gemeente Rheden

B en W-voorstel

portefeuillehouder	begrotingsprogramma	Draagt bij aan Global Goal(s)
T.A.F.A. Klomberg	7 Overhead	16 Vrede, veiligheid en sterke publieke diensten

b en w-vergadering	agendapunt	bijlage(n)
		6

rol raad
N.v.t.

onderwerp
Aangepaste collegeverklaring ENSIA, aangepaste rapportage ENSIA

INHOUD VOORSTEL
1. De collegeverklaring ENSIA 2021 inzake informatiebeveiliging DigiD en Suwinet, inclusief bijlagen DigiD/Suwinet, vast te stellen.
2. Kennisnemen van het concept rapportage ENSIA en het verbeterplan.
3. Ondertekening van de collegeverklaring en de ondertekende collegeverklaring te uploaden op ENSIA voor verantwoording aan de toezichthouders.

1 Wat is de aanleiding?

Toevoeging 19-4-2022:
Als gevolg van een miscommunicatie is er één Digi-D aansluiting niet meegenomen in de ENSIA audit, namelijk die van iBurgerzaken. Deze aansluiting is in 2021 in gebruik genomen, waarvoor we een aansluit-audit succesvol hebben afgerond. Indien de Digi-D aansluiting na maart in gebruik is genomen, hoeft er in hetzelfde jaar bij de ENSIA controle geen verantwoording over afgelegd te worden. Onze audit vond plaats in mei, waardoor wij (in overleg met de auditor) er vanuit gingen hier bij de ENSIA controle 2021 geen verantwoording over af te hoeven leggen. Echter is de aansluiting in maart in gebruik genomen, waardoor wij deze wel in de ENSIA controle mee hadden moeten nemen. Na overleg met de auditor zijn we gezamenlijk tot de conclusie gekomen, dat we over 2021 voldoende hebben aangetoond aan de normen voor de Digi-D aansluiting te voldoen. Volgens het formele proces dienen de resultaten van de audit van de Digi-D aansluiting onderdeel te zijn van de collegeverklaring, vandaar deze toevoeging. De toevoegingen betreffen 1 regel in de college verklaring en de bijlage *'825010 _Gemeente Rheden_CV ENSIA Bijlage 1 DigiD 3 2021'* . De rest van de documenten is onveranderd gebleven. **Einde toevoeging**

Gemeenten dienen zich elk jaar te verantwoorden over de status van de informatieveiligheid van diverse informatiesystemen. Met ingang van 2017 is er een nieuwe systematiek voor verantwoording van de informatiebeveiliging ingevoerd, de ENSIA-systematiek en dit staat voor Eenduidige Normatiek Single Information Audit. Deze systematiek vloeit voort uit een resolutie van de Buitengewone Algemene Ledenvergadering van de VNG.

ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid. Hiermee kan met één verklaring zowel horizontaal (van het college naar de raad) als verticaal (van het college naar de landelijke toezichthouders, Bureau Keteninformatisering Werk & Inkomen (BWKI, onderdeel van het ministerie van Sociale Zaken en Werkgelegenheid) en LOGIUS (onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties) verantwoording worden afgelegd.

De verklaring met bijlagen en de rapportages over het Geo-domein (BAG, BGT en BRO) zijn opgesteld aan de hand van landelijke modellen.

De collegeverklaring gaat over een beperkt deel van de gehele ENSIA. Voor zowel dit jaar als vorig jaar hoeft de gemeente slechts over een selectie van de normen uit het gehele normenkader voor

DigiD en Suwinet verantwoording af te leggen en assurance te verkrijgen. Het betreft in dit jaar alleen een verklaring over de opzet en bestaan van de normen voor DigiD en Suwinet en niet over de werking van de normen.

Om tot een positief oordeel te komen, dient elk onderdeel van elke norm als voldoende beoordeeld te worden. Dit is in 2021 bij ons niet het geval gebleken. De audit beoordeelt bij ons twee Digi-D aansluiting en het gebruik van Suwinet. Bij de Digi-D aansluiting voor het CMS van Visma Roxit is 1 instelling van 1 norm bij de leverancier onjuist gebleken. Hierdoor is het totaaloordeel onvoldoende. Bij de gemeente voldeden we in 2021 wel aan alle normen. Bij de Digi-D aansluiting voor de belastingbalie is de audit bij de Connectie in 2022 uitgevoerd, waardoor we deze niet mogen gebruiken voor de rapportage over 2021. Hiervoor zullen we een hertest uit moeten voeren, waarvoor de verklaring uit 2022 wel bruikbaar is. Alle normen in deze verklaring staan op voldoende.
Voor Suwinet zijn er meerdere normen waar we niet aan voldoen. Deze normen bestaan uit meerdere onderdelen, waarbij we vaak aan 1 of 2 van deze onderdelen niet voldoen. De belangrijkste verbeterpunten zijn de tijdige periodieke controle van autorisaties, het tijdig uitvoeren van bewustwordingstrainingen en het inzichtelijk hebben en beoordelen van logging. Deze punten zijn opgenomen in het verbeterplan en zijn direct dit jaar opgepakt.

Na vaststelling van de collegeverklaring zal de auditor zijn assurance-rapport afgeven. De IT-auditor verklaart hierin dat de collegeverklaring een getrouw beeld geeft. Deze collegeverklaring en het rapport van de auditor dienen uiterlijk 30 april te zijn ingeleverd bij ENSIA.

Conform de ENSIA systematiek dient het college ook aan de gemeenteraad verantwoording af te leggen over de status van Informatieveiligheid. Dit zal in de paragraaf Bedrijfsvoering van de Jaarrekening opgenomen worden en daarmee uiterlijk 15 juli aangeleverd worden aan BZK.

2 Wat is het bestaand beleid c.q. kader?
Informatiebeveiligingsbeleid gemeente Rheden (2019-2021)
Privacybeleid Rheden (2019-2022)
VNG Resolutie informatieveiligheid (2013)

3 Wat willen wij bereiken op de genoemde Global Goal(s)?
Wij gebruiken DigiD en Suwinet voor de dienstverlening aan onze inwoners: Met het vaststellen van de collegeverklaring voldoet het college van burgemeester en wethouders aan de verplichting om verantwoording af te leggen over de informatiebeveiliging (2021: DigiD en Suwinet) van onze gemeente. Deze collegeverklaring inclusief bijlagen DigiD/Suwinet en het verbeterplan worden aangeboden aan de controlerende IT-auditor, die deze zal beoordelen en verwoorden in een Assurancerapport.

Hiermee beogen wij de dienstverlening aan onze inwoners te kunnen waarborgen.

4 Wat gaan wij ervoor doen?
De vastgestelde collegeverklaring inclusief bijlagen DigiD/Suwinet en het verbeterplan verstrekken aan de IT-auditor. Die geeft op basis van een audit assurance af over de collegeverklaring.
Gedurende de periode tot uiterlijk 30 april worden de collegeverklaring inclusief bijlagen DigiD/Suwinet en het assurance-rapport geüpload in de ENSIA tool. Hiermee voldoen wij aan de eisen voor verticale verantwoording.
In het verbeterplan staat een schematische weergave van de verbeterpunten, met de daarbij behorende planning.

5 Wat gaat het kosten?
Er is dekking voor de kosten van de onafhankelijke IT-auditor binnen de begroting Overhead. Het verbeterplan zal met de bestaande middelen uitgevoerd kunnen worden.

6 Wat zijn de risico's?
Zonder tijdige collegeverklaring kan onze gemeente worden afgesloten van het gebruik van DigiD en Suwinet. We voldoen dan immers niet aan de ENSIA verplichting, namelijk het tijdig en op de juiste wijze verantwoorden over de beveiliging van DigiD en Suwinet. Dit kan resulteren in afsluiting van deze voorzieningen door de toezichthouders. Afsluiting van deze voorzieningen heeft grote negatieve impact op de bedrijfsvoering en op de dienstverlening aan onze burgers. Daarnaast is het mogelijk

dat wij als gemeente verplichtingen opgelegd krijgen om onder toezicht en door de ministeries aangegeven termijnen verbeteringen door te voeren.

7 Wat is het draagvlak voor dit voorstel?
-

8 Hoe en met wie wordt er gecommuniceerd?
De collegeverklaring inclusief bijlagen DigiD/Suwinet en het verbeterplan overleggen we aan de controlerende IT-auditor.
Voor de verantwoording richting de gemeenteraad over de status van de Informatieveiligheid verwijzen we naar de paragraaf Bedrijfsvoering in de jaarrekening die uiterlijk 15 juli aangeleverd wordt aan BZK.

9 Wordt er een evaluatie uitgevoerd?
-