\gemeente
voerendaal

Raadhuisplein 1
6367 ED Voerendaal
Postbus 23000
6367 ZG Voerendaal

T 045 - 575 33 99
F 045 - 575 11 95
E info@voerendaal.nl
W voerendaal.nl

55432

38. Ter kennisname raad

ONTVANGEN 18 JULI 2019

Uw brief van	Uw kenmerk	Ons kenmerk	Voerendaal
		55045	15-07-2019
Onderwerp		**Behandeld door**	**Bijlagen**
Raadsinformatiebrief zelfevaluatie ENSIA 2018		G.G.H. Hollands	3

VERZONDEN 18 JULI 2019

Geacht raadslid,

Met deze raadsinformatiebrief wordt u geïnformeerd over de resultaten van de jaarlijkse audit op het gebied van informatieveiligheid (ENSIA) en de stand van zaken op informatieveiligheidsgebied van de gemeente Voerendaal.

ENSIA staat voor Eenduidige Normatiek Single Information Audit en is sinds 2017 verplicht voor gemeenten. De ENSIA omvat de verantwoording over de BIG (Baseline Informatiebeveiliging Gemeenten), DigiD (Digitale Identiteit), SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen), BRP (Basisregistratie Personen), PUN (Paspoortuitvoeringsregeling) , BAG (Basisregistratie Adressen en Gebouwen) en BGT (Basisregistratie Grootschalige Topografie). De gemeente Voerendaal verantwoordt zich middels ENSIA verticaal richting de verschillende toezichthouders en horizontaal richting de gemeenteraad.

Samenvattend is de uitkomst van de ENSIA verantwoording over het jaar 2018 voor de gemeente Voerendaal als volgt:

- Informatieveiligheid is een continue proces van analyseren en verbeteren (PDCA cyclus). Deze verantwoording over informatieveiligheid levert daar een belangrijke bijdrage aan. Informatieveiligheid kan/ zal nooit voor 100% op orde zijn. Er is altijd ruimte voor verbetering. Daarnaast noodzaakt veranderende wet- en regelgeving tot regelmatige bijstelling van het informatiebeveiligingsbeleid.

- De gemeente is goed op weg in het verbeteren van de informatiebeveiliging, maar voldoet nog niet volledig aan de BIG (daaraan zal op dit moment

overigens geen enkele gemeente voldoen). Dit is pas het tweede jaar dat gemeenten deelnemen aan de ENSIA verantwoording. Belangrijke randvoorwaarden zoals informatiebeveiligingsbeleid, risico analyses, informatiebeveiligingsplan, procedures, projectgroep informatiebeveiliging en de formatie voor informatiebeveiliging zijn echter aanwezig.

- Nu de BIG wordt vervangen door de BIO (Baseline Informatiebeveiliging Overheid) met 2019 als transitiejaar, zullen waar nodig bestaande stukken aangepast worden aan de nieuwe regelgeving.

- Voor het verantwoordingsjaar 2018 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring Informatiebeveiliging. Met deze collegeverklaring voldoet de gemeente Voerendaal over het verantwoordingsjaar 2018 ten aanzien van de interne beheersingsmaatregelen - in opzet en bestaan- aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring is als bijlage toegevoegd.

- De zelfevaluatie BRP en PUN, BAG en BGT zijn vóór de deadline aan de toezichthouders gestuurd.

- Aan de zelfevaluatie BRP en PUN worden geen procentuele scores meer toegekend, maar wordt gekeken in hoeverre wordt voldaan aan alle wettelijke vereisten of dat er aanbevelingen tot verdere verbetering zijn. Er zijn verbeterpunten voor de gemeente Voerendaal. Deze worden waar mogelijk in Voerendaal geïmplementeerd.

- De gemeente Voerendaal scoort ten aanzien van BAG 78% (norm is 75%) en ten aanzien van BGT 90% (norm 75%)

Voor de volledige rapportage zelfevaluatie ENSIA 2018, de collegeverklaring en het assurancerapport van de auditor wordt verwezen naar de bijlagen.

Met vriendelijke groeten,

Burgemeester en Wethouders van Gemeente Voerendaal

De secretaris	De burgemeester
H.H.M. Timmermans	W. Houben

Rapportage zelfevaluatie ENSIA verantwoordingsjaar 2018

Gemeente Voerendaal

Datum: 25 juni 2019
Versie: 1.0

0. Leeswijzer

In hoofdstuk 1 wordt toegelicht wat ENSIA is, welke documenten ontstaan uit ENSIA en welke mijlpalen er zijn gezien in de tijd. De aanpak en werkwijze van het ENSIA project wordt toegelicht in hoofdstuk 2.

Hoofdstuk 3 is de kern van deze rapportage. In dit hoofdstuk worden de status en de verbeterpunten van de gemeente ten aanzien van de Baseline Informatieveiligheid Gemeenten (BIG) benoemd.

In hoofdstuk 4 en 5 wordt het resultaat van respectievelijk de Suwinet- en DigiD audit toegelicht.

In hoofdstuk 6 wordt samenvattend aangegeven hoe de gemeente ervoor staat qua informatiebeveiliging. Er wordt ook kort ingegaan op de rapportages BRP/PNIK/BAG/BGT

Gelet op het openbare karakter van de rapportage zijn diverse elementen niet gedetailleerd beschreven. Dit zou de informatiebeveiliging van de gemeente in gevaar kunnen brengen.

1. Inleiding

Wat is ENSIA?

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

Het project ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). Het verantwoordingsproces over informatieveiligheid bij gemeenten wordt hiermee verder geprofessionaliseerd door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan hier ook beter op sturen.

ENSIA helpt gemeenten in een keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Inkomen (SUWInet) is samengevoegd en gestroomlijnd.

Uitgangspunt is het horizontale verantwoordingsproces door het college van Burgemeester en Wethouders aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan de nationale partijen die een rol hebben in het toezicht op informatieveiligheid.

Voor het jaar 2018 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring Informatiebeveiliging. De Collegeverklaring is opgesteld op basis van de bevindingen uit de zelfevaluatie en deze wordt getoetst door een IT-auditor. In de Collegeverklaring wordt - mede vanwege de vertrouwelijke aard van de informatie - een samenvatting van de

bevindingen op hoofdlijnen opgenomen. Met de vastgestelde collegeverklaring en het assurancerapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.

ENSIA bestaat uit:

- Vragenlijst zelfevaluatie informatiebeveiliging;
- Collegeverklaring ENSIA inzake informatiebeveiliging;
- Assurance rapport
- Separate Rapportage Informatiebeveiliging
- Rapportage BAG en BGT
- Zelfevaluatie BRP/PUN

Voor 2018 loopt het project ENSIA van 1 juli 2018 tot 15 juli 2019. Op hoofdlijnen verloopt de planning als volgt:

- Invullen en aanleveren zelfevaluatie vragenlijst (juli – december 2018);
- Opstellen en uploaden Collegeverklaring informatiebeveiliging; uitvoeren IT-audit en opstellen en uploaden van Assurance rapport (vóór 01 mei 2019);
- Opstellen en uploaden rapportage BAG en BGT (vóór 01 mei 2019);
- Het College van B&W legt verantwoording af over informatieveiligheid aan de gemeenteraad en toesturen van de jaarstukken aan de minister van BZK (vóór 15 juli 2019).

2. Aanpak en werkwijze

In dit hoofdstuk wordt aangegeven hoe de uitvoering van de ENSIA binnen de gemeente is vormgegeven/ georganiseerd.

In augustus 2018 is door de gemeentesecretaris een coördinator ENSIA aangewezen. In zijn rol als adviseur privacy en informatiebeveiliging is Guido Hollands aangewezen als ENSIA coördinator.

De ENSIA coördinator heeft samen met de beleidsadviseur bedrijfsvoering, medewerkers HRM, facilitair en burgerzaken de vragenlijsten ingevuld. Daarnaast zijn de samenwerkingsverbanden Kompas, het Gegevenshuis en Parkstad-IT benaderd om input te verzorgen voor de vragenlijsten.

Vóór 1 maart 2019 zijn de vragen m.b.t. de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN via PNIK vragenlijst) beantwoord en definitief gemaakt.

In oktober 2018 is een opdracht verstrekt aan de IT-auditor, BKBO. In december 2018 zijn de antwoorden op de vragenlijsten definitief gemaakt en ingediend.

In februari en maart zijn de noodzakelijke documenten aangereikt aan de IT auditor voor de uitvoering van de audit. In april heeft de IT auditor zijn rapportages opgemaakt en aangeleverd.

De rapportage zelfevaluatie ENSIA is opgesteld.

3. Status Baseline Informatieveiligheid Gemeenten (BIG)

Wat is de BIG?

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij gemeenten. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als kwaliteitscriterium voor een gezonde bedrijfsvoering is een bittere noodzaak geworden.

De Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.

2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.

3. De auditlast bij gemeenten te verminderen.

4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

De integrale Baseline Informatiebeveiliging Nederlandse Gemeenten bestaat uit drie delen:

1. BIG – Strategische Baseline[1]

   De Strategische Baseline kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente.
2. BIG – Tactische Baseline[2]

   De Tactische Baseline beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/ maatregelen die als baseline gelden voor de gemeenten.
3. BIG – Operationele baseline

   De operationele producten van de BIG zijn opgebouwd uit aanvullend beleid, procedures, handreikingen, aanwijzingen en patronen, en geven hiermee antwoord op het 'hoe'. In deze producten wordt gedetailleerd omschreven welke stappen er

[1] https://www.noraonline.nl/images/noraonline/e/e1/Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-BIG.pdf

[2] https://www.noraonline.nl/images/noraonline/6/6a/Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-BIG.pdf

genomen dienen te worden om tot implementatie van een of meerdere BIG maatregelen over te gaan.

In dit hoofdstuk wordt in elke paragraaf een onderdeel van de BIG uitgelicht. Op hoofdlijnen wordt aangegeven wat de status is binnen de gemeente, welke acties in 2017 zijn uitgevoerd en welke verbeteringen nog doorgevoerd moeten worden.

3.1 Implementatie tactische baseline

Voor het voldoen aan de BIG worden normen gesteld aan de wijze waarop de BIG is geïmplementeerd in de gemeentelijke organisatie. In de BIG is dit vertaald in het benoemen van verantwoordelijken, het uitvoeren van een GAP-analyse en het op basis daarvan samenstellen van een informatiebeveiligingsplan en rapporteren over de voortgang.

3.1.1 Status

De gemeente beschikt over informatiebeveiligingsbeleid waarin verantwoordelijkheden ten aanzien van informatiebeveiliging zijn benoemd. In samenwerking met de gemeente Simpelveld is in 2016 en 2017, onder begeleiding van Sincerus, gewerkt aan een risico-analyse, GAP-analyse en informatiebeveiligingsplan.

3.1.2 Uitgevoerde acties

Er hebben geen wijzigingen in het informatiebeveiligingsplan plaatsgevonden in 2018.

3.1.3 Nog te verbeteren

Het informatiebeveiligingsplan is op dit moment een te statisch document. Het plan (en dus de informatiebeveiliging) zal in een PDCA cyclus van implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren een dynamisch document moeten worden.

3.2 Risicobeoordeling en risicoafweging samenwerkingsverbanden

Hoofdstuk 4 van de BIG gaat over het beoordelen en afwegen van risico's om te komen tot een goede inschatting van het benodigde beveiligingsniveau voor gemeentelijke ICT en bijbehorende processen. Binnen ENSIA zijn de normen over risicobeoordeling en -afweging vertaald vanuit het perspectief van gemeentelijke samenwerking.

Samenwerkingsverbanden zijn verlengd lokaal bestuur. Het college legt verantwoording af over informatieveiligheid, ook over de informatieveiligheid van samenwerkingsverbanden. Door de afspraken over informatieveiligheid vast te leggen maken deze integraal onderdeel uit van de samenwerking.

3.2.1 Status

De status van de informatiebeveiliging ten aanzien van de samenwerkingsverbanden is onbekend/ onduidelijk. Van Kompas, BsGW en het Gegevenshuis is bekend dat zij actief zijn op het gebied van informatiebeveiliging.

3.2.2 Uitgevoerde acties in 2018

- De GR het Gegevenshuis heeft privacy en informatiebeveiligingsbeleid opgesteld. Dit beleid is begin 2018 vastgesteld door het algemeen bestuur.

Daarnaast zijn in de bijgestelde begroting 2018 middelen opgenomen om te komen tot uitvoering van het privacy en informatiebeveiligingsbeleid.
- Eventuele andere acties bij samenwerkingsverbanden zijn onbekend.

3.2.3 Nog te verbeteren

- Een risico analyse uitvoeren ten aanzien van de samenwerkingsverbanden met betrekking tot informatiebeveiliging. In 2019 is een inventarisatie ten aanzien van informatiebeveiligingsmaatregelen en privacymaatregelen aan alle GR gestuurd.
- Met samenwerkingsverbanden afspraken maken over de (gemeenschappelijke) norm m.b.t. informatiebeveiliging (BIO) en over de verantwoording t.a.v. informatiebeveiliging.

3.3. Beveiligingsbeleid

Hoofdstuk 5 van de BIG gaat over het realiseren van een aantoonbaar niveau van informatiebeveiliging op basis van relevante wetgeving dat geaccepteerd is door de gemeentelijke (keten-)partners. Dit zorgt voor een fundament voor het leveren van betrouwbare dienstverlening en het kunnen doorgaan van kritische processen bij een calamiteit of incident.

3.3.1 Status

De gemeente beschikt over een actueel informatiebeveiligingsbeleid op basis van de BIG.

3.3.2 Uitgevoerde acties in 2018

Er zijn in 2018 geen specifieke acties uitgevoerd met betrekking tot het informatiebeveiligingsbeleid.

3.3.3 Nog te verbeteren

Uiterlijk in 2019 zal het informatiebeveiligingsbeleid opnieuw beoordeeld moeten worden en eventueel aangepast worden. Dit met het oog op de invoering van de BIO (Baseline Informatiebeveiliging Overheid) die de BIG vervangt

3.4 Organisatie van de informatiebeveiliging

Hoofdstuk 6 van de BIG gaat over het organisatorisch beheren van de informatiebeveiliging binnen de gemeente. Een adequate organisatie van de informatiebeveiliging is onderdeel van het voldoen aan de BIG.

3.4.1 Status

De gemeente is deelnemer bij de Informatiebeveiligingsdienst (IBD) van de VNG. Medewerkers nemen regelmatig deel aan bijeenkomsten van de IBD. Daarnaast worden er contacten onderhouden met andere overheidsinstanties zoals bijvoorbeeld RvIG en Logius.

Met betrekking tot medewerkers (interne, externe en inhuur) is er aandacht voor geheimhouding (VOG en geheimhoudingsverklaringen).

3.4.2 Uitgevoerde acties in 2018

- Gezamenlijk met gemeente Simpelveld is één formatieplaats gecreëerd ten aanzien van privacy en informatiebeveiliging (0,5 FTE per gemeente);
- Er is een wervingscampagne geweest voor het vinden van een geschikte kandidaat voor de functie. Per 1 augustus 2018 is de functie ingevuld.
- Per 1 oktober 2018 is de heer R. Schols van het Privacyhuys de FG voor de gemeenten Voerendaal en Simpelveld.
- De gezamenlijke projectgroep informatiebeveiliging is in vergaderingen bijeen geweest.
- Met meerdere leveranciers waaraan zaken zijn uitbesteed en waarbij persoonsgegevens zijn betrokken zijn bewerkers- c.q. verwerkersovereenkomsten afgesloten.

3.4.3 Nog te verbeteren

- Opstellen nieuw informatiebeveiligingsbeleid op basis van BIO in 2019.
- Identificatie van risico's die betrekking hebben op externe partijen.
- Planmatiger omgaan met realiseren van maatregelen informatiebeveiliging.
- Onafhankelijke toets/ beoordeling van de informatiebeveiligingsactiviteiten.
- Borgen van (wettelijke) grondslag, doelbinding en proportionaliteit ten aanzien van de verwerking van persoonsgegevens.
- In contracten met externe partijen dient meer aandacht te zijn voor beveiligingsmaatregelen op basis van een risicoafweging.

3.5 Informatiebeveiligingsplan

3.5.1 Status

In samenwerking met de gemeente Simpelveld is in 2016 en 2017, onder begeleiding van Sincerus, gewerkt aan een risico-analyse, GAP-analyse en informatiebeveiligingsplan.

De gemeente beschikt over een actueel informatiebeveiligingsplan, op basis van de BIG, waarin wordt beschreven welke maatregelen gerealiseerd zijn en welke maatregelen nog verbeterd/ genomen moeten worden. Onderstaande hoofdstukken zijn opgenomen in het informatiebeveiligingsplan:

- Beheer van bedrijfsmiddelen
- Personele beveiliging
- Fysieke beveiliging en beveiliging van de omgeving
- Beheer van communicatie en bedieningsprocessen
- Toegangsbeveiliging
- Verwerving, ontwikkeling en onderhoud van informatiesystemen
- Beheer van informatiebeveiligingsincidenten
- Bedrijfscontinuïteitsbeheer
- Naleving

Voor een betrouwbare informatiebeveiliging is het vastleggen en naleven van procedures van groot belang. In dat kader zijn de afgelopen jaren een kleine veertig procedures opgesteld. Deze worden jaarlijks gecontroleerd en geactualiseerd.

3.5.2 Uitgevoerde acties in 2018

- Actualisatie en controle van de procedures m.b.t. informatiebeveiliging.
- Overleg met leveranciers over informatiebeveiliging en maatregelen.
- In samenwerking met de ICT-leverancier is een ICT uitwijk test uitgevoerd.

3.5.3 Nog te verbeteren

Onderstaand een opsomming van diverse verbeteringen:

- Formeel vaststellen van een verantwoordelijk manager voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit.
- Opstellen van regels voor het juist gebruik van bedrijfsmiddelen.
- Opstellen van classificatiesysteem en -richtlijnen voor informatie en classificeren van de gegevensverzamelingen.
- Opstellen van een disciplinair proces, conform CAR/UWO, voor werknemers die inbreuk maken op het informatiebeveiligingsbeleid.
- Implementeren van procedures en maatregelen voor het werken in en toezien op beveiligde ruimtes.
- Opstellen van een procedure voor het beheerst uitvoeren van wijzigingen op de IT voorzieningen (een wijzigingsbeheerproces).
- Opstellen van een testprocedure voor accepteren van nieuwe en gewijzigde systemen (zowel door de gebruikersorganisatie als het beheer).
- Opstellen van procedure voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.
- Beleid en procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling, zowel binnen als buiten de gemeente.
- Regelmatig informeren van medewerkers over de regels voor het juist en veilig gebruik van hun mobiele apparatuur, zoals laptops, smartphones en tablets.
- Instellen van een een clear desk-beleid voor papier, usb-sticks, externe schijven en mobiele devices en een clear screen-beleid voor ICT-voorzieningen.
- Opstellen van beleid en eventueel aanvullende maatregelen voor de inrichting en gebruik van laptops, tablets en andere mobiele communicatie apparaten.
- Meer aandacht voor informatiebeveiligingseisen bij de aanschaf van nieuwe informatiesystemen.
- Periodiek uitvoeren van penetratietest en vulnerability assessments.
- Opstellen van een bedrijfscontinuïteitsplan met daarin expliciet aandacht voor de continuïteit van processen en diensten bij uitval van IT-systemen en andere infrastructurele voorzieningen.
- Uitvoeren van een business impact analyse (BIA) voor alle (kritische) processen.

4. Suwinet IT-audit

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. Als een gemeente gebruik maakt van de Suwinet diensten, dan moet de gemeente voldoen aan het Suwinet-normenkader. In de ENSIA zelfevaluatie wordt getoetst of de gemeente voldoet aan het normenkader.

De bevindingen uit de zelfevaluatie zijn verwerkt in een Collegeverklaring. De IT-auditor toetst de Collegeverklaring. Voor de onderdelen waar niet wordt voldaan dient een verbeterplan opgesteld te worden. De auditor toetst of dit verbeterplan is opgesteld.

4.1 Suwinet voor de Participatiewet, IOAZ en IOAW

De werkzaamheden zijn gedelegeerd uitbesteed aan de ISD Kompas. Wij zijn als gemeente verantwoordelijk en leggen zelf verantwoording af over het gebruik van Suwinet [3].

Voor het afleggen van verantwoording heeft Kompas een Third Party Memorandum (TPM)[4] laten uitvoeren. Het oordeel van de auditor is dat de beheersingsmaatregelen van de ISD Kompas in opzet en bestaan voldoen aan de geselecteerde normen voor het Suwinet.

4.2 Suwinet voor Burgerzaken

De gemeente Voerendaal maakt geen gebruik meer van Suwinet voor burgerzaken.

5. DigiD

DigiD staat voor Digitale identiteit. DigiD is een authenticatiemiddel voor digitale dienstverlening bij de overheid en de zorg. De gemeente maakt gebruik van DigiD om digitale dienstverlening aan te bieden aan de burgers.

Organisaties die DigiD gebruiken moeten voldoen aan de DigiD beveiligingsnormen. In de ENSIA zelfevaluatie wordt getoetst of de gemeente voldoet aan de DigiD normen.

De bevindingen uit de zelfevaluatie zijn verwerkt in een Collegeverklaring. De IT-auditor toetst de Collegeverklaring. Voor de onderdelen waar niet wordt voldaan dient een verbeterplan opgesteld te worden. De auditor toetst of dit verbeterplan is opgesteld.

Het oordeel van de auditor is dat de beheersingsmaatregelen inzake DigiD in opzet en bestaan voldoen aan de geselecteerde normen voor DigiD.

6. Samenvattend: Hoe staan we ervoor?

Informatieveiligheid is een continue proces van analyseren en verbeteren (PDCA cyclus). Deze verantwoording over informatieveiligheid levert daar een belangrijke bijdrage aan. Informatieveiligheid kan/ zal nooit voor 100% op orde zijn. Er is altijd ruimte voor verbetering. Daarnaast noodzaakt veranderende wet- en regelgeving tot regelmatige bijstelling van het informatiebeveiligingsbeleid.

De gemeente is goed op weg in het verbeteren van de informatiebeveiliging, maar voldoet nog niet volledig aan de BIG (daaraan zal op dit moment overigens geen enkele gemeente

[3] Op basis van regeling Suwinet betreffen de artikelen 5.22 en 6.4 de verantwoording over de Suwinormen

[4] Een Derde verklaring of Third Party Memorandum (TPM) is een verklaring die afgegeven wordt door een onafhankelijk audit partij over de kwaliteit van een ICT-dienstverlening en – beheersing van een organisatie.

voldoen). Dit is pas het tweede jaar dat gemeenten deelnemen aan de ENSIA verantwoording. Belangrijke randvoorwaarden zoals informatiebeveiligingsbeleid, risico analyses, informatiebeveiligingsplan, procedures, projectgroep informatiebeveiliging en de formatie voor informatiebeveiliging zijn echter aanwezig.

Nu de BIG wordt vervangen door de BIO (Baseline Informatiebeveiliging Overheid) met 2019 als transitiejaar, zullen waar nodig bestaande stukken aangepast worden aan de nieuwe regelgeving.

Voor het verantwoordingsjaar 2018 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring Informatiebeveiliging. Met deze collegeverklaring voldoet de gemeente Voerendaal over het verantwoordingsjaar 2018 ten aanzien van de interne beheersingsmaatregelen -in opzet en bestaan- aan de geselecteerde normen inzake DigiD en Suwinet.

De zelfevaluatie BRP en PUN. BAG en BGT zijn vóór de deadline aan de toezichthouders gestuurd.

Aan de zelfevaluatie BRP en PUN worden geen procentuele scores meer toegekend, maar wordt gekeken in hoeverre wordt voldaan aan alle wettelijke vereisten of dat er aanbevelingen tot verdere verbetering zijn. Verbeterpunten worden waar mogelijk geïmplementeerd.

De gemeente Voerendaal scoort ten aanzien van BAG 78% (norm is 75%) en ten aanzien van BGT 90% (norm 75%)

.

Collegeverklaring ENSIA 2018

inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Voerendaal

Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Voerendaal

Gemeentelijk kenmerk collegeverklaring ENSIA:	52159
Naam auditfirma:	Bureau voor Kwaliteitsborging bij de Overheid (BKBO)
Naam auditor:	drs. M.B.H. IJpelaar
Datum:	Handtekening of paraaf auditor

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Voerendaal voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Gemeenten (BIG), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Voerendaal betreft dit in 2018 DigiD en Suwinet. De verklaring omvat het op 31 december 2018 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2018.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk 52159/bijlage 1) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener worden uitgevoerd, wordt door de dienstverlener verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan ISD Kompas.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en

ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 52159/bijlage 1) en Suwinet (bijlage 2 Suwinet met kenmerk 52159/bijlage 2]) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 52159/bijlage 1) en voor Suwinet (bijlage 2 Suwinet met kenmerk 52159/bijlage 2) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Voerendaal op 31 december 2018 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in een verbeterplan opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1000177	Ja	Neen
Suwinet voor SUWI-taken	Ja	Neen
Suwinet voor niet-SUWI-taken	Niet van toepassing	Niet van toepassing

Voerendaal, 23-04-2019

College van B en W gemeente Voerendaal

De secretaris De burgemeester

H.H.M. Timmermans W. Houben

ENSIA assurance rapport
DigiD en Suwinet
verantwoordingsjaar 2018
gemeente Voerendaal

BKBO bv
Kenmerk BKBO/181019-3/2/AR
drs. M.B.H. IJpelaar RE CEH CISA

8 april 2019
Dit assurancerapport heeft 9 pagina's
www.bkbo.nl

FEIT

Ook al zegt men dat
de wetenschap voor niets staat,
blijft het een feit
dat de zon voor niets opgaat.

Jules Deelder

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor

1.1 Ons oordeel

Wij hebben de bijgevoegde collegeverklaring ENSIA 2018 inzake informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van de gemeente Voerendaal onderzocht.

Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van de gemeente Voerendaal, in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

1.2 De basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de collegeverklaring verricht in overeenstemming met Richtlijn 3000-A (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance informatie voldoende en geschikt is als basis voor ons oordeel.

1.3 Beperking in gebruik en verspreidingskring

Dit assurancerapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Ons assurancerapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

1.4 Verantwoordelijkheden van het college van de gemeente Voerendaal

Het college van burgemeester en wethouders van de gemeente Voerendaal is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot Suwinet, zijn naast de collegeverklaring en dit assurance rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

- de risico's die het bereiken van de geselecteerde normen voor Suwinet in gevaar brengen, werden geïdentificeerd; en
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

Het College is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

1.5 Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de collegeverklaring nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de collegeverklaring en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang bevat;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van

inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen; en
- het evalueren van de toereikendheid van de assurance-informatie zoals opgenomen in de collegeverklaring en bijbehorende bijlage(n).

Vlijmen d.d. 8 april 2019

Bureau voor Kwaliteitsborging Bij de Overheid b.v.


drs. M.B.H. IJpelaar RE CEH CISA, directeur

C.H.G. Schaap MA CISO, auditor in opleiding

Bijlage Rapport van bevindingen DigiD

Deze bijlage is niet bestemd voor de verticale toezichthouder en wordt slechts verstrekt aan de gemeente Voerendaal.

Bijlage Rapport van bevindingen Suwinet

Deze bijlage is niet bestemd voor de verticale toezichthouder en wordt slechts verstrekt aan de gemeente Voerendaal.