gemeente Terschelling

Memo

Aan	:	**Gemeenteraad**
Datum	:	**26 juni 2018**
Afzender	:	**College van burgemeester en wethouders**
Onderwerp	:	**Ensia Audit**
Bijlage(n)	:	

Via dit memo informeert het college u over de stand van zaken van informatieveiligheid binnen de gemeente Terschelling.

Ontstaan en context verantwoording

De reden hiervoor is als volgt. In een bijzondere algemene ledenvergadering van VNG besloten dat het college vanaf 2017 de raad informeert over de stand van zaken op het terrein van informatieveiligheid. Deze verantwoording kent als scope volledige breedte van de gemeentelijke standaard voor informatieveiligheid, de Baseline Informatiebeveiliging Gemeenten (BIG). Daarnaast zal specifiek nog verantwoording afgelegd worden over twee stelsels waarvoor ook verticaal toezicht is ingericht, namelijk DigID en Suwinet.

Zoals gezegd is 2017 het eerste jaar van deze verantwoording. Om deze verantwoording landelijk op een eenduidige manier in te richten is ENSIA (Eenduidige Normatiek Single Information Audit) in het leven geroepen. ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken, de VNG, gemeenten, het ministerie van Sociale Zaken & Werkgelegenheid en het ministerie van Infrastructuur & Milieu. Er wordt in deze systematiek op basis van de BIG (Baseline Informatiebeveiliging Gemeenten) verantwoording afgelegd over informatieveiligheid voor de volgende stelsels:

- Basisregistratie Personen
- Paspoort Uitgifteregeling Nederland/Nederlandse Identiteitskaarten
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- DigID
- SUWInet

Voor de laatste twee onderwerpen geldt de plicht om hiervoor een formele collegeverklaring naar de raad te zenden, welke is goedgekeurd door een externe auditor. Omdat de gemeente Terschelling haar DigID aansluiting in een vereniging heeft ondergebracht is zij niet zelfstandig auditplichtig. Daarom treft u alleen deze formele verklaring voor Suwinet als bijlage aan.

Algemeen beeld van het college

In 2017 is op krachtige wijze invulling gegeven aan het verder implementeren van maatregelen voor informatieveiligheid. Hiervoor heeft het college in 2016 een informatieveiligheidsbeleid conform de BIG vastgesteld.
De basis voor het succesvol zijn van maatregelen is het integraal bekijken van het onderwerp informatieveiligheid. Dit betekent in de praktijk dat er risicoafwegingen zijn gemaakt en maatregelen zijn geïmplementeerd die daadwerkelijk bijdragen aan het terugdringen van deze risico's. De integrale aanpak houdt ook in dat de combinatie is gezocht tussen de onderwerpen privacy, rechtmatigheid en informatieveiligheid. Hieraan al in 2018 nog verdere opvolging worden gegeven. De samenwerking vanuit de GR de Waddeneilanden en de ICT samenwerking met SSC (Shared ServiceCentrum Leeuwarden) zorgt voor meer slagkracht door de hiermee gerealiseerde schaalgrootte.
Verdere verbijzondering van dit beeld treft u aan in de paragrafen focus 2017 en ambitie 2018.

Focus 2017

Belangrijke resultaten die invulling geven aan het beleid in 2017 zijn geweest:

1. *Het scholen van medewerkers op het gebied van informatieveiligheid*

Om incidenten te voorkomen en te herkennen is het kennisniveau van medewerkers van groot belang. Daarom is aan alle medewerkers een e-learning aangeboden met hierin de meest relevante onderwerpen op het gebied van informatieveiligheid

2. *Het actief beproeven van medewerkers op deze kennis*

Medewerkers zijn getoetst op de kennis, ondermeer door het uitvoeren van een phishingtest, toetsvragen in de e-learning en het uitvoeren van een mysteryguest-onderzoek.

3. *Het sturen op de actiepunten in het informatieveiligheidsplan dat in 2016 was opgesteld*
4. *Het verbeteren van monitoring van de technische infrastructuur*

Hiervoor zijn passende maatregelen geïmplementeerd door SSC.

5. *Het uitvoeren van een "één-meting" op de BIG maatregelen SSC*

Na de eerder uitgevoerde nulmeting in 2015 heeft SSC in 2017 voor alle BIG maatregelen getoetst of deze in opzet en bestaan aanwezig zijn.

6. *Het verbeteren van maatregelen voor continuïteit*

In 2017 is de verhuizing van onze ICT systemen van het gemeentehuis in Leeuwarden naar een extern datacenter afgerond. Door gebruik te maken van een ISO27001 gecertificeerd datacentrum is de continuïteit en de fysieke beveiliging beter geborgd.

Ambitie 2018

Voor 2018 is de belangrijkste ambitie het verder professionaliseren van het informatieveiligheidswerkveld door:

1. *Het verder borgen van de in het informatieveiligheidsplan 2018 genoemde punten*

Op dit moment worden belangrijke maatregelen regelmatig getoetst en bijgesteld. De ambitie is om dit in 2018 voort te zetten. Waar nodig

zullen op basis van de PDCA cyclus, wijzigingen in wet en regelgeving (zoals de AVG) en het dreigingsbeeld dat de gemeente via de Informatiebeveiligingsdienst Gemeenten en andere kanalen ontvangt, verdere maatregelen worden ingevoerd.

2. *Voorbereiding naar bredere werking van maatregelen*

Op specifieke normen toetst de gemeente al op opzet, bestaan en werking. Voor de meeste normen geldt dat op dit moment het beschrijven (opzet) en het aantoonbaar uitvoeren (bestaan) voldoende is. Om de informatieveiligheid te borgen en ook te kunnen voldoen aan de auditeisen die in de komende jaren steeds scherper zullen worden, zal gekeken worden welke maatregelen aangescherpt dienen te worden naar werking (in alle voorkomende gevallen volgens de opzet uitgevoerd).

3. *Het beter toetsbaar maken van maatregelen bij samenwerkingspartners*

SSC is voornemens voor 2018 een ISAE verklaring af te leggen over de door hen geïmplementeerde maatregelen. Wij zullen ook bij andere samenwerkingspartners sturen op zorgvuldige maatregelen

Meerjarenperspectief

Voor de verdere toekomst voorzien wij dat:

- het onderwerp informatieveiligheid actueel zal blijven als belangrijke pijler voor een betrouwbare overheid
- samenwerking op het gebied van informatieveiligheid steeds belangrijker zal worden. Zowel tussen overheidsorganisaties als met marktpartijen
- het maatregelenkader van de BIG herzien zal worden om passend voor toekomstige dreigingen en de manier waarop ICT systemen zich ontwikkelen

Realiteit

Ondanks het feit dat de gemeente Terschelling op een passend ambitie- en uitvoeringsniveau invulling geeft aan het onderwerp informatieveiligheid is het goed om te benadrukken dat dit geen garantie kan geven voor het uitsluiten van incidenten. Er kunnen nog steeds fouten gemaakt worden en wij zijn afhankelijk van de kwaliteit zoals deze door leveranciers van hard- en software wordt geleverd.

Terugkerend

Waar 2017 het eerste jaar is van de verantwoording van het college aan de raad over het onderwerp informatieveiligheid, zal de raad over dit onderwerp vanaf nu ieder jaar geïnformeerd worden

Bijlagen Suwinet

In de bijlagen van deze memo treft u de verantwoording over Suwinet en de ondertekende collegeverklaring aan. Deze kennen een verplichte layout en opzet vanwege de uniformiteit van de verantwoording aan de stelselverantwoordelijken.
Deze bijlage is, inclusief de verklaring van de auditor over de correctheid van de verklaring, naar de verticale toezichthouders Logius en het ministerie van SZW gezonden. Indien er niet op alle normen voldaan wordt aan de gestelde eisen kunt u dit lezen in deze bijlagen en zult u ook een verbeterplan aantreffen.