Onderwerp ENSIA 2020 – Verantwoording Informatiebeveiliging

Steller B.A.J. Verheijen

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon 050-3679134 Bijlage(n) 15 Ons kenmerk

Datum 31-3-2021 Uw brief van Uw kenmerk -

Geachte heer, mevrouw,

Hierbij informeren wij u over de stand van zaken van informatiebeveiliging binnen de gemeente Groningen. Naar aanleiding van een resolutie van de Buitengewone Algemene Ledenvergadering van de VNG, heeft de VNG samen met het Rijk een verantwoordingssystematiek ontwikkeld: de Eenduidige Normatiek Single Information Audit (ENSIA). De 'ENSIA-verantwoording informatiebeveiliging' gaat uit van het principe van Single Information & Single Audit (SISA). Dit betekent eenmalige informatieverstrekking en eenmalige IT-audit. De uitkomsten van deze audit zijn door ons college vastgesteld en hebben betrekking op de periode 2020. Met deze brief leggen wij hierover verantwoording af aan uw raad.

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente Groningen. Het verlies van informatie, uitval van ICT, of het door onbevoegden kennisnemen of (bewust) manipuleren van informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Het kan direct of indirect ook leiden tot consequenties doordat maatschappelijke en/of financiële schade kan ontstaan en de gemeente Groningen daarmee imagoschade oploopt. Incidenten kunnen mogelijk ernstig negatieve gevolgen hebben voor burgers, bedrijven, partners en/of de eigen organisatie. Informatieveiligheid is daarom van groot belang en informatiebeveiliging is het proces dat daaraan invulling geeft.

Hiervoor zijn de verantwoordingssystematieken voor de Basisregistratie Personen (BRP), Reisdocumenten (PUN), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO), Digitale persoonsidentificatie (DigiD) en

Inkomen (Suwinet) samengevoegd en gestroomlijnd. Dit betekent dat niet voor alle onderdelen afzonderlijke audits (die elkaar deels overlappen) moeten worden uitgevoerd. Ook hoeven er geen afzonderlijke rapportages opgesteld te worden.

In 2017 hebben alle gemeenten voor de eerste keer de verantwoording aan hun eigen toezichthouder, de raad, en de toezichthouders van het Rijk middels de ENSIA-systematiek uitgevoerd. Voor de verantwoording aan de gemeenteraad sluit ENSIA aan op de gemeentelijke planning- en controlcyclus. ENSIA neemt sinds 2020 de Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt. Vanuit deze horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij het Rijk afgeleid, de zogenaamde verticale verantwoording. Voor de uitvoering wordt gebruik gemaakt van zelfevaluaties.

De ENSIA-werkwijze in het kort
Gemeenten voeren een zelfevaluatie informatiebeveiliging uit onder meer gericht op beveiligingsnormen van de BRP, PUN, BAG, BGT, BRO, DigiD en Suwinet. De zelfevaluatie heeft ook betrekking op een aantal aspecten van de Algemene Verordening Gegevensbescherming (AVG) en niet-informatiebeveiligingsaspecten van BRP, PUN, BAG, BGT en BRO. Het college van B&W stelt een collegeverklaring ENSIA op over een aantal geselecteerde beveiligingsnormen. Een IT-auditor controleert de collegeverklaring en stelt een assurancerapport op.

Wij rapporteren vervolgens aan de gemeenteraad over de informatiebeveiliging middels deze brief aan de raad.

De scope van ENSIA is als volgt:

- Implementatie Baseline Informatiebeveiliging Overheid (BIO)
- Basisregistratie Personen (BRP)
- Reisdocumenten (PUN)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Digitale persoonsidentificatie (DigiD)
- Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Een verkorte weergave van de uitkomsten treft u aan verderop in deze brief.

Activiteiten in 2020
De gemeente Groningen is een informatie-intensieve organisatie. De randvoorwaarde voor succesvolle dienstverlening is een betrouwbare en veilige informatievoorziening. De medewerkers, van deze verschillende afdelingen en van de verbonden organisaties die gebruikmaken van deze

dienstverlening, moeten beschikken over betrouwbare informatie om de klanten optimaal te kunnen helpen en adviseren. Daarnaast dient de privacy van burgers en bedrijven aantoonbaar te zijn gewaarborgd, zodat zij erop kunnen vertrouwen dat hun gegevens in goede handen zijn binnen de gemeente Groningen.

In 2020 is hard gewerkt om de basis van informatiebeveiliging verder op orde te brengen. Daarbij lag de focus in 2020 op het doorvoeren van verbetermaatregelen naar aanleiding van ENSIA-auditbevindingen uit 2019.

Afgelopen jaar zijn workshops voor medewerkers georganiseerd gericht op het vergroten van het informatiebeveiligingsbewustzijn; wat de risico's zijn en wat men er zelf aan kan doen. De workshops gingen dit jaar, vooral digitaal en niet fysiek, onder meer het over het veilig gebruik van e-mail en het veilig opslaan van wachtwoorden. Daarnaast zijn er verschillende video's opgenomen voor de communicatie via intranet, is er een thuiswerkchallenge gedaan, heeft in oktober de cybersecurityweek plaatsgevonden, is er een enquête onder medewerkers gehouden en is het project voor de uitrol van gepersonaliseerde toegangspassen gestart.
Verder is in 2020 de vierde en laatste ronde van de game 'Zet jezelf of scherp' gemeentebreed gespeeld, zodat alle medewerkers op een praktische manier nader kennis hebben kunnen maken met dit onderwerp. Tevens zijn de voorbereidingen getroffen voor de nieuwe modules Informatieveiligheid en Privacy in het nieuwe Leer Management Systeem (LMS) dat in maart 2021 is live gebracht.

Het risicobeheer is verder aangescherpt voor de eerste processen en applicaties door inzichtelijk te maken wat de precieze informatiebeveiligings-eisen zijn. Deze zijn expliciet vastgelegd in de applicatieprofielen met minimale maatregelensets.

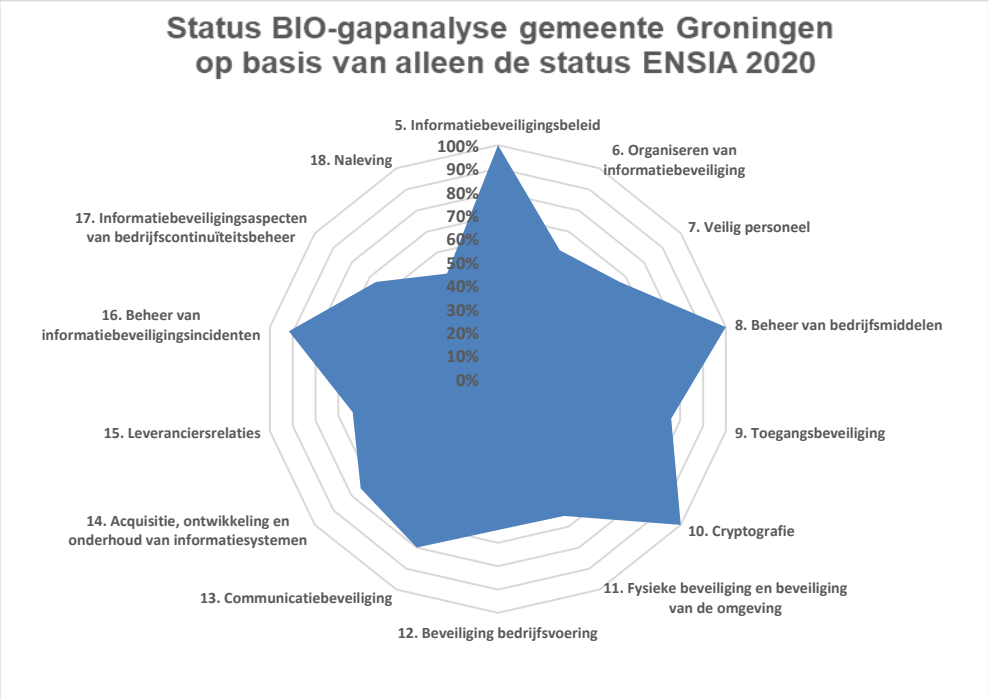
Informatiebeveiligingscontext
Begin 2020 kreeg de gemeente Groningen te maken met de internationale uitdaging van de Citrix-problematiek. Het risico was te groot voor collega's om via het thuiswerkportaal in te loggen. In maart begon vervolgens de coronacrisis, waardoor iedereen juist werd verplicht om zo veel mogelijk vanuit huis te werken. Kortom twee extreme omstandigheden die het uiterste van onze medewerkers hebben gevraagd om te kunnen blijven werken met de uitdaging dat ook nog veilig te doen.

Wij hebben ons in 2020 sterk gericht op de organisatorische maatregelen om verder te gaan voldoen aan de relevante wet- en regelgeving.
Dit is extra belangrijk in de context van het programma voor de uitbesteding van de technische ICT-dienstverlening aan Fujitsu.
Enerzijds zijn in 2020 de reeds *bestaande* technische risico's serieus toegenomen binnen de *oude* IT-infrastructuuromgeving. Wij nemen daar waar

mogelijk aanvullende beheersmaatregelen om deze risico's zoveel mogelijk te mitigeren.
Daartegenover staan de verbeteringen in de *nieuwe* IT-infrastructuur, waarin de nodige technische informatiebeveiligingsmaatregelen zijn gerealiseerd in 2020. Het realiseren van een meer veilige werkomgeving ging geenszins vanzelf. Er zijn verscheidene voorbeelden waarbij bestaande informatiebeveiligingsmaatregelen vroegtijdig en abrupt zijn beëindigd om vervolgens nog te moeten worden opgebouwd in de nieuwe IT-infrastructuur. Een spoedige én beheerste afronding van de transformatiefase van dit transitieprogramma in 2021 is vanuit informatiebeveiligingsperspectief derhalve van het grootste belang.

Resultaten in 2020
Eind 2020 is voor de derde keer een volledige pre-audit uitgevoerd op de beantwoording van alle zelfevaluatievragenlijsten van ENSIA. Daarmee is een extern getoetst beeld naar voren gekomen van de huidige status van een groot gedeelte van de totale informatiebeveiliging binnen de gemeente Groningen.

Zelfevaluatie BIO
Onderstaand spindiagram geeft de resultaten van BIO-vragenlijsten uit ENSIA 2020 weer.



N.B. De ENSIA 2020 zelfevaluatievragenlijsten toetsten nagenoeg alle 139 BIO-normen, dit in tegenstelling tot ENSIA 2019 dat slechts circa de helft van de 303 BI***G***-normen toetste. De verantwoording van 2020 geeft daarmee een volledig beeld van de informatiebeveiliging conform het wettelijk kader.

Let wel alleen in *opzet* en *bestaan*, want de *werking* van de BIO-maatregelen wordt uitdrukkelijk niet met de ENSIA-systematiek verantwoord.
Resultaten per stelsel
Vanuit de uitgevoerde zelfevaluaties is vanuit de ENSIA-systematiek ook verantwoording afgelegd aan het Rijk. Met onderstaande uitwerking informeren wij u per stelsel over de uitkomsten. De rapportages zijn als bijlagen opgenomen bij deze collegebrief.

Domein	**Bevindingen en door te voeren verbeteringen**
Basisregistratie Personen (BRP)	Score: 1.140 van de 1.200 punten behaald. Eindoordeel: 1 van de 3 ENSIA-domeinen/thema's voldoet niet volledig aan de wettelijk norm (95%). Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlagen: *11. ENSIA 2020 - Uittreksel Zelfevaluatie BRP Groningen br raad.* *12. ENSIA 2020 - Uittreksel BRP Verantwoordingsrapportage Groningen br raad.* *15. ENSIA 2020 - Verbeterplan BRP & Reisdocumenten in Collegevoorstel br raad.*
Paspoortuitvoeringsregeling Nederland (RNI)	Score: 635 van de 650 punten behaald. Eindoordeel: 1 van de 3 ENSIA-domeinen/thema's voldoet niet volledig aan de wettelijk norm (98%). Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlagen: *13. ENSIA 2020 - Uittreksel Reisdocumenten Verantwoordingsrapportage Groningen br raad.* *14. ENSIA 2020 - Uittreksel Zelfevaluatie Reisdocumenten Groningen br raad.* *15. ENSIA 2020 - Verbeterplan BRP & Reisdocumenten in Collegevoorstel br raad.* *16. ENSIA 2020 - Uittreksel Zelfevaluatie RNI Groningen br raad.* *17. ENSIA 2020 - Verbeterplan RNI (geen nodig) in Collegevoorstel br raad.*

Domein	Bevindingen en door te voeren verbeteringen
Digitale persoonsidentificatie (DigiD)	Gemeente Groningen gebruikt vier DigiD-aansluitingen. Hierbij zijn op basis van zelfevaluatie 2 bevindingen (bij twee DigiD-aansluitingen dezelfde bevinding) geconstateerd, waarvoor één verbeterplan is opgesteld. De zelfevaluatie is getoetst door een IT-auditor, zie onderstaande bijlagen bij de ENSIA-collegeverklaring: *02. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen cv.* *03. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1 DigiD cv.* *09. Verbeterplan ENSIA 2020 - Beveiligingsassessment DigiD cv.*
Basisregistratie Adressen en Gebouwen (BAG)	De zelfevaluatie BAG door de lijnverantwoordelijken leveren een puntenscore op van 150 uit het maximaal aantal te behalen punten van 205. De score (73%) is te beoordelen als nagenoeg voldoende. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *06. Verantwoordingsrapportage ENSIA BAG 2020 Groningen cv.*
Basisregistratie Grootschalige Topografie (BGT)	De zelfevaluatie BGT door de lijnverantwoordelijken leveren een puntenscore op van 140 uit het maximaal aantal te behalen punten van 150. De score (93%) is te beoordelen als voldoende. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *07. Verantwoordingsrapportage ENSIA BGT 2020 Groningen cv.*

Domein	Bevindingen en door te voeren verbeteringen
Basisregistratie Ondergrond (BRO)	De zelfevaluatie BRO door de lijnverantwoordelijken leveren een puntenscore op van 100 uit het maximaal aantal te behalen punten van 120. De score (83%) is te beoordelen als voldoende. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *08. Verantwoordingsrapportage ENSIA BRO 2020 Groningen cv.*
Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).	Voor de volgende taak wordt Suwinet binnen de gemeente Groningen gebruikt: Participatiewet/IOAW/IOAZ. Voor de volgende niet-SUWI-taak wordt Suwinet binnen de gemeente Groningen gebruikt: Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC). Hierbij zijn op basis van zelfevaluatie geen bevindingen geconstateerd. De zelfevaluatie is getoetst door een IT-auditor, zie onderstaande bijlagen: *02. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen cv.* *04. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 2 Suwinet cv.* *05. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 3 assurancerapportage cv.* *N.B. De gemeente Groningen is in 2020 door het BKWI geattendeerd op nog een 3-tal andere aansluitingen voor niet-SUWI-taken. Over de afgelopen 3 jaar is door het college van B&W onterecht geen verantwoording afgelegd over deze 3 aansluitingen. Na onderzoek blijkt echter dat van deze aansluitingen in de afgelopen 5 jaar geen (onterecht) gebruik is gemaakt. De aansluitingen zijn inmiddels formeel afgesloten door het BKWI.*

Resultaatafspraken
Op basis van de bevindingen vanuit de zelfevaluaties zijn de adviezen met verbetermaatregelen toegewezen aan en afgestemd met het desbetreffende verantwoordelijk lijnmanagement. Op basis hiervan zijn per afdeling / discipline verbeterplannen opgesteld, waarbij per verbetermaatregel een actiehouder en planning is bepaald. De ENSIA-coördinator bewaakt de voortgang en rapporteert periodiek de opvolging van de bevindingen aan het lijnmanagement.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd. Vanzelfsprekend zijn wij bereid een technische sessie hierover te verzorgen, indien uw raad dat wenst.

Met vriendelijke groet,
burgemeester en wethouders van Groningen,

burgemeester,
Koen Schuiling

secretaris,
Christien Bronda

Deze brief is elektronisch aangemaakt en daarom niet ondertekend.