de Gemeenteraad en de rapportage aan de landelijke overheden.

Uitwerking strategisch beleid
Het strategische beleid wordt als kader en basis gebruikt voor het uitwerken van de tactische beleidsplannen. Hiermee geeft het richting voor de verdere invulling van IB binnen de operationele doelstellingen en inspanningsverplichtingen binnen de gemeente Zundert. Dit zal worden vertaald in een tactisch en operationeel beleid. De gemeente Zundert heeft haar ICT grotendeels uitbesteed aan Equalit (SSC ICT gemeente Oosterhout) en om die reden bestaat dit tactisch/operationeel beleid uit twee documenten:

- Procedures waarbij de uitvoering voor 100% bij Equalit ligt, zijn vastgelegd in het Technisch informatiebeveiligingsbeleid.
- Procedures waarbij de uitvoering geheel of gedeeltelijk bij de gemeente ligt, zijn vastgelegd in het Algemeen informatiebeveiligingsbeleid.

De daaruit voortkomende werkzaamheden worden uitgewerkt in een Informatiebeveiligingsplan (IBP). Door ieder jaar een nieuw operationeel plan (IBP) te schrijven, is het mogelijk om snel in te kunnen spelen op de actualiteit en andere ontwikkelingen. Het maakt de gemeente flexibeler en daardoor veiliger. Voor het gestructureerd bijhouden van de status rondom IB wordt gewerkt met een ISMS (Information Security Management System). Deze tool ondersteund de jaarlijkse PDCA-cyclus.



Slotbepalingen

Intrekking oude regeling
Intrekking van het voorgaande strategisch informatiebeveiligingsbeleid.

Inwerkingtreding
Deze beleidsregels treden in werking:
» één dag na de bekendmaking

Citeertitel
Deze beleidsregels worden aangehaald als "Strategisch Informatiebeveiligingsbeleid".

Aldus besloten in de vergadering van 20 december 2022

Burgemeester en wethouders van Zundert,
de secretaris,
drs. J.W.F. Compagne

de burgemeester,
J.G.P. Vermue