gemeente Zaanstad
ZNSTD
GEMEENTEBLAD
Officiële uitgave van de gemeente Zaanstad
Nr. 422167
7 oktober
2024

Informatiebeveiligingsbeleid Gemeente Zaanstad 2024-2026

1 Inleiding

Als gemeente Zaanstad gebruiken we veel gegevens van onze inwoners. Als overheid hebben wij een verantwoordelijkheid om zorgvuldig met deze gegevens om te gaan. Door toenemende dreigingen en incidenten bij andere gemeenten heeft de VNG aangegeven dat informatiebeveiliging chefsache is. Het is een taak van het bestuur en de directie omdat het grote gevolgen kan hebben als het mis gaat.

Die verantwoordelijkheid nemen wij serieus. We willen het zelf, maar er is ook steeds meer toezicht op of we hieraan voldoen. Hiervoor leveren wij informatie (op deelgebieden) over de informatiebeveiligingsmaatregelen.

Behalve aan toezichthouders verantwoorden wij ons ook aan de gemeenteraad.
Het verhaal richting de raad hoeft niet heel technisch te zijn, als iedereen maar beseft wat de risico's zijn. Het gaat om basiskennis en informatie waarmee raadsleden zich kunnen inbeelden wat de gevaren zijn. Dat is best een uitdaging en dat moet nog dit jaar gebeuren. Ook colleges en ambtenaren moeten het goed tussen de oren krijgen. Gemeenten werken met privacygevoelige gegevens van inwoners. Daar moet je zorgvuldig mee omgaan.[1]

Om tot goede maatregelen te komen en continue te verbeteren, meten wij onszelf steeds aan wetgeving en standaarden. De komende tijd komen er meerdere nieuwe wetten op ons af, waarbij de Europese wetgeving Network and Information Security directive (NIS2) een zeer belangrijke wordt voor informatiebeveiliging van gemeenten.

Dit informatiebeveiligingsbeleid is gebaseerd op de tien bestuurlijke principes zoals vastgesteld door de VNG en de Informatiebeveiligingsdienst (IBD). Deze principes zijn een leidraad voor ons beleid en het fundament voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van onze informatie.

Dit informatiebeveiligingsbeleid is vastgesteld door B&W van de gemeente Zaanstad. Onderliggend aan dit beleid zijn richtlijnen over de invulling hiervan. Deze worden door de concerndirectie vastgesteld.

Dit informatiebeveiligingsbeleid wordt tenminste iedere 3 jaar vastgesteld door B&W. Mochten de ontwikkelingen daar aanleiding toe geven dan zal dit beleid eerder worden aangepast

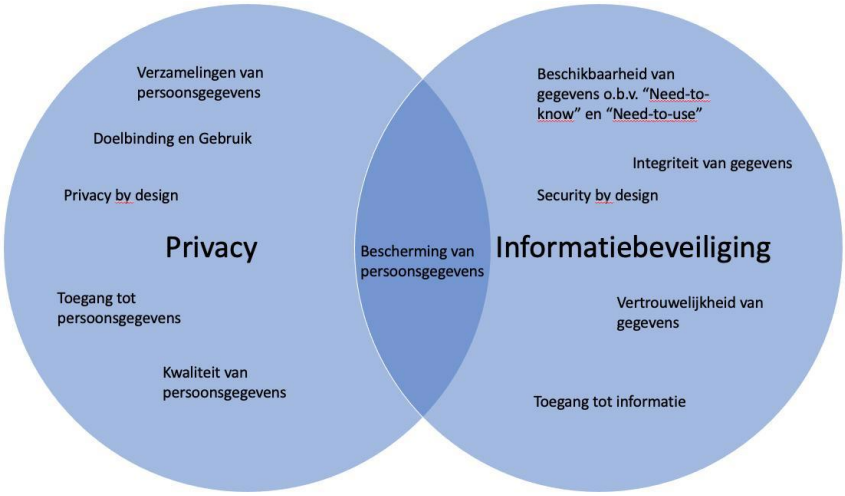
2 Wat is Informatiebeveiliging?

Informatieveiligheid gaat om het beschermen, beheren en beheersen van alle informatie. Je kan daarbij denken aan een digitale dreiging zoals diefstal van een wachtwoord. Maar ook analoge informatie op papier die door de verkeerde persoon wordt ingezien. Door de toenemende digitalisering van de maatschappij neemt het risico op een inbreuk toe.
Tegelijkertijd worden we als gemeente steeds afhankelijker van het werken en (digitaal) verzamelen van gegevens van inwoners. Diverse wetten stellen eisen aan de manier waarop we die gegevens verzamelen en verwerken (bijvoorbeeld participatie, WMO, etc.).
Een goede inrichting van informatieveiligheid verkleint de kans op schade die van invloed is op de kwaliteit van het functioneren van de gemeente.

2.1 Relatie tussen informatiebeveiliging en privacy Informatieveiligheid

Zowel informatiebeveiliging als privacy gaan over het beschermen, beheren en beheersen van informatie. Waarbij privacy specifiek aandacht vereist voor zorgvuldig omgaan met persoonsgegevens. Bij informatiebeveiliging gaat het juist om de bescherming van álle relevante informatie. Beide onderwerpen zijn nauw met elkaar verbonden. In onderstaand figuur is de relatie tussen deze onderwerpen weergegeven. Om veilig met informatie om te gaan is aandacht nodig voor de beveiliging van informatie én het zorgvuldig omgaan met persoonsgegevens.

1) Cyberweerbaarheid: Digitale veiligheid is chefsache; VNG-magazine 5 2024



2.2 Standaarden informatiebeveiliging
Onze gegevens te beschermen nemen wij maatregelen. We toetsen ons aan standaarden rond informatiebeveiliging. Dit helpt ons in onze standaarden te verhogen. Maar er is ook toenemende wet- en regelgeving die dit van ons vereist.

Daarom is de basis voor dit beveiligingsbeleid de Baseline Informatiebeveiliging Overheid (BIO[2]). BIO is gebaseerd op de standaarden voor informatiebeveiliging ISO 27002 en voor een deel (ISMS) op ISO27001.
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 van de Informatiebeveiligingsdienst (IBD[3])

We volgen de ontwikkelingen rond de standaarden. De komende jaren zal de BIO naar een nieuwe versie gaan die meer uitgaat van risicogerichtheid. (BIO 2.0) Ook moeten Nederlandse gemeenten voldoen aan Europese wetgeving, namelijk de NIS2.

De Network and Information Security directive, of NIS2-richtlijn, is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2 vergroot de reikwijdte van de eerste richtlijn door meer sectoren te omvatten.[4] Gemeenten zijn daarbij gecategoriseerd als essentiële diensten. Daarmee zijn wij onderworpen aan verhoogde en kritischer maatregelen.

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 processen in de openbare ruimte. Denk hier vooral aan industriële automatisering.

Informatiebeveiliging houdt zich bezig met de volgende aspecten:

Beschikbaarheid:

2) 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.
3) 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.
4) NIS2-richtlijn NIS2-richtlijn - Digitale Overheid

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 staan in aanvullende documenten.

3 10 bestuurlijke principes voor informatiebeveiliging

Als gemeente is onze missie om het volwassenheidsniveau van onze informatiebeveiliging te verhogen, in lijn met nationale richtlijnen en de 10 bestuurlijke principes van de VNG/IBD, en te voldoen aan de Europese regelgeving op het gebied van gegevensbescherming.

Daarom willen wij deze principes omarmen. In dit hoofdstuk werken wij uit hoe wij invulling willen geven aan deze principes. Hiermee trekken wij informatiebeveiliging op een hoger niveau en bereiden wij ons voor op nieuwe wetgeving, zoals de NIS2.

3.1 Bestuurders bevorderen een veilige cultuur

Bestuurders en directie stimuleren een cultuur waarin informatiebeveiliging en privacy door het gehele management worden ondersteund en uitgedragen. Het bestuur van de gemeente Zaanstad erkent het belang van een veilige cultuur voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Het bestuur zal actief beleid en initiatieven bevorderen die de bewustwording van informatiebeveiliging vergroten en een cultuur van veiligheid en compliance aanmoedigen binnen alle afdelingen en teams.

Het bestuur en directie geeft invulling aan het bevorderen van een veilige cultuur door: tijd, ruimte en middelen ter beschikken te stellen en voorbeeldgedrag te laten zien.

3.2 Informatiebeveiliging is van iedereen

Informatiebeveiliging is niet alleen een taak van de IT-afdeling. Iedereen bij de gemeente heeft een taak hierin. Het is één van de vele zaken die we moeten managen en in de gaten moeten houden. Het is onderdeel van goed je werk doen als ambtenaar en je verantwoordelijkheid nemen.

De verantwoordelijkheden staan verder uitgewerkt in een bijlage over de rollen en taken rond informatiebeveiliging. In dit beleid benadrukken we een aantal taken die van belang zijn om te laten zien dat organisatieonderdelen zelf ook een belangrijke rol hebben

Proceseigenaren zijn verantwoordelijk voor de informatieveiligheid van hun systemen en gegevens (zie visie). Hiervoor kunnen zij worden ondersteund door de specialisten in de organisatie rond informatiebeveiliging.

Informatieveiligheid valt onder de integrale verantwoordelijkheid van de proceseigenaren/managers. De managers zijn verantwoordelijk voor het (laten) uitvoeren van dit beleid en de onderwerp specifieke beleidsregels en procedures aanvullend op dit beleid. Hierover leggen zij verantwoording af aan de gemeentesecretaris/algemeen directeur. De managers zien erop toe dat de afdelingshoofden en medewerkers adequate maatregelen nemen voor de bescherming van de gegevens die onder hun verantwoordelijkheid vallen. Maatregelen zijn adequaat als ze voldoende risico afdekken.

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. Voor veel processen en systemen is er al een eigenaar.

Afdelingshoofden
Zaanstad organiseert trainingen en opleidingen rond informatiebeveiliging. Afdelingshoofden stellen hun medewerkers in staat om deze te volgen.

Afdelingshoofden hebben een belangrijke rol om voorbeeldgedrag te laten zien door zichzelf goed aan de regels te houden. Ook geven ze ruimte geven aan medewerkers voor trainingen e.d. en houden ze bij of iedereen de basistrainingen heeft gevolgd.

Alle medewerkers van de gemeente Zaanstad hebben een rol te spelen bij het waarborgen van de informatiebeveiliging. Iedereen wordt aangemoedigd om verantwoordelijkheid te nemen voor het beschermen van informatie, het melden van beveiligingsincidenten en het naleven van de geldende beleidsregels en procedures.

In de bijlage over taken en verantwoordelijkheden rond informatiebeveiliging staan deze zaken verder uitgewerkt.

3.3 Informatiebeveiliging is risicomanagement
Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Als we in ons risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn onze maatregelen op termijn wellicht niet doeltreffend of doelmatig

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Lijnmanagers zijn verantwoordelijk voor risicomanagement en bepalen de risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover

Risico's met betrekking tot informatiebeveiliging zullen worden geïdentificeerd, geëvalueerd en beheerd in overeenstemming met de risicobeheerprocessen van de organisatie.
Momenteel hebben we een eerste aanzet gemaakt door informatiebeveiliging en privacy onderdeel te laten zijn van het risicomanagement,

Risicomanagement zorgt ervoor dat we niet zomaar maatregelen nemen. Als gemeente nemen we veel goede maatregelen, maar soms zijn deze te veel incident gedreven (door incidenten bij ons of andere organisaties). Risicomanagement kan ervoor zorgen dat we onze capaciteit efficiënter inzetten.

3.4 Risicomanagement is onderdeel van de besluitvorming
Bij alle besluitvormingsprocessen binnen de gemeente Zaanstad zal rekening worden gehouden met de mogelijke informatiebeveiligingsrisico's. Informatiebeveiliging zal integraal worden opgenomen in strategische, operationele en projectbeslissingen.

Risicomanagement is belangrijk als er nieuwe processen en systemen worden ingevoerd. Maar ook bij bestaande processen is het belangrijk dat we doorlopend controleren of er door maatschappelijke ontwikkelingen of door toezichthouders extra eisen worden gesteld.

B&W en de directie kunnen alleen de juiste richting aangeven als de informatie hen bereikt. Door dreigingen en risico's mee te nemen in de vragen die ze stellen aan managers en adviseurs kunnen ze er in de besluitvorming rekening mee houden. B&W krijgt op zijn minst jaarlijks het jaarverslag informatiebeveiliging en de audits en rapportages die naar de toezichthouders worden gestuurd.
Zo kan B&W en de directie bijsturen voordat risico's zich voordoen en kan escalatie worden voorkomen.

3.5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
Het risicomanagementproces moet passen bij de organisatie en ondersteunend zijn aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht

De keten waarin wij werken bestaat uit andere (semi)overheidsorganisaties, bestuursorganen. Maar het gaat ook om IT-leveranciers waar we contracten mee hebben, beveiligingssystemen, facilitaire zaken, telecom e.d. De eisen die wij hebben aan onze informatiebeveiliging moeten we doorvertalen aan deze leveranciers.

3.6 Informatiebeveiliging is een proces
Informatiebeveiliging is een voortdurend proces van het registeren van risico's, door identificeren, evalueren en beheren anticiperen van risico's. De gemeente Zaanstad zal een continu verbeteringsproces implementeren om de informatiebeveiligingsmaatregelen voortdurend te verbeteren en aan te passen aan het veranderende bedreigingslandschap.

3.7 Informatiebeveiliging kost geld

De gemeente Zaanstad erkent dat informatiebeveiliging investeringen vereist in technologie, training en processen. Er zal een passend budget worden toegewezen om te zorgen voor de benodigde middelen voor effectieve informatiebeveiliging.

Tijdens ons risicomanagementproces maken we een risicoclassificatie. Hiermee kunnen we onze grootste risico's afdekken, op basis van dreigingen en van maatschappelijke ontwikkelingen. Zo weten we hoe we onze geld en capaciteit het beste kunnen inzetten.

"Informatiebeveiliging wordt vaak gezien als een (onnodige) kostenpost. De kosten voor preventieve maatregelen staan in geen verhouding tot de kosten van een incident. Die lopen al gauw op tot tonnen of miljoenen euro's. Zo'n incident heeft ook een grote impact op medewerkers. Een getroffen organisatie is vaak weken of maanden bezig om de bedrijfsprocessen en informatiebeveiliging weer op orde te krijgen en de complete gegevensregistraties opnieuw op te bouwen. Beveiligings- en privacy- incidenten schaden ook het vertrouwen van burgers in de overheid, de reputatie van de organisatie en haar bestuurders." (IBD)[5]

3.8 Onzekerheid dient te worden ingecalculeerd

Wat vandaag nog veilig lijkt kan binnenkort verouderd zijn. Zo is er altijd een race tegen de klok. Ook staan we als gemeente in een steeds veranderende maatschappij die andere eisen aan ons stelt. Dit maakt dat een 100 procent beveiliging nooit te garanderen is. En wat we nu veilig genoeg vinden hoeft dit volgend jaar niet meer te zijn.

De gemeente Zaanstad erkent dat er altijd onzekerheden zijn op het gebied van informatiebeveiliging. Daarom zullen we periodiek moeten controleren waar we staan en hierover rapporteren aan de concerndirectie of op managementniveau.
Er zullen passende maatregelen worden genomen om deze onzekerheden te identificeren, te evalueren en te beheren om de impact ervan op de organisatie te minimaliseren.

3.9 Verbetering komt voort uit leren en ervaring

De gemeente Zaanstad wil leren van eerdere incidenten, best practices en ervaringen om de informatiebeveiliging continu te verbeteren. We willen toe naar een cultuur van leren en verbeteren, waarin we leren van fouten en we onszelf steeds verbeteren.

Aangezien phisingmails steeds slimmer worden en we steeds verder digitaliseren maken we ongetwijfeld fouten. De kunst is om te leren van de fouten.
Medewerkers worden aangemoedigd in werkoverleggen met collega's te bespreken waar ze tegenaan lopen. Fouten of mogelijke fouten worden gemeld, zodat we de schade kunnen beperken en we ook kunnen leren en verbeteren.
We omarmen daarmee het motto: "je bent een held als je je informatiebeveiligingsfout of datalek meldt"

3.10 Het bestuur controleert en evalueert

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.

4 Jaarcyclus Informatiebeveiliging

4.1 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.

5) Uit "Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023-2024" Informatiebeveiligingsdienst

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 OT-automatisering. Die wordt toegepast bij bruggen gemalen en verkeerslichten. Ook hier gaat het om continue meten, beoordelen en verbeteren.

4.2 Bijhouden voortgang verbetermaatregelen in ISMS

Zaanstad gaat een ISMS[6] (Information Security Management System) proces opzetten en gaat hierop sturen. Hiermee komen we tot een continue verbetercyclus.

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.

De verbeteracties die Zaanstad uitzet worden jaarlijks getoetst en bijgesteld op basis van een PDCA-cyclus.

Een ISMS helpt gemeenten om de security en privacy beveiligingsdoelstellingen te ondersteunen. Bijvoorbeeld door:
- Het waarborgen van bedrijfscontinuïteit.
- Het bewaken van de betrouwbaarheid en de kwaliteit van de informatievoorziening.
- Risico's te beheersen.
- Het bijdragen aan verbeterde interne controle over informatiebeveiliging en privacy.
- Lering te trekken uit informatiebeveiligingsincidenten en datalekken.
- Rapportages op te stellen en verantwoording via de P&C-cyclus af te leggen.
- Het bijdragen aan een juiste en passende beveiliging van middelen van de gemeente.
- Het reduceren van kosten die nodig zijn om beveiligingsmaatregelen te implementeren.

Momenteel houden we ieder jaar de zelfevaluatie aan de hand van de BIO. Een aantal specialisten kiest dan onderwerpen uit waarop we interne audits houden. Dit is het begin van een verbetercyclus.
Wat nog ontbreekt is het uitzetten van de acties en toezicht houden op de verbetermomenten. Ook het voorleggen van de onderwerpen die we nader onderzoeken (aan bijvoorbeeld de directie) ontbreekt nog.

4.3 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 kennen hierin twee stromen:
- Verantwoording over het geheel aan informatiebeveiliging naar de gemeenteraad
- Verantwoording aan toezichthouders van de diverse stelsels over de deelgebieden.

6) 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.

In de verantwoorden richting de gemeenteraad verantwoorden ons over het geheel aan informatiebeveiligingsmaatregelen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad. De basis van deze vragenlijst is de Baseline Informatiebeveiliging Overheid (BIO).

In de verantwoorden naar toezichthouders, zoals Logius, BKWI, en het ministerie van BZK verantwoorden we ons 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[7] 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.

5 Focus komende jaren

In dit hoofdstuk staat een doorkijk naar waar we de komende jaren extra aandacht aan moeten besteden om de informatiebeveiliging op pijl te houden.

5.1 Nieuwe wetgeving: aantoonbaarheid en risicogericht belangrijk

Zoals eerder genoemd gaat eind 2024 de nieuwe Europese wetgeving in rond informatiebeveiliging, namelijk de NIS2, wetgeving rond netwerk- en informatiebeveiliging. Nederlandse gemeenten zullen zeer waarschijnlijk moeten kunnen aantonen in hoeverre ze voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Hiervoor moeten we in Zaanstad nog een betere vorm van bijhouden waar we staan t.o.v. de BIO. Het invullen van de BIO is nu een vragenlijst die als een ‘vrijblijvende’ zelfevaluatie werkt. In het kader van de NIS2 dient niet alleen de vragenlijst te worden ingevuld, maar is het ook zaak om vast te kunnen stellen dat deze juist en volledig is ingevuld.
Het invoeren van de ISMS zoals genoemd is in paragraaf 4.2 kan ons hierbij helpen.

5.2 Continue aandacht voor bewustwording

Uit diverse phishing acties bleek dat Zaanstad gemiddeld minder goed scoort dan andere gemeenten bij phishing acties. De acties die eerder zijn uitgezet zijn we nu aan het evalueren.
Bewustwording is niet iets dat je eenmalig inregelt en dat het daarna goed is. Maar dit zal ook de komende jaren continue aandacht nodig hebben. De uitdagingen worden steeds groter.

5.3 Bedrijfscontinuïteit voorbereiden/ aanscherpen

Vanuit de techniek zijn er diverse uitwijk- en back-up scenario’s maatregelen. Ook zijn er risicoclassificaties gemaakt van de meest bedrijfskritische processen. Deze zijn echter nog niet door de business getest en vastgesteld.
Los van de techniek moeten de businessonderdelen nadenken over hoe ze de bedrijfscontinuïteit kunnen blijven waarborgen. Bedrijfsonderdelen moeten nadenken of er bepaalde processen zo kritisch zijn dat die altijd door moeten gaan. Vervolgens moet gekeken worden wat hiervoor geregeld moet worden. Dit is niet alleen de techniek, maar kan ook locatie of bepaalde middelen zijn.
Hiervoor gaan we de komende tijd bedrijfscontinuïteitsplannen maken.

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

5.4 Aandacht voor Operationele techniek

Ook rond procesautomatisering is veel te doen. Bruggen en sluizen e.d. zijn cruciaal. En hier komt meer aandacht voor, ook dankzij de NIS2 wetgeving. Zaanstad was al bezig de cyberveiligheid rond procesautomatisering te verhogen. We moeten nu zorgen dat dit geen eenmalige acties zijn en dat we dit structureel inregelen.

6 Link met andere beleidsstukken en richtlijnen

In dit informatiebeveiligingsbeleid is in hoofdlijnen uitgewerkt welke principes Zaanstad wil omarmen om zorgvuldig met de gegevens om te gaan.

Zoals al eerder genoemd is er een sterke samenhang met het privacy beleid. In de gemeenschappelijke visie zijn nog hoger liggende principes bepaald.

Zowel de visie privacy en informatiebeveiliging, het privacy beleid en dit informatiebeveiligingsbeleid worden vastgesteld door B&W.

Dit beleid geeft echter nog geen invulling aan operationele en tactische zaken. Deze zijn deels aanwezig, of worden momenteel gemaakt. Deze richtlijnen zullen worden vastgesteld door de concerndirectie. De eerste richtlijnen zullen voor eind 2024 klaar zijn.

We kennen hierbij de volgende richtlijnen:

- Beveiligingsorganisatie: taken, verantwoordelijkheden en rollen
- Overzicht webformulieren
- ISMS-richtlijnen
- Suwinet beveiligingsrichtlijnen
- Wachtwoordrichtlijnen
- Identity & access management
- Installatie en hardening
- Dreigingen, kwetsbaarheden en patchmanagement
- Sleutel en certificaatmanagement
- Informatiebeveiligingsincident management
- Monitoring, logging, detectie en response