

Bezoekadres: Stadhuis Coolsingel 40
3011 AD Rotterdam
Postadres: Postbus 70012
3000 KP Rotterdam**Website:** www.rotterdam.nl
E-mail: bbo@rotterdam.nl
Inlichtingen: D.Brak
Telefoon: 0613320898**Cluster:** BCO
Ons kenmerk: 22bo4453
Uw kenmerk:**Datum:** 29 juni 2022**Betreft:** Reactie op uw mail van 8 juni over
ENSIA*Via de griffie (commissie Bestuur)*

Geachte heer Gisolf,

Begin juni hebt u per mail een aantal vragen en opmerkingen aan de gemeenteraad gestuurd, dit naar aanleiding van de ENSIA-stukken die op de agenda van de gemeenteraad stonden. Hierbij onze reactie op uw vragen inzake de ENSIA-collegeverklaringen DigiD en Suwinet.

Elk jaar informeert het college van B&W de raad over de resultaten van de ENSIA-audit. Dit jaar is ervoor gekozen om de brief feitelijk te houden op de auditresultaten van de huidige auditperiode (2021), waarbij we hebben getracht om in de raadsbrief zoveel mogelijk informatie over de verschillende audits te verschaffen. Omdat de uitkomst van de audits (in het bijzonder die voor DigiD) inzicht kan geven in kwetsbaarheden die door kwaadwillenden herleid kunnen worden naar de bijbehorende applicatie/url, kiezen wij er om veiligheidsredenen voor om de collegeverklaringen niet openbaar te maken. Naar aanleiding van de discussie daarover in de raad, is in tweede instantie besloten om de collegeverklaring alsnog openbaar te maken, maar de gevoelige informatie daarin zwart te lakken. Dit is de werkwijze die wij in het vervolg zullen toepassen.

Uit uw brief van 8 juni begrijpen we dat u aanvullende vragen heeft naar aanleiding van deze openbaar gemaakte collegeverklaring over DigiD en Suwinet audit. Hieronder geven we antwoord op de door u gestelde vragen;

1. Heeft er in 2021 een interim controle plaatsgevonden door de auditor ten aanzien van Suwinet? a. Zo nee, waarom niet? Op basis van deze controle hadden de bevindingen vroegtijdig gesignaleerd kunnen worden en hadden deze voor 31 december kunnen worden geadresseerd.

b. Zo ja, waarom zijn de geconstateerde bevindingen niet voor 31 december geadresseerd?

Voorafgaand aan de ENSIA-audits voeren we diverse tussentijdse controles uit. De bevindingen zijn afkomstig uit twee applicaties die dit jaar vervangen worden. De auditor heeft op 31 december 2021 vastgesteld dat er nog aan vier normen voor Suwinet niet werd voldaan. In de raadsstukken is toegelicht dat de geconstateerde bevindingen inmiddels opgelost zijn en/

of betrekking hebben op applicaties die inmiddels vervangen zijn of dit jaar worden uitgefaseerd.

2. Heeft de auditor na 31 december 2021 vastgesteld dat de gemeente Rotterdam aan alle Suwinet-normen voldeed?

De auditor heeft zijn oordeel gegeven over de periode 2021 (tot aan 31-12-2021). Bij het opstellen van de verbeterplannen zijn, zoals bij de vorige vraag toegelicht, de Suwinet bevindingen niet meer van toepassing en of opgelost.

3. a. De toegangsrechten van Suwinet-gebruikers dienen volgens norm 9.2.5.3 minimaal twee keer per jaar beoordeeld te worden. Hiermee wordt voorkomen dat deze rechten als gevolg van bijvoorbeeld een wijziging in taken van een ambtenaar te ruim worden. Hoe vaak zijn de toegangsrechten van Suwinet-gebruikers binnen de gemeente Rotterdam in 2021 gecontroleerd?

b. Zijn naar aanleiding van die controle (indien nodig) toegangsrechten van gebruikers gewijzigd?

- a. Het klopt dat er minimaal twee keer per jaar een controle wordt uitgevoerd op de toegangsrechten.
- b. De aanvullende periodieke controle helpt om eventuele onvolkomenheden in de toegangsrechten te signaleren en indien nodig te corrigeren. Naar aanleiding van periodieke controles komt het voor dat we toegangsrechten moeten aanpassen.

4. Norm 12.4.1 stelt dat de logging van het gebruik van Suwinet door gebruikers periodiek moet worden beoordeeld met als doel onrechtmatig gebruik van Suwinet op te sporen. Aan deze norm wordt door de gemeente Rotterdam niet voldaan. a. Indien de logging in 2021 niet is beoordeeld, is dit dan achteraf alsnog gedaan?

b. Is uit de beoordeling van de logging onrechtmatig gebruik gebleken?

De applicatie waardoor er voor norm 12.4.1 (logging) niet werd voldaan, is inmiddels uitgefaseerd.

5. Is door de auditor geconstateerd of per heden bij alle DigiD-aansluitingen wel aan het normenkader wordt voldaan?

De bevindingen zijn nog niet beoordeeld door de auditor. Als er aan een norm niet (volledig) wordt voldaan, eist Logius (DigiD) concrete oplostermijnen. Vanuit een multidisciplinair team wordt gewerkt om de bevindingen binnen de gestelde termijn op te lossen.

6. Heeft er in 2021 een interim controle plaatsgevonden door de auditor ten aanzien van deze DigiD-aansluiting? a. Zo nee, waarom niet? Op basis van deze controle hadden de bevindingen vroegtijdig gesignaleerd kunnen worden en hadden deze voor 31 december kunnen worden geadresseerd.

b. Zo ja, waarom zijn de geconstateerde bevindingen niet voor 31 december geadresseerd?

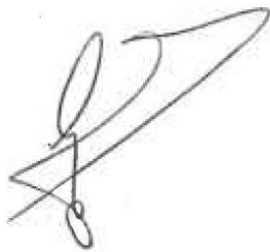
De geconstateerde bevindingen komen voort uit de technische penetratietest die einde van het jaar is opgeleverd. In 2021 zijn er nieuwe sub-aansluitingen bijgekomen die gebruik maken van dezelfde hoofdaansluiting. Deze sub-aansluitingen hebben we dit jaar ook meegenomen in de zelfevaluatie en de pentest. De resultaten hebben we opgenomen in de collegeverklaring.

7. Vindt de gemeente dat het risico van een maatwerk applicatie waard is in vergelijking met die van een standaard applicatie en wat maakt dit grotere risico acceptabel/nodig?

Zoals in de vorige vraag is toegelicht hebben de bevindingen betrekking op een sub-aansluiting die voor een groot deel standaardsoftware is. We gebruiken binnen de gemeente zowel maatwerk als standaardapplicaties, die moeten allebei voldoen aan de beveiligingseisen die we als gemeente stellen.

We hopen u hiermee voldoende te hebben geïnformeerd,

Met vriendelijke groet,

A handwritten signature in black ink, consisting of a stylized 'G' and 'J' followed by a long horizontal stroke.

G.J.M. Vreugdenhil

Wethouder Financiën, Organisatie, Dienstverlening, Grote Projecten