Onderwerp ENSIA 2021 - Verantwoording Informatiebeveiliging

ter informatie

Steller B.A.J. Verheijen

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon 9134 Bijlage(n) 17 Ons kenmerk 80048-2022

Datum 09-03-2022 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 2021. 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/RNI), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO), Digitale persoonsidentificatie (DigiD), Inkomen (Suwinet) en Waarderegistratie Onroerende Zaken (WOZ) 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/RNI, BAG, BGT, BRO, WOZ, DigiD en Suwinet. De zelfevaluatie heeft ook betrekking op een aantal aspecten van de Algemene Verordening Gegevensbescherming (AVG) en niet-informatiebeveiligingsaspecten van BRP, PUN/RNI, BAG, BGT, BRO en WOZ. 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)
- Waarderegistratie Onroerende Zaken (WOZ)
- Rapportage Verhogen Digitale Weerbaarheid (VDW).

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

Activiteiten in 2021
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 2021 is hard gewerkt om de basis van informatiebeveiliging verder op orde te brengen. Daarbij lag de focus in 2021 op het doorvoeren van verbetermaatregelen naar aanleiding van ENSIA-auditbevindingen uit 2020.

Afgelopen jaar zijn enkele workshops en hackdemonstraties voor medewerkers georganiseerd gericht op het vergroten van het informatiebeveiligingsbewustzijn; wat de risico's zijn en wat men er zelf aan kan doen (zoals het veilig gebruik van e-mail en het veilig opslaan van wachtwoorden). Daarnaast heeft in oktober weer de cybersecurityweek plaatsgevonden, is er een enquête onder medewerkers gehouden en is het project voor de uitrol van gepersonaliseerde toegangspassen nagenoeg afgerond. Tevens is het Leer Management Systeem (LMS) in maart 2021 live gebracht met de nieuwe modules Informatieveiligheid en Privacy, als onderdeel van Het Digitale Rijbewijs. Deelname aan deze modules is verplicht gesteld voor alle medewerkers van gemeente Groningen die werken met informatie. Eind 2021 is een start gemaakt met de verbetering van de informatiebeveiliging van de websites van gemeente Groningen.

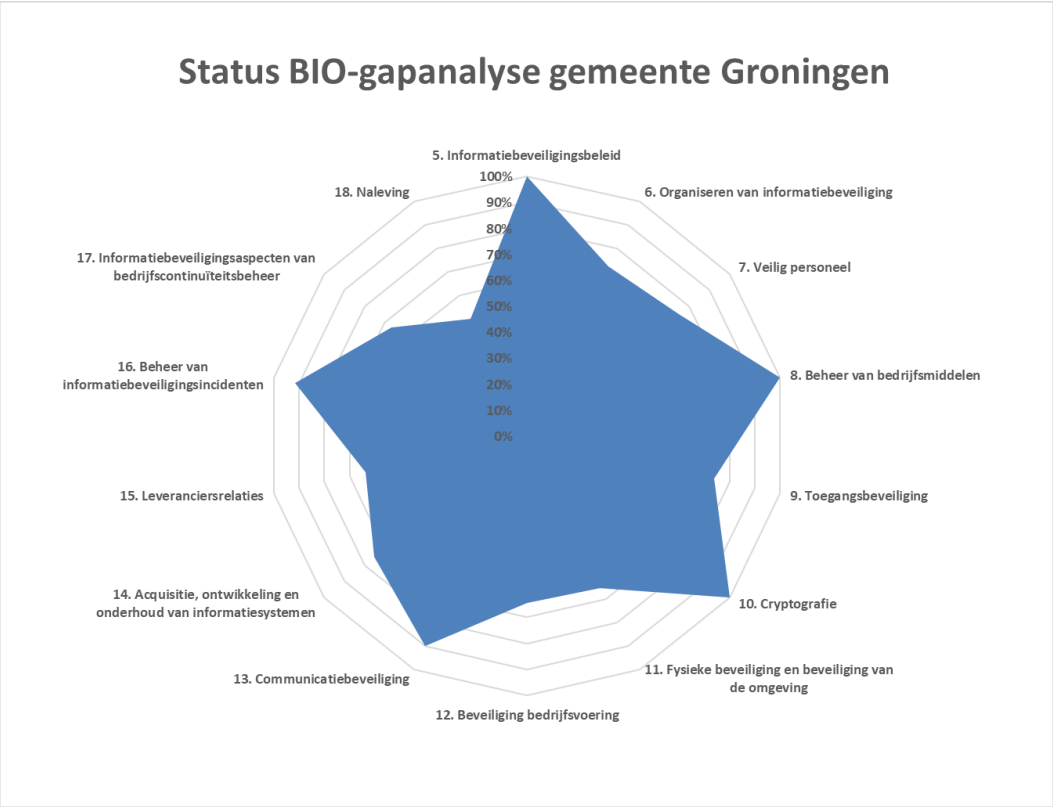
Tot slot is het risicobeheer dit jaar verder aangescherpt voor de eerste processen en applicaties door inzichtelijk te maken wat de precieze informatiebeveiligings-eisen zijn. Deze zijn expliciet vastgelegd in de applicatieprofielen met minimale maatregelensets.

Informatiebeveiligingscontext
Eind 2021 kreeg de gemeente Groningen te maken met de internationale technische uitdaging van de Apache Log4J-problematiek. Daarnaast had de coronacrisis ook dit jaar nog een belangrijk impact. De meeste medewerkers werden wederom verplicht om, zo veel mogelijk, vanuit huis te werken. Kortom een omstandigheid die veel van onze medewerkers heeft gevraagd om te kunnen blijven werken met de uitdaging dat tevens veilig te doen.

Wij hebben ons in 2021 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 2021 de reeds *bestaande* technische risico's serieus toegenomen binnen de *oude* IT-infrastructuuromgeving. Wij nemen 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 2021. 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 van de ICT-outsourcing in 2022 is vanuit informatiebeveiligingsperspectief derhalve van het grootste belang.

Resultaten in 2021
Eind 2021 is voor de vierde 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 2021 weer.



N.B. De ENSIA 2021 zelfevaluatievragenlijsten toetsten nagenoeg alle 139 BIO-normen. De verantwoording van 2021 geeft daarmee een volledig beeld van de informatiebeveiliging conform het wettelijk kader.
Let wel alleen in *opzet* en *bestaan*. 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: 1.170 van de 1.200 punten behaald. Eindoordeel: 1 van de 3 ENSIA-domeinen/thema's voldoet *niet* volledig aan de wettelijk norm (97,5%). Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlagen: *14. ENSIA 2021 - Uittreksel BRP Verantwoordingsrapportage Groningen br raad.* *15. ENSIA 2021 - Uittreksel Zelfevaluatie BRP Groningen br raad.* *19. ENSIA 2021 - Verbeterplan BRP & Reisdocumenten & RNI br raad.*
Paspoortuitvoeringsregeling Nederland (PUN) & Registratie Niet-Ingezetenen (RNI)	Score: 1200 van de 1200 punten behaald. Eindoordeel: 3 van de 3 ENSIA-domeinen/thema's voldoen volledig aan de wettelijk norm (100%). Voor RNI zijn op basis van zelfevaluatie eveneens *geen* ENSIA-bevindingen geconstateerd. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlagen: *16. ENSIA 2021 - Uittreksel Reisdocumenten Verantwoordingsrapportage Groningen br raad.* *17. ENSIA 2021 - Uittreksel Zelfevaluatie Reisdocumenten Groningen br raad.* *18. ENSIA 2021 - Uittreksel Zelfevaluatie RNI Groningen br raad.* *19. ENSIA 2021- Verbeterplan BRP & Reisdocumenten & RNI br raad.*

Domein	Bevindingen en door te voeren verbeteringen
Digitale persoonsidentificatie (DigiD)	Gemeente Groningen gebruikt vijf DigiD-aansluitingen. Hierbij zijn op basis van zelfevaluatie *geen* bevindingen geconstateerd. De zelfevaluatie is getoetst door een IT-auditor, zie onderstaande bijlagen bij de ENSIA-collegeverklaring: *02. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen cv.* *03. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1a DigiD Combi 1000913 ENSIA 2021 cv.* *04. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1b DigiD SaaS 1001382 ENSIA 2021 cv.* *05. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1c DigiD SaaS 1001913 ENSIA 2021 cv.* *06. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1d DigiD SaaS 1002498 ENSIA 2021.* *07. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1e DigiD SaaS 1003635 ENSIA 2021 cv.*
Basisregistratie Adressen en Gebouwen (BAG)	De zelfevaluatie BAG door de lijnverantwoordelijken levert een score op van 85%. Dit is te beoordelen als *voldoende*. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *10. Verantwoordingsrapportage BAG-BGT-BRO ENSIA 2021 cv.*
Basisregistratie Grootschalige Topografie (BGT)	De zelfevaluatie BGT door de lijnverantwoordelijken levert een score op van 81%. Dit is te beoordelen als *voldoende*. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *10. Verantwoordingsrapportage BAG-BGT-BRO ENSIA 2021 cv.*
Basisregistratie Ondergrond (BRO)	De zelfevaluatie BRO door de lijnverantwoordelijken levert een score op van 77%. Dit is te beoordelen als *voldoende*. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *10. Verantwoordingsrapportage BAG-BGT-BRO ENSIA 2021 cv.*

Domein	Bevindingen en door te voeren verbeteringen
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 bij de ENSIA-collegeverklaring: *02. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen cv.* *08. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen bijlage 2 Suwinet ENSIA 2021 cv.* *09. Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet Groningen bijlage 3 Assuranceverklaring ENSIA 2021 cv.*
Waarderegistratie Onroerende Zaken (WOZ)	Gemeente Groningen heeft de WOZ-werkzaamheden uitbesteed aan het Noordelijk Belastingkantoor (NBK). Op basis van zelfevaluatie zijn *geen* bevindingen geconstateerd. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *11. Bestuurlijke verantwoordingsrapportage WOZ ENSIA 2021 cv.*
Verhogen Digitale Weerbaarheid (VDW)	Gemeente Groningen heeft dit jaar voor het eerst de rapportage Verhogen Digitale Weerbaarheid opgesteld. Daarin is kernachtig omschreven wat de focus van gemeente Groningen dient te zijn van de komende periode. Voor meer informatie met betrekking tot de bevindingen en door te voeren verbeteringen, zie onderstaande bijlage: *12. Rapportage Verhogen Digitale Weerbaarheid ENSIA 2021 cv.*

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.

Vanzelfsprekend zijn wij bereid een technische sessie hierover te verzorgen, indien uw raad dat wenst.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
burgemeester en wethouders van Groningen,

burgemeester, Koen Schuiling	secretaris, Christien Bronda

Deze brief is elektronisch aangemaakt en daarom niet ondertekend.