Inkomend Griffie gemeente Houten: 18GR0302

INKGR: 18GR0302 | Reg: 10/07/2018
Casenummer: 18CV000278
Aan: Raadslid of -leden | B-INFO: Collegebrieven
Griffie gemeente Houten

Staf

Onderdoor 25
Postbus 30, 3990 DA Houten
Telefoon 030 639 26 11
Fax 030 639 28 99
E-mail: gemeentehuis@houten.nl
Internet: www.houten.nl

VERZONDEN 16 JULI 2018

gemeente Houten

Aan de leden van de raad
i.a.a. de commissieleden

Datum	Uw kenmerk	Uw brief van	Ons kenmerk	Bijlagen
5 juli 2018	18GR0302		18.000263	2

Onderwerp
Collegebrief inzake verantwoording informatieveiligheid

Geachte leden van de raad,

In deze collegebrief informeren wij u over de resultaten van de zelfevaluatie op het gebied van de informatieveiligheid en van de IT-audit alsmede het daarbij behorende assurancerapport.

Aanleiding
Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Daarmee is het startsein gegeven voor de invoering van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Verder hebben alle gemeenten daarmee afgesproken hun eigen toezichthouder, de gemeenteraad, jaarlijks te informeren over informatieveiligheid. Gelijktijdig is het project ENSIA (Eenduidige Normatiek Single Information Audit) van start gegaan. De ENSIA zelfevaluatie is een initiatief van de VNG en de ministeries van BZK, I&M en SZW en helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid zowel in verticale zin, dat wil zeggen naar de Rijksoverheid, als in horizontale zin naar de gemeenteraad. De zelfevaluatie wordt aangevuld met een IT-audit door een onafhankelijke auditor waarmee een oordeel wordt gegeven over enkele specifieke punten.

Geen project maar een proces
Informatieveiligheid is geen project maar een proces. Het treffen van en blijvend voldoen aan informatiebeveiligingsmaatregelen behoort deel uit te maken van de planning- en controlcyclus. In het strategisch informatiebeveiligingsbeleid, zoals door het college vastgesteld, is opgenomen dat de aanpak van informatiebeveiliging 'risk-based' is. Op basis van risicoanalyses en de jaarlijkse zelfevaluatie worden steeds de prioriteiten voor het lopende jaar bepaald.

Finetuning van maatregelen
In de jaren 2016 en 2017 is al veel werk verzet om de informatiebeveiliging 'BIG compliant' te maken. Naast het vaststellen van het strategisch informatiebeveiligingsbeleid en informatiebeveiligingsplan voor 2017 en 2018 zijn inmiddels meerdere onderwerpen op operationeel niveau uitgewerkt. Daarmee zijn bijna 200 van de 303 BIG-maatregelen opgepakt waarmee de voortgang van de beleids-ontwikkeling goed op schema ligt. In 2018 zal extra aandacht zijn voor de implementatie van dit beleid. Voor de prioritering van de maatregelen is gekeken naar het aanpakken van de grootste risico's. Dat wil niet zeggen dat op de genoemde punten nog geen maatregelen zijn genomen. Integendeel, op alle genoemde punten is al het nodige in gang gezet, maar er dient nog een verdere finetuning plaats te vinden om te zorgen dat de getroffen maatregelen ook volledig passen binnen de BIG.

Een nader overzicht van de maatregelen die hiervoor in aanmerking komen treft u aan in de bijlage 'Rapportage zelfevaluatie ENSIA en BIG 2017'.

Collegeverklaring en assurancerapport
Conform de verantwoordingssystematiek van ENSIA heeft het college bij besluit van 17 april 2018 de verplichte collegeverklaring vastgesteld waarmee een uitspraak wordt gedaan over de beheersingsmaatregelen op het gebied van de informatiebeveiliging van Suwinet (het systeem waarin gemeenten met overheidsinstanties informatie over burgers delen). Het betreft de maatregelen die Werk en Inkomen Lekstroom (WIL), de Regionale Sociale Recherche Nieuwegein (RSRN) en de Belastingsamenwerking gemeenten en hoogheemraadschap Utrecht (BghU) hebben genomen. Bij deze drie organisaties wordt gebruik gemaakt van een Suwinet-aansluiting, mede ten behoeve van inwoners van de gemeente Houten.

Uit de collegeverklaring, en in het bijzonder de daarbij behorende bijlage, blijkt dat negen van de tien interne beheersingsmaatregelen bij BghU in 2017 niet voldeden aan de gestelde normen voor de Suwinet-aansluiting. Gebruikelijk is dat een organisatie vervolgens een verbeterplan maakt om alsnog op de juiste wijze aan deze normen te gaan voldoen. De BghU heeft echter besloten dat niet te doen maar volledig te stoppen met de Suwinet-aansluiting en het verkrijgen van de informatie waarvoor Suwinet werd gebruikt op een andere wijze te regelen. Overigens riep dit de vraag op in hoeverre de BghU op andere punten wél voldoet aan de vereisten voor informatiebeveiliging. Inmiddels is ook daarover duidelijkheid. De directie van de BghU heeft op 24 mei 2018 een compleet Informatiebeveiligingsplan vastgesteld waarin alle aspecten zijn meegenomen, zoals die ook in de BIG c.q. in ISO 27001 voorkomen.

Voor de beide andere organisaties, WIL en de RSRN geldt dat zij volledig voldoen aan de gestelde eisen.

Indien u nog vragen heeft kunt u contact opnemen met de heer P.D.M. Woudt, Chief Information Security Officer, via telefoonnummer 030 – 6392 611.

Met vriendelijke groet,
het college van burgemeester en wethouders
de secretaris, de burgemeester,

H.S. den Bieman W.M. de Jong

Bijlagen(n):
1. Rapportage zelfevaluatie ENSIA en BIG 2017
2. Assurancerapport van de onafhankelijke IT-auditor