Informatiebeveiligingsbeleid

Gemeente Zaanstad.

2020 - 2023

Inrichten

Auteur: Judith Unk CISO

www.zaanstad.nl

ZNSTD

Inhoudsopgave

1 Inleiding

De komende tijd staan we voor nieuwe uitdagingen: door het covid-19 virus zijn onze werkwijzen snel veranderd.
De verwachting is dat we de komende periode nog niet massaal op kantoor kunnen werken. Mogelijk komen er nog meerdere periodes van lock-down als de ziekenhuizen de nieuwe gevallen niet meer aankunnen.
Niet alleen onze interne medewerkers werken meer op afstand, ook onze inwoners worden snel digitaal. E-diensten, teleconferenties zijn in sneltreinvaart uitgerold. Inwoners verwachten meer digitaal, al zal er altijd een groep blijven die meer moeite heeft om hierin mee te komen.

Onze digitale ambities liggen steeds hoger en onze processen worden vergaand geautomatiseerd. Dit biedt voordelen voor burgers, bedrijven en belanghebbenden. Digitaliseren bevordert gemak, reduceert kosten en kan procedures vergemakkelijken. Als gemeente willen we de kansen van deze ontwikkelingen benutten.

Aan deze ontwikkelingen kleven ook risico's. Zo staat de informatieveiligheid onder druk. En als de informatie op enig moment niet beschikbaar is, loopt de continuïteit van onze dienstverlening gevaar. Alternatieven voor digitale gegevenswerking bestaan al bijna niet meer. Daarnaast zijn er dreigingen zoals de toename van cybercriminaliteit en onbedoelde inzage of aanpassing van de gegevens door onbevoegden.

De uitdaging die we hebben is om optimaal te profiteren van de ontwikkelingen rond digitalisering maar tegelijkertijd de risico's van digitalisering te beperken. Als we informatiebeveiligingsmaatregelen niet mee laten groeien met onze digitale ambities, lopen we kans dat onze gegevens op straat liggen, niet meer kloppen of niet op tijd beschikbaar zijn. Onze primaire processen kunnen dan niet meer doorgaan.

De toename van digitalisering is niet alleen terug te zien in onze administratieve processen, maar ook in onze openbare ruimte waar ook steeds meer gebruik wordt gemaakt van digitalisering (Zoals ICS/SCADA).

Om te zorgen dat onze informatiebeveiliging op orde blijft en in lijn blijft met de toename van de digitalisering hebben we een visie en een beleid opgesteld.

In onze 'visie informatiebeveiliging en privacy' staan onze uitgangspunten. In dit stuk werken we de organisatie van de informatiebeveiliging uit.
Eerst beschrijven we in hoofdstuk twee de rol van informatie en leggen we uit hoe de samenhang van dit beleid is met onderliggende uitwerkingen.
In hoofdstuk 3 beschrijven we de beveiligingsorganisatie.
Hoofdstuk 4 beschrijft hoe we invulling geven aan de PDCA-cyclus. En vervolgens besteedt hoofdstuk 5 aandacht aan onze ENSIA-verantwoording.

2 Informatiebeveiligingsbeleid

2.1 Waarom informatiebeveiliging?

Door de digitalisering wordt (digitale) informatie een steeds belangrijker bedrijfsmiddel. Dit geldt niet alleen voor onze administratieve processen op het gemeentehuis (zoals paspoortuitgifte, uitkering verstrekking e.d.), maar ook voor ander processen, zoals bijvoorbeeld de brugbediening. Informatie verzamelen en informatie verwerken is niet een doel op zich, maar is noodzakelijk voor bijna alle gemeentelijke processen. Informatie is daarmee de fundering van veel gemeenteplannen en processen. Als we die niet goed beschermen zakt het huis (lees onze plannen en taken) vroeg of laat in of komen er scheuren in het fundament.

Los van dat we onze eigen verantwoordelijkheid willen nemen, komt er ook steeds meer wet- en regelgeving waaraan wij ons moeten houden. Zo toetsen wij ons aan de normen volgens de ENSIA-methodiek, en verantwoorden wij ons daarmee aan de raad en aan de externe toezichthouders.

2.2 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is de Baseline Informatiebeveiliging Overheid (BIO[1]) . Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Wij maken ook gebruik van onderliggende praktische handreikingen, zoals een handleiding voor het uitvoeren van een risicoanalyse, de handreiking dataclassificatie en onderliggende richtlijnen. We maken hierbij gebruik van de standaarden die opgesteld zijn door de Informatiebeveiligingsdienst (IBD[2])

2.3 Reikwijdte informatiebeveiliging

De scope van dit beleid omvat:

- Alle gemeentelijke processen, onderliggende informatiesystemen
- 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.

Bij informatiebeveiliging gaat het niet alleen om onze administratieve processen, maar ook om datagestuurde processen in de openbare ruimte. Denk hier vooral aan industriële automatisering (SCADA).

Informatiebeveiliging houdt zich bezig op de volgende aspecten:

- *Beschikbaarheid: de mate waarin informatie beschikbaar moet zijn en de gegevensverwerking ongestoord voortgang moet hebben;*
- *Integriteit: klopt de informatie met de werkelijkheid. De informatie is juist, volledig en tijdig;*
- *Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen kennis kunnen nemen van gegevens of die kunnen verwerken.*

Dit 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.

---

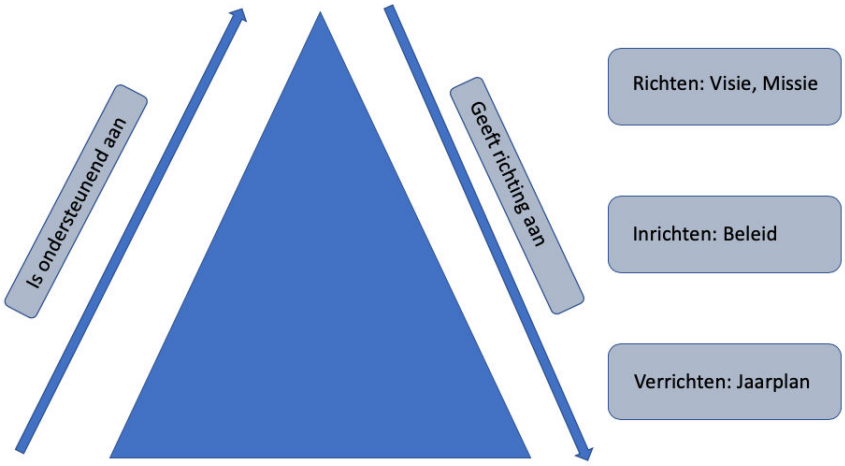
[1] De BIO is gebaseerd op de NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

[2] De Informatiebeveiligingsdienst (IBD) is onderdeel van de VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD draagt namens gemeenten bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft regelmatig kennisproducten uit

2.4 Samenhang Visie en vorige versie beleid

Dit stuk is een vervolg op ‘Onze visie op privacy en informatieveiligheid’

Het inrichtingsmodel voor de aanpak van Informatiebeveiliging in Zaanstad is gebaseerd op het model zoals in het onderstaande plaatje is weergegeven.



Figuur 1: Sturingsmodel informatiebeveiliging en privacy

Het Waarom van Privacy wordt behandeld in het visiedocument voor de gemeente Zaanstad. De visie op informatiebeveiliging en privacy geeft richting aan de manier waarop we met informatiebeveiliging en privacy willen omgaan.
De visie ondersteunt bij het opstellen van beleidskaders.
De beleidskaders ondersteunen in het vaststellen van de opdrachten en bij het toetsen of volgens de kaders wordt gewerkt.

Ook het Governance model, dat later in dit document wordt behandeld, kent eenzelfde inrichting.
Zo sluiten de verschillende lagen van sturen tot en met uitvoeren goed op elkaar aan.

3 Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk staan de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en op welke plaats die belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defense (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De medewerkers hebben zelf de verantwoordelijkheid om volgens deze processen te werken. De tweede lijn ondersteunt de informatiebeveiliging en de privacyofficers. Zij adviseert het management of de verantwoordelijkheden daadwerkelijk genomen worden. In de derde lijn beoordeelt de CISO het geheel en stelt verbeteringen voor. De CISO rapporteert ook aan de directie over de stand van informatiebeveiliging.

3.1 Aansturing: directieteam en sectorhoofden

De directie:
- Zorgt ervoor dat alle processen en systemen en de daarbij behorende middelen onder de verantwoordelijkheid vallen van een afdelingsmanager.
- Zorgt ervoor dat de afdelingsmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust.
- Zorgt ervoor dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over informatiebeveiliging
- Stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast door kritische bedrijfsprocessen vast te stellen
- Draagt zorg voor het uitwerken van het strategisch en tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO

3.2 Uitvoering: Sectorhoofden en Afdelingshoofden

Informatiebeveiliging valt onder de verantwoordelijkheden van sectorhoofden en afdelingshoofden. De tweede lijn ondersteunt hen daarbij. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben; er is dus altijd iemand verantwoordelijk.

Taken van de sectorhoofden en afdelingshoofden in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en, de daaruit voortvloeiende procedures.
- Het stimuleren van het bewustzijn onder medewerkers, bijvoorbeeld door de e-learning informatiebeveiliging te stimuleren en door het onderwerp periodiek terug te laten komen in de afdelingsoverleggen
- Het signaleren van bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten met de IBPO'ers en de consequenties die dit moet hebben voor beleid en maatregelen.

Als de werkzaamheden binnen één afdeling liggen is het afdelingshoofd verantwoordelijk. Als de werkzaamheden sector breed zijn, is het sectorhoofd verantwoordelijk.

Sectorhoofden en afdelingshoofden kunnen worden ondersteund door de CISO en/of de IBPO'ers.

3.3 Uitvoering: Gebruikers

Medewerkers hebben zelf een verantwoordelijkheid voor het zorgvuldig omgaan met de aan hun toegekende informatie en middelen. Ze volgen de aangeboden leermiddelen om voldoende op de hoogte te zijn, zoals de e-Learning informatiebeveiliging en privacy.
Als zij incidenten zien dan melden ze die aan hun leidinggevende of aan de Servicedesk IBT.

3.4 Ondersteuning

Een team van FG, CISO en Informatiebeveiliging en Privacy Officers (IBPO-ers) ondersteunt en adviseert de sectorhoofden, afdelingsafdelingshoofden en de 'ambassadeurs' bij de implementatie en borging van informatiebeveiliging.

De IBPOers
- Informeren de FG en CISO over de stand van zaken rond de maatregelen

- Bepalen het operationele en tactisch beleid op informatiebeveiliging en privacy
- Adviseren de lijn op het vakgebied en ondersteunt de lijn in het verbeteren van processen en systemen
- Ontwikkelen, verzamelen en delen kennis t.b.v. vakontwikkeling
- Borgt de technische kant van informatiebeveiliging
- Zijn gepositioneerd binnen de afdeling IBT

Voor basiskernregistraties BRP/PUN en SUWI zijn vanuit de wet- en regelgeving aparte security officers aangesteld. Zij ondersteunen en adviseren de afdelingsmanager bij de verwerking van de gegevens binnen deze processen en de verantwoording daarover.

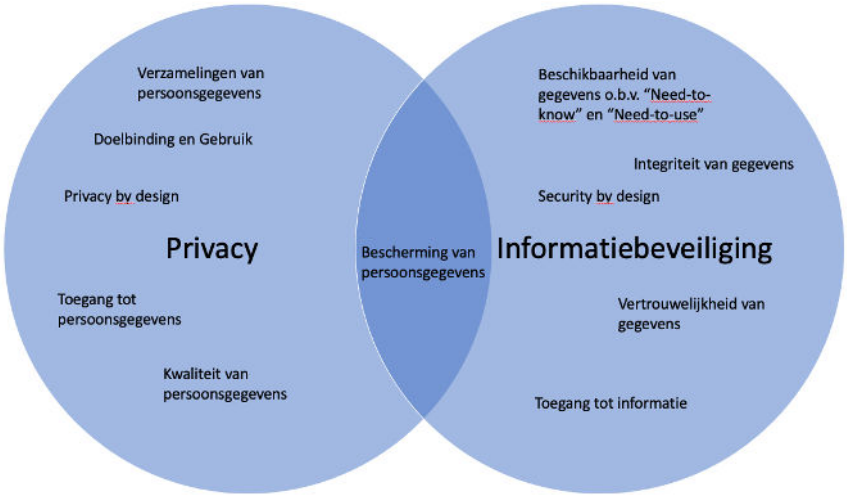
3.5 Controle en Verantwoording

Het informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur en directie. De bestuurders en directeuren zullen volgens de principes uit de visie ‘privacy en informatiebeveiliging’ richting en sturing geven aan het onderwerp informatiebeveiliging.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan portefeuillehouders. De directie rapporteert daarnaast over hoe zij invulling heeft gegeven aan het uitwerken van het beleid.
De voorbereiding en coördinatie van de rapportages rond informatiebeveiliging ligt bij de CISO. De CISO bespreekt ieder kwartaal samen met de FG in het Directie Overleg de stand van zaken rond informatiebeveiliging.

4 Informatieveiligheid en Privacy werken samen

Privacy en Informatiebeveiliging zijn twee terreinen die met elkaar verbonden zijn. In de bescherming rond persoonsgegevens hebben beide een eigen en een gezamenlijke taak.

Dit blijkt ook uit de AVG (art. 5, lid 1, f) waarin staat dat persoonsgegevens op een veilige manier verwerkt moeten worden door het nemen van de juiste technische en organisatorische maatregelen. Maatregelen die ervoor moeten zorgen dat het verwerken van persoonsgegevens op een passende beveiliging kan rekenen. Op het bijgevoegde plaatje is de overlapduidelijk aangegeven.



Figuur 2: Samenhang Privacy en Informatieveiligheid

5 Verbetercyclus Informatiebeveiliging

5.1 ENSIA en andere meetlatten helpen ons verbeterpunten te vinden

Om mee te kunnen groeien met de digitale ambitie en ons te verzetten tegen de druk van hackers leggen we de lat van informatiebeveiliging steeds hoger. De veranderende omgeving stelt steeds hogere eisen. Wat vandaag een veilige optie is, kan morgen een bekend lek hebben. Als we niet continue meegroeien worden we geleid door de waan van de dag.
Om te voorkomen dat we alleen maar reageren op incidenten en verplichte audits, maken wij gebruik van een PDCA-cyclus.

De PDCA-cyclus wordt ondersteund door de ENSIA-methodiek. Door ENSIA meten wij ons aan de hand van de normen uit de Baseline Informatiebeveiliging Overheid (BIO), aangevuld met specifieke normenkaders, zoals voor de DigiD aansluitingen.
Ons doel is en blijft om onze beveiliging goed te houden en risicogericht maatregelen te nemen. ENSIA is hierbij een hulpmiddel, waarmee we op een bepaald moment de thermometer in de organisatie steken om te kijken waar we staan.

ENSIA gaat vooral over de administratieve processen. We hebben echter ook informatiebeveiligingsmaatregelen voor industriële automatisering, ook wel ICS/ SCADA-automatisering. Die wordt toegepast bij bruggen gemalen en verkeerslichten. Het normenkader voor de ICS/SCADA-automatisering hebben we gevonden via een extern onderzoeksbureau. Ook hier gaat het om continue meten, beoordelen en verbeteren.

5.2 Bijhouden voortgang verbetermaatregelen in ISMS

Om onze PDCA te ondersteunen, maken wij gebruik van een ISMS[3] (Information Security Management System) en de bijbehorende systematiek.

Door ISMS-proces kan Zaanstad de sturing en verantwoording ten aanzien van informatiebeveiliging op een geautomatiseerde wijze vormgeven.

Door ISMS kunnen we beoordelen of de beveiligingsmaatregelen passend en effectief zijn. Zo niet dan stellen we ze bij. Het ISMS is een proces dat de basis legt voor passende beveiligingsmaatregelen voor de gemeente Zaanstad over de lange termijn.

Hierdoor kunnen op lange termijn analyses uitgevoerd worden. Ook wordt het mogelijk om op deze wijze de (bijkomende)werkdruk en knelpunten in een vroeg stadium op een onderbouwde wijze in kaart te brengen.

Beleid wordt jaarlijks getoetst en bijgesteld op basis van een PDCA-cyclus.

[3] ISMS tooling: Het ISMS is een proces dat de basis legt voor passende beveiligingsmaatregelen voor de gemeente over de langere termijn. Het ISMS wordt uitgevoerd door de (virtuele) informatiebeveiligingsorganisatie met verschillende activiteiten in de PDCA-cyclus van het ISMS.

5.3 Rapportage en verantwoording Informatiebeveiliging

Gemeenten rapporteren sinds 2017 over informatiebeveiliging volgens de ENSIA-methodiek. ENSIA is in eerste instantie een zelfevaluatie, waarbij sommige onderdelen onder een verplichte audit vallen.

Onze rapportages over informatiebeveiliging volgen de ENSIA-systematiek. We maken een horizontale verantwoordingsrapportage en een verticale verantwoordingsrapportage.

In de horizontale verantwoordingsrapportage verantwoorden we ons richting de gemeenteraad over informatiebeveiliging. We verantwoorden ons hier over het geheel aan informatiebeveiligingsmaatregelen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

In de verticale verantwoording verantwoorden we ons naar toezichthouders, zoals Logius, BKWI, en het ministerie van BZK. De verantwoording die de toezichthouders krijgen gaan over de voor hen relevante onderdelen (zoals de DigiD aansluitingen, Suwinet, BRP, BAG, BGT en BRO). Onderdeel van de verticale verantwoording is de collegeverklaring. Met deze verklaring geeft het college van B&W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging met betrekking tot de DigiD en Suwinet. De IT auditor [4] geeft assurance op de collegeverklaring.

Gemeenten wijzen een ENSIA-coördinator aan die ervoor zorgt dat de zelfevaluatie op tijd is ingeleverd, dat de audits en onderzoeken hebben plaatsgevonden en dat de rapportages en collegeverklaring op tijd af zijn en ingestuurd. Bij onze gemeente ligt de rol van ENSIA-coördinator bij de CISO.

4 Dit moet een register EDP auditor (RE) zijn ingeschreven in het register van NOREA.