Notitie Verantwoordingsstelsel ENSIA

Versie: 26 augustus 2020 – Definitief 1.0

Inleiding

Doel van deze notitie is het bieden van een eenduidige beschrijving van het verantwoordingsstelsel Eenduidige Normatiek Single Information Audit (ENSIA) voor alle partijen en personen die betrokken zijn bij het ontwikkelen, invoeren en beheren van ENSIA.

Achtergrond

Het project ENSIA (Eenduidige Normatiek Single Information Audit) is in juli 2015 gestart en in juli 2018 afgerond en heeft geresulteerd in een geïmplementeerd verantwoordingsstelsel ENSIA. Het was een gezamenlijk project van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het toenmalige ministerie van Infrastructuur & Milieu (I&M) en de Vereniging van Nederlandse Gemeenten (VNG). Het project had tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatiebeveiliging gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Uitgangspunt is dat aangesloten wordt op de gemeentelijke P&C-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatiebeveiliging en kan hier ook beter op sturen.

Het project is een resultaat van de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” die in november 2013 tijdens de Buitengewone Algemene Ledenvergadering van de VNG is aangenomen.

In deze resolutie hebben de gemeenten het belang van informatiebeveiliging erkend en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) aangenomen als hét gemeentelijk basisnormenkader voor informatiebeveiliging. De gemeenten hebben zich gecommitteerd aan de implementatie van de BIG in de eigen organisatie. Daarnaast informeert een college van B en W de gemeenteraad over informatiebeveiliging in het jaarverslag. In de resolutie hebben de gemeenten ook een oproep gedaan aan de rijksoverheid en ketenpartners om de verantwoordingslast over informatiebeveiliging te verminderen. Dit laatste vormde de aanleiding voor de start van het project ENSIA. De BIG is in 2020 vervangen door de BIO.

De notitie Verantwoordingsstelsel ENSIA adresseert de volgende onderwerpen:

- (Toelichting op) Het verantwoordingsstelsel ENSIA;
- De gemeentelijke producten;
- Informatieverstrekking met behulp van ENSIA-tooling;
- Samenwerkingsverbanden;
- Algemene Verordening Gegevensbescherming (AVG);
- Verantwoording over gemeentelijke objecten;
- Transparantie en benchmarking via ‘Waar staat je gemeente?’;
- Afspraken over de ENSIA-verantwoording en het groeipad.

Versiehistorie

- Versie 29 juni 2016, vastgesteld in stuurgroep 12 juli 2016.

- Versie 21 november 2016, vastgesteld in de stuurgroep van 24 november 2016. Deze versie is aangepast aan voortschrijdend inzicht in de afgelopen maanden.

- Versie 16 december 2016: aangepast n.a.v. resultaten van de impactanalyse: redactieslag, aanpassing van het tijdpad, verdere uitwerking van bijlage 2 met detailafspraken over 2017 met nadere toelichting van de reikwijdte van de zelfevaluatie informatiebeveiliging, de Collegeverklaring informatiebeveiliging en de IT-audit. Besproken in de stuurgroep op 22 december 2016.

- Versie 16 maart 2017: aangepast n.a.v. herijking tijdpad en reikwijdte Collegeverklaring en IT-audit, herijkte formats Collegeverklaring (bijlage 2) en Assurancerapport (bijlage 4) na afstemming met NOREA, handreiking voor de paragraaf Informatiebeveiliging in het jaarverslag (bijlage 5) toegevoegd en diverse aanpassingen op basis van voortschrijdend inzicht. Te bespreken in de stuurgroep op 23 maart.

- Versie 27 maart 2017: vastgestelde versie. Oplegger en vragen aan de stuurgroep verwijderd, procesplaat toegevoegd op pagina 2.

- Versie 29 juni 2017: n.a.v. diverse opmerkingen tekstaanpassingen ter verduidelijking doorgevoerd.

- Versie 23 oktober 2017: nadere duiding van te leveren producten in de tabel met de tijdspaden, aanpassingen in format Collegeverklaring en Assurancerapport met afzonderlijke bijlagen voor DigiD en Suwinet.

- Versie 27 november 2017: verwerken besluitvorming stuurgroep 25 oktober 2017: in bijlage 2 is de afgestemde bijlage Suwinet bij de Collegeverklaring opgenomen; verder op basis van voortschrijdend inzicht: een toelichting op de notitie Voortschrijdend inzicht, in bijlage 1 enkele technische aanpassingen in de mapping van de Suwinet-normen op de BIG en in de tabel met de reikwijdte van de zelfevaluatie.

- Versie 21 december 2017: aanpassingen in format Collegeverklaring en Assurancerapport.

- Versie 18 mei 2018: diverse aanpassingen voor het verantwoordingsjaar 2018: conform eerdere besluitvorming van de stuurgroep toevoegen van AVG en BRO, verwerken aangepaste wettelijke termijnen zelfevaluatie BRP/PUN.

- Versie 5 juli 2018: diverse aanpassingen voor het verantwoordingsjaar 2018.De volgende aanpassingen volgen nog: geactualiseerde procesplaten, geactualiseerde en vereenvoudigde formats Collegeverklaring en Assurancerapport, geactualiseerde toelichting op de paragraaf informatiebeveiliging in het jaarverslag en het verwerken van de besluitvorming van de stuurgroep over ‘Waar staat je gemeente’.

- Versie 1 november 2018: diverse aanpassingen voor het verantwoordingsjaar 2018: geactualiseerde procesplaten, geactualiseerde en vereenvoudigde formats Collegeverklaring (inclusief bijlagen) en Assurancerapport, geactualiseerde toelichting op de paragraaf informatiebeveiliging in het jaarverslag en het verwerken van de besluitvorming van de stuurgroep over ‘Waar staat je gemeente’. De volgende beschrijvingen volgen nog: escalatieprotocollen, herindelingsprotocol.

- Versie 12 december 2018: aanpassing datum en ‘aanpassing’ m.b.t. escalatie- en herindelingsprotocollen gewijzigd in ‘beschrijvingen’. De volgende beschrijvingen volgen nog: escalatieprotocollen, herindelingsprotocol.

- Versie 29 mei 2019: Actualisatie verantwoordingsjaar 2019-2020, informatiebeveiliging BAG en BGT uit ENSIA-zelfevaluatie, geactualiseerde procesplaten toegevoegd, geactualiseerd overzicht informatieverstrekking, Paspoortuitvoeringsregeling (PUN) aangepast in wet- en regelgeving reisdocumenten.

- Versie 7 juni 2019: Opmerkingen vanuit het Partneroverleg verwerkt.

- Versie januari 2020: Resultaat BIO Pilot ENSIA

- Versie mei 2020: Actualisatie verantwoordingsjaar 2020-2021, introductie BIO en uitkomsten BIO-Pilot, geactualiseerde procesplaat toegevoegd, geactualiseerd overzicht informatieverstrekking, werkwijze Suwinet, wijzigingen die de leesbaarheid bevorderen.

- Versie 26 augustus 2020: Opmerkingen vanuit het Partneroverleg verwerkt.
-

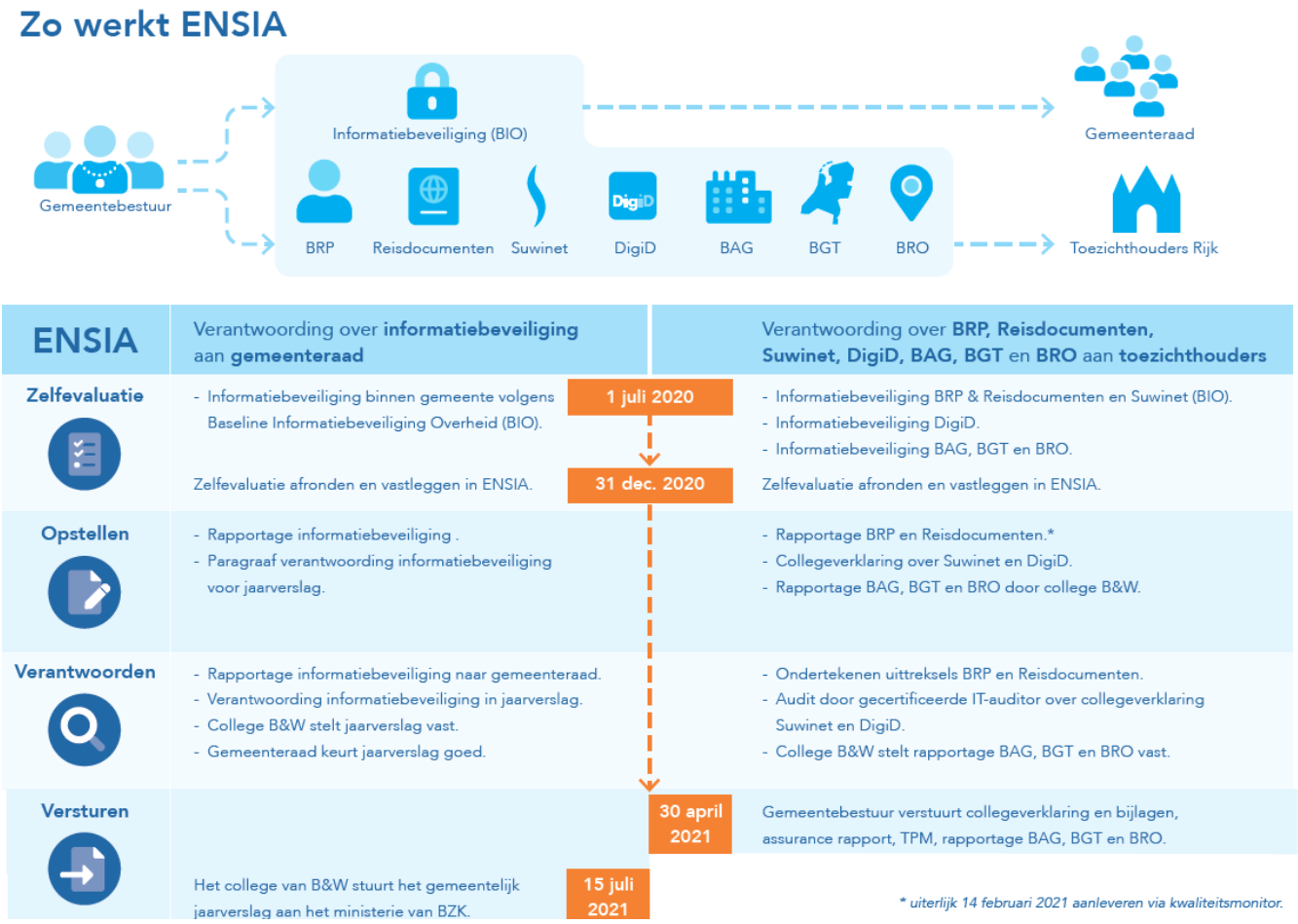
Het verantwoordingsstelsel ENSIA

De ‘ENSIA-verantwoording informatiebeveiliging’ gaat uit van het principe van Single Information & Single Audit (SISA). Dit betekent eenmalige informatieverstrekking en eenmalige IT-audit.

De ENSIA-werkwijze in het kort
Gemeenten voeren een zelfevaluatie informatiebeveiliging uit die onder meer gericht is op de beveiligingsnormen van de BRP en wet- en regelgeving reisdocumenten, DigiD en Suwinet. De zelfevaluatie heeft ook betrekking op de niet-informatiebeveiligingsaspecten van BAG, BGT en BRO. Het college van B&W stelt een Collegeverklaring ENSIA op over een aantal geselecteerde beveiligingsdoelstellingen. Een IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. Het college van B&W rapporteert vervolgens aan de gemeenteraad over de informatiebeveiliging. De ENSIA-tooling ondersteunt het uitvoeren van de zelfevaluatie en het beschikbaar stellen van relevante informatie aan de betrokken partijen met een toezichthoudende verantwoordelijkheid. ENSIA is in 2017 met een beperkte scope gestart. ENSIA zal de komende jaren middels een groeipad worden doorontwikkeld. Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in de Regieraad ENSIA[1] daarover afspraken. In 2017, voor verantwoordingsjaar 2018, is informatieverstrekking aan ‘Waar staat je gemeente’ toegevoegd aan de scope van ENSIA. Voor verantwoordingsjaar 2019 is door DGBRW aangegeven dat de informatiebeveiligingsaspecten van de BAG en BGT geen onderdeel uitmaken van de zelfevaluatie over informatiebeveiliging. Daarnaast is verantwoording over de BRO als verplicht onderdeel toegevoegd aan de scope van ENSIA.

Baseline Informatiebeveiliging Overheid (BIO)
In 2020 is de BIO binnen de overheid verplicht. Hiermee is de BIG vervallen. Binnen ENSIA is daarom de voor de zelfevaluatie opgestelde BIG-vragenlijst vervangen door een BIO-vragenlijst. Voor de beveiliging van Suwinet geldt dat de BIO, met een bijbehorend Basisbeveiligingsniveau 2, het vereiste gemeenschappelijke beveiligingsniveau invult. Het specifiek Suwinet Normenkader is niet langer van toepassing, de verantwoording over Suwinet is gericht op de naleving van een selectie van in de BIO geformuleerde normen en maatregelen.

[1] Voor 2019 heeft de Regieraad ENSIA deze afspraken gemaakt.



Afbeelding 1: procesplaat verantwoordingsstelsel ENSIA

De gemeentelijke producten

- **Paragraaf Informatiebeveiliging in het jaarverslag / separate Rapportage Informatiebeveiliging**
  Het college van B en W neemt in het jaarverslag in de paragraaf Bedrijfsvoering een aparte subparagraaf op over informatiebeveiliging. Hierin rapporteert het college aan haar toezichthouder (de gemeenteraad) over informatiebeveiliging. Deze werkwijze hebben gemeenten in de eerdergenoemde resolutie afgesproken.[2] In de praktijk blijkt dat met verslaglegging via de paragraaf bedrijfsvoering onvoldoende inhoud gegeven kan worden aan de verantwoording over informatiebeveiliging aan de gemeenteraad. Als alternatief adviseren we om de gemeenteraad te informeren via een aparte rapportage met daarin een beschrijving van de stand van zaken rond informatiebeveiliging. Daarmee wordt verstrengeling met de werkzaamheden van de financial auditor vermeden. Door de rapportage op basis van geheimhouding (in het kader van veiligheid) te verstrekken is er een beperkt risico dat de rapportage in onbevoegde handen terechtkomt. In bijlage 4 is een handreiking opgenomen voor het opstellen van de paragraaf Informatiebeveiliging en de separate rapportage. In toenemende mate kiezen gemeenten voor deze werkwijze omdat zij verwachten een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

[2] Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente, BALV 29-10-2013: “Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag”.

- **Collegeverklaring ENSIA inzake informatiebeveiliging**
  Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen hebben voldaan aan de voor de ENSIA-verantwoording geselecteerde normen en indien aan de orde welke onderdelen daarvan zijn uitgezonderd. Ook wordt melding gemaakt van eventuele verbetermaatregelen die de gemeente gaat treffen. Zie bijlage 2 voor de uitwerking van de Collegeverklaring ENSIA en de bijlagen bij de Collegeverklaring voor DigiD en Suwinet.

- **Zelfevaluatie informatiebeveiliging**
  Met de ingevulde zelfevaluatievragenlijst geeft het college van B en W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van deze vragenlijst is vastgesteld waar de normen van BRP en wet- en regelgeving reisdocumenten, en Suwinet aansluiten op de BIO-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIO-normen. Voor specifieke normen van BRP en wet- en regelgeving reisdocumenten en DigiD, zijn aanvullende vragen geformuleerd (als subvraag bij een generieke BIO-vraag of separaat van de BIO-vragen). De paragraaf Informatiebeveiliging / separate Rapportage Informatiebeveiliging en de Collegeverklaring ENSIA zijn gebaseerd op de zelfevaluatie.

- **Assurancerapport**
  Een bij de NOREA geregistreerde IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. Deze werkzaamheden van de IT-auditor duiden we ook wel aan als de IT-audit. De IT-auditor verklaart in het Assurancerapport dat de Collegeverklaring een getrouw beeld geeft. Getrouw betekent dat de Collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de Collegeverklaring. De NOREA stelt jaarlijks een format voor het Assurancerapport op. Dit format wordt na vaststelling aan de geregistreerde IT-audtiors aangeboden via de website van NOREA. Indien het College van B en W op basis van de IT-audit tot voortschrijdende inzichten komt betreffende de antwoorden van de zelfevaluatie, dan zal het College een notitie opstellen met per vraag een toelichting op het actuele inzicht[3].

- **Zelfevaluatie en verantwoording domeinspecifieke aspecten BAG, BGT en BRO**
  Met de ingevulde zelfevaluatie domeinspecifieke vragenlijsten voor de BAG, BGT en BRO geeft het college van B en W aan in hoeverre de domeinspecifieke beheersmaatregelen (anders dan voor informatiebeveiliging) zijn ingericht. Op basis van de zelfevaluatievragenlijsten voor de BAG, BGT en BRO worden met behulp van de ENSIA-tooling de bestuurlijke rapportages voor de genoemde basisregistraties samengesteld, die als basis dienen voor de verantwoording door gemeenten.

Informatieverstrekking met behulp van de ENSIA-tooling
Via de ENSIA-tooling stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie, de Collegeverklaring ENSIA en het Assurancerapport aan de minister van BZK ten behoeve van het toezicht op de BRP en Reisdocumenten, DigiD, de BAG, de BGT en de BRO. Namens de minister van BZK verwerkt Logius de verantwoordingsinformatie over DigiD. Verder bieden gemeenten via ENSIA transparantie aan de beheerder van de centrale omgeving van de GeVS4 (BKWI) ten behoeve van het jaarlijks opstellen van een totaaloverzicht van de beveiliging van de GeVS. Deze rapportage wordt uitgebracht aan het ketenoverleg GeVS en de minister van SZW. De Inspectie SZW houdt onafhankelijk signalerend toezicht op het functioneren van het stelsel werk en inkomen.

[3] De noodzaak van deze notitie is gelegen in het afronden van de zelfevaluatie per 31 december, waarna de antwoorden beschikbaar worden gesteld aan BKWI en niet meer kunnen worden gewijzigd. Met de notitie Voortschrijdend inzicht is voor alle betrokkenen binnen de gemeente een eenduidige en expliciete beschrijving beschikbaar over verschillen tussen de zelfevaluatie en de Collegeverklaring. De notitie vormt derhalve de brug tussen zelfevaluatie en Collegeverklaring en bevordert daardoor dat alle geconstateerde tekortkomingen in verbeterplannen worden betrokken.

Als de inspectie daartoe aanleiding ziet, kan de inspectie onderzoek doen naar de beveiliging van Suwinet bij gemeenten. Om de daarbij door de inspectie gevraagde informatie aan te leveren, kunnen gemeenten putten uit de via de ENSIA-tooling beschikbare verantwoordingsinformatie.

De hiernavolgende tabel geeft inzicht in de aard van de informatieverstrekking aan toezicht- en stelselhouders.

Overzicht aard informatieverstrekking aan toezichthouders

Type	**Organisatie**	**Type gegevens uit ENSIA-tooling**	**Datum opleveren ruwe data**	**Documenten uit ENSIA-tooling**	**Datum opleveren documenten**	**Publicatie**	**Aan stelselhouder**
BRP	RvIG	Ruwe data uit vragenlijst BIO zelfevaluatie	Na 1 mei 2021	Uittreksel BRP*	1 jan - 14 feb 2021	Rapportage BRP door minister BZK.	BZK
Wet- en regelgeving reisdocumenten	RvIG	Ruwe data uit vragenlijst BIO zelfevaluatie	Na 1 mei 2021	Uittreksel reisdocumenten*	1 jan - 14 feb 2021	Rapportage Reisdocumenten door minister BZK.	BZK
BAG	DGBRW	Ruwe data uit rapportage	Na 1 mei 2021	Bestuurlijke rapportage	1 jan - 1 mei 2021	Openbare publicatie van rapportages inclusief beoordelingsoverzicht.	BZK
BGT	DGBRW	Ruwe data uit rapportage	Na 1 mei 2021	Bestuurlijke rapportage	1 jan - 1 mei 2021	Openbare publicatie van rapportages inclusief beoordelingsoverzicht.	BZK
BRO	DGBRW	Ruwe data uit rapportage	Na 1 mei 2021	Bestuurlijke rapportage	1 jan - 1 mei 2021	Openbare publicatie van rapportages inclusief beoordelingsoverzicht.	BZK
Suwinet	BKWI	-	Na 1 mei 2021	Collegeverklaring en bijlage Suwinet Assurancerapport	1 jan - 1 mei 2021	Totaaloverzicht beveiliging GeVS door minister SZW.	SZW
DigiD	Logius	-	-	Collegeverklaring en bijlage(n) DigiD en TPM's Assurancerapport	1 jan - 1 mei 2021	Niet van toepassing	BZK
WSJG	Nvt	Ruwe data uit vragenlijst	Na 1 mei 2021	-	-	Publicatie via www.wsjg.nl	-

*Upload via Kwaliteitsmonitor

Samenwerkingsverbanden
Bij samenwerkingsverbanden blijft het college van B en W als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan het college van B en W om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken (zie nadere informatie in bijlage 3). Bij DigiD verantwoordt de 'Aansluithouder DigiD' zich via Logius aan de minister van BZK.

Algemene Verordening Gegevensbescherming (AVG)
Middels het voldoen aan de BIO-maatregelen wordt voor persoonsgegevens ook deels invulling gegeven aan de vereiste uit de AVG om passende organisatorische en technische maatregelen te nemen.

Verantwoording over gemeentelijke objecten
Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de jaarlijkse verantwoording over gemeentelijke objecten die onder de BIO vallen. Dit betreft objecten anders dan BRP, wet- en regelgeving reisdocumenten, DigiD en Suwinet. Hierbij kan een gemeente een groeipad toepassen. Op termijn is denkbaar dat de verantwoordingssystematiek doorgroeit naar een collegeverklaring (in control statement) die zowel de hiervoor genoemde objecten als de overige gemeentelijke objecten omvat.

Transparantie en benchmarking via 'Waar staat je gemeente?'
Via de website Waarstaatjegemeente.nl kunnen Nederlandse gemeenten aan de hand van thema's op gemeenteniveau zien hoe ze op verschillende gemeentelijke onderwerpen, waaronder Informatiebeveiliging, 'presteren'. Gemeenten kunnen hun eigen gegevens vergelijken met die van andere gemeenten. De informatie is openbaar toegankelijk. Gemeenten kunnen de data uit het dashboard meenemen in de besluitvorming, beleidsvorming, voor agendavorming, verantwoording of voor onderzoek. De ENSIA-tooling ondersteunt gemeenten met het beschikbaar stellen van gegevens over informatiebeveiliging aan 'Waar staat je gemeente'. De ENSIA-tooling voorziet in een specifiek voor 'Waar staat je gemeente' in te vullen vragenlijst en de mogelijkheid om de antwoorden in 'Waar staat je gemeente' in te lezen. Deze vragen zijn gebaseerd op de BIO. Gemeenten bepalen zelf of ze 'Waar staat je gemeente' met informatie over informatiebeveiliging vullen.

Afspraken over de ENSIA-verantwoording en het groeipad
Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in de Regieraad ENSIA[4] afspraken over de inhoud van de ENSIA-verantwoording. Het betreft afspraken over te selecteren objecten, normen/vragen en over opzet/bestaan/werking, rapportageperiode, rapportagemoment en de IT-audit. In de eerste jaren zal sprake zijn van een groeipad.

Dit groeipad heeft zich vertaald in de volgende toevoegingen binnen ENSIA:

Verantwoordingsjaar	Groei en ontwikkeling
2017	Eerste verantwoordingsjaar
2018	Aanvulling BRO (nog niet verplicht)
2019	BRO verplicht
2020	BIO vragenlijst en pilot WOZ
2021	Nieuwe tooling – nieuwe mogelijkheden

In 2020 is de ENSIA-verantwoordingssystematiek geëvalueerd. In het vervolg zal met enige regelmaat worden getoetst of ENSIA nog aan haar doelstellingen voldoet en voldoende aansluit op veranderingen in het landschap van toezichthouders en overheidsorganen (gemeenten, provincies en waterschappen).

De verantwoordingssystematiek dient optimaal bij te dragen aan het niveau van informatiebeveiliging van een gemeente. In de huidige vorm omvat de ENSIA-systematiek voor een aantal specifieke objecten een zelfevaluatie en voor Suwinet en DigiD aanvullen een IT-audit. In de situatie dat een IT-audit jaar op jaar bevestigt dat een object aan de gestelde eisen voldoet, kan de vraag gesteld worden of de audit-inspanningen nog voldoende waarde toevoegen. Het risicoprofiel rondom het betreffende object is immers met de getroffen maatregelen beperkt. Kunnen hiermee gemoeide middelen niet beter worden aangewend voor andere beheerprocessen en applicaties en zo bijdragen aan het algehele niveau van informatiebeveiliging?

Een uitwerking kan zijn dat gemeenten een meerjarige planning gaan toepassen voor hun controle-inspanningen en daarin jaarlijks een of meer thema's raken.

Binnen het groeipad van ENSIA worden er ook aanvullende onderdelen voorzien. In 2019 is de BRO verplichtend toegevoegd, op dit moment wordt onderzocht of de Wet Onroerende Zaken (WOZ) met de waarderingskamer als toezichthouder (onder verantwoordelijkheid van het ministerie van Financiën) kan worden toegevoegd. Verwacht wordt dat in de komende jaren aanvullende toezichthouders (niet alleen voor gemeenten maar ook voor provincies en waterschappen) zich zullen aansluiten bij ENSIA om vanuit hier één platform voor verantwoording te creëren.

Doordat er meerdere toezichthouders zullen aansluiten, is het heel goed denkbaar dat meerdere toezichthouders dezelfde onderdelen gaan uitvragen bij gemeenten, provincies en waterschappen. Hierbij dient onderscheid gemaakt te worden tussen algemene onderdelen en specifieke onderdelen. De algemene onderdelen (general controls) worden dan eenmalig ingevuld en aan meerdere toezichthouders verspreid. Specifieke onderdelen (applicatie controls) worden per toepassing uitgevraagd.

Ook wordt binnen het groeipad gekeken wanneer de tijd rijp is voor de mogelijkheid dat er gewerkt kan worden met risicogestuurde en thematische toetsingen in plaats van de huidige volledige toetsingen. Wanneer een gemeente, provincie of waterschap bijvoorbeeld drie jaar op een rij heeft aangetoond dat zij haar zaakjes goed geregeld heeft, is het mogelijk dat er dan vanuit de toezichthouder bepaalde thema's worden geselecteerd waarop wordt getoetst in plaats van dat zij elk jaar opnieuw volledig getoetst wordt.

[4] Voor 2020 heeft de Regieraad nog geen afspraken gemaakt.

Hoe meer toezichthouders de verantwoording van bronhouders via ENSIA laten verlopen, hoe meer het ook mogelijk is om te kijken naar de harmonisatie van de toetsing, het taalgebruik en de verantwoordingsafspraken om de verantwoording voor gemeenten, provincies en waterschappen richting de centrale overheid eenduidiger te maken.

Toetreding van nieuwe participanten vergt dat de governance toetredingsafspraken zal moeten vormgeven en de reeds opgestelde uittredingsafspraken eventueel zal herzien.
Middels het groeipad kan de ENSIA-systematiek met realistische jaarlijkse stappen doorgroeien naar een eindperspectief dat aansluit op de noodzaak en het ambitieniveau van gemeenten om het informatiebeveiligingsbeleid zowel bestuurlijk als ambtelijk in de organisatie te borgen.
Uitgangspunt is dat in het eindperspectief de verantwoording over BRP en wet- en regelgeving reisdocumenten, op aspecten anders dan informatiebeveiliging, op hetzelfde moment wordt afgelegd als de verantwoording over informatiebeveiliging. Daarbij wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken. Afspraken hierover kunnen onderdeel zijn van het groeipad. Het eindperspectief voor de harmonisatie op taalgebruik, tooling en verantwoordingsafspraken geldt ook voor de domeinspecifieke verantwoording over de BAG, BGT en BRO.

Afspraken over het jaar 2020

1. De verantwoordingsrichtljn Suwinet is vernieuwd. Het is met ingang van het verantwoordingsjaar 2020 volledig gebaseerd op de BIO-controls. De nieuwe richtlijn is vastgelegd in de Suwinet Verantwoordingsrichtlijn GeVS 2020 (versie 1.0)
2. De verantwoording is gematcht met de BIO-controls, en de Suwinet-vragen in de ENSIA-vragenlijst zijn verweven met de BIO-controls en maatregelen.
3. Een nieuwe Suwinet-guidance is beschikbaar gesteld.
4. Vanaf dit verantwoordingsjaar zal voor de verantwoording Suwinet gebruik gemaakt worden van de zogenaamde ‘carve-out’ methodiek. Deze werkwijze vertoont overeenkomsten met die voor de verantwoording op DigiD: de auditor van de Collegeverklaring steunt op de ontvangen TPM's van dienstenleveranciers. De auditor geeft assurance op de Collegeverklaring en de TPM’s, maar voert geen inhoudelijk onderzoek uit naar de juistheid en de beoordeling in de TPM’s en neemt dus ook geen verantwoordelijkheid voor de inhoud van de beschikbaar gestelde TPM’s.

Over het verantwoordingsjaar 2020 richt de IT-audit zich in ieder geval op de DigiD-normen en de voor Suwinet geselecteerde BIO-controls.

Tijdpad ENSIA in 2020 en in het eindperspectief
In onderstaande tabel is weergegeven welke deadlines voor ENSIA en de kwaliteitsmonitor zullen gelden. In de kolom 'eindperspectief' is het uiteindelijk te realiseren beeld geschetst.

Stap	2020	Eindperspectief
1. Afspraken maken over de verantwoording	Uiterlijk 1 april 2020	1 april
2. Invullen van de zelfevaluatie vragenlijsten	1 juli – 31 december 2020	1 juli – 31 december over opzet en bestaan per 31/12 en in de toekomst de werking over het kalenderjaar.
3. Afsluiten vragenlijsten met peildatum 31 december	Uiterlijk 31 december 2020	Uiterlijk 31 december
4. - Opstellen van een Collegeverklaring inclusief bijlagen. - Uitvoeren van een IT-Audit en het daarbij opstellen van een Assurancerapport. - Opstellen van een bestuurs-rapportage BAG, een bestuurs-rapportage BGT en een bestuursrapportage BRO. 5. Genereren van uittreksels informatiebeveiliging voor BRP en wet- en regelgeving reisdocumenten. 6. Beschikbaar stellen van de bestuursrapportage BRP en reisdocumenten	1 januari – 30 april 2021 1 januari – 14 februari 2021 Uiterlijk 14 februari 2021	1 januari – 30 april
7. Beschikbaar stellen van Collegeverklaring inclusief bijlagen, Assurancerapport en evt. TPM's voor BKWI en Logius op basis van IT-audit. - Beschikbaar stellen van de ruwe datarapportage (ingeleverde antwoorden) inzake de BIG vragen voor Suwinet. - Beschikbaar stellen van de bestuursrapportages voor BAG, BGT, BRO,	Uiterlijk 30 april 2021	Uiterlijk 30 april
8. Vaststellen van de jaarstukken door de gemeenteraad, toesturen van de jaarstukken aan de minister van BZK	Uiterlijk 15 juli 2021	Uiterlijk 15 juli[5]

[5] Wettelijke termijn voor het aanleveren van het jaarverslag en de jaarrekening aan de minister van BZK

Toelichting op de data van het proces in 2020:

- Deze data passen binnen bestaande wettelijke kaders van de stelsels die een onderdeel uitmaken van ENSIA.

Toelichting op de data in het eindperspectief:

1. Uitgangspunt is dat de verantwoording over informatiebeveiliging onderdeel wordt van de jaarlijkse verantwoordingscyclus bij gemeenten. De periode waarover in het jaarverslag verantwoording wordt afgelegd betreft daarbij het kalenderjaar. Voor de opzet en het bestaan van maatregelen is 31 december een logische datum. Het afleggen van verantwoording over de werking van maatregelen betreft het kalenderjaar.

2. Het geschetste tijdpad in de derde kolom is gericht op het eindperspectief ENSIA.
   Hierbij geldt:
   a. Waar nodig worden de bestaande wettelijke termijnen in lijn gebracht met het tijdpad in het eindperspectief.
   b. De verantwoordingssystematiek groeit in de komende jaren stapsgewijs toe naar het eindperspectief, er is sprake van een groeipad. Zo is bij de start van ENSIA besloten om de eerste jaren te starten met een verantwoording over opzet en bestaan en de werking op een later moment toe te voegen. Het groeipad kan, gezien de bestaande wettelijke termijnen, ook betrekking hebben op het tijdpad.

3. De Collegeverklaring ENSIA, het Assurancerapport en eventuele TPM’s dienen uiterlijk 30 april beschikbaar te worden gesteld middels een upload met de ENSIA-tooling. De datum van 30 april geeft voldoende ruimte voor het opstellen van de Collegeverklaring en het Assurancerapport en ligt vóór de start van de volgende jaarcyclus waarbij per 1 juli de zelfevaluatievragenlijst wordt opengesteld.

Bijlage 1 Detail Afspraken over de ENSIA-verantwoording 2020

1. Inleiding

In deze bijlage zijn de voor het verantwoordingsjaar 2020 gemaakte afspraken over de ENSIA-verantwoording nader beschreven. Deze afspraken zijn gemaakt in de regieraad van het project ENSIA. Het betreft afspraken over te selecteren objecten, normen/vragen en over opzet en bestaan, rapportageperiode, rapportagemoment en de IT-audit. Na afronding van dit project gaan vertegenwoordigers van gemeenten en betrokken departementen jaarlijks in de Regieraad ENSIA afspraken maken over de ENSIA-verantwoording.

Middels een groeipad kan de ENSIA-systematiek met realistische jaarlijkse stappen doorgroeien naar een eindperspectief dat aansluit op de noodzaak en het ambitieniveau van gemeenten om het informatiebeveiligingsbeleid zowel bestuurlijk als ambtelijk in de organisatie te borgen en daarbij te voldoen aan de eisen van BRP, wet- en regelgeving reisdocumenten, DigiD en Suwinet, GeVS,.

Uitgangspunt is dat in het eindperspectief de verantwoording over BRP, wet- en regelgeving reisdocumenten, BAG, BGT en BRO op aspecten anders dan informatiebeveiliging, op hetzelfde moment wordt afgelegd als de verantwoording over informatiebeveiliging. Daarbij wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken. Afspraken hierover kunnen onderdeel zijn van het groeipad.

De wet Basisregistratie Ondergrond (BRO) is per 1 januari 2018 in werking getreden. Gemeenten zijn wettelijk verplicht zich te verantwoorden over de BRO. De verantwoording van de BRO richt zich op niet-informatiebeveiligingsaspecten. Voor gemeenten is het afleggen van verantwoording over de BRO via ENSIA efficiënter in vergelijking met het alternatief waarbij gemeenten separaat van ENSIA verantwoording afleggen. De toezichtparagraaf is niet helder in de wet meegenomen en wordt nog in afstemming met de achterban aangepast. Vanaf 2019 leggen bronhouders verantwoording af over de BRO. De tijdslijnen zijn overeenkomstig aan de BAG en BGT.

2. Normering

Voor het verantwoordingsjaar 2020 zijn in de volgende documenten het verantwoordingskader/de van kracht zijnde normen geformuleerd voor de objecten waarover verantwoording wordt afgelegd:

- BIO -1.04;
- Verantwoordingsrichtlijn GeVS 2020, versie 1.0;
- Digid: Het DigiD normenkader 2.0;
- BAG: Wet en regelgeving BAG;
- BGT: Wet en regelgeving BGT;
- BRP: Wet en regelgeving BRP;
- BRO: Wet en regelgeving BRO;
- PUN: Wet en regelgeving reisdocumenten;
- PNIK: Wet en regelgeving reisdocumenten.

3. Reikwijdte zelfevaluatie informatiebeveiliging

Met de ingevulde zelfevaluatievragenlijst geeft het college van B en W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van de zelfevaluatievragenlijst is vastgesteld waar de normen van BRP, wet- en regelgeving reisdocumenten en Suwinet, aansluiten op de BIO-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIO-normen. Voor specifieke normen van BRP, wet- en regelgeving reisdocumenten, DigiD en Suwinet zijn aanvullende vragen geformuleerd. De DigiD-norm kent een andere scope dan de BIG en ook een ander object van onderzoek. DigiD richt zich op de webomgeving van de DigiD-aansluiting met een geheel eigen set van normen. Om die reden zijn de DigiD-vragen losgeweekt van de ENSIA-vragenlijst. Matching met BIO-normen is daarom niet van toepassing.

Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de verantwoording in de paragraaf Informatiebeveiliging over de overige gemeentelijke objecten die onder de BIO vallen (informatie over de beveiliging in brede zin).

4. Reikwijdte Collegeverklaring ENSIA inzake informatiebeveiliging en IT-audit

De Collegeverklaring ENSIA en de IT-audit hebben betrekking op opzet en bestaan van de beheersingsmaatregelen per 31 december 2020 voor de gearceerde normen (controls) en objecten in de onderstaande tabellen.

Het DigiD normkader 2.0

Als eerste is er de DigiD-norm met een andere scope dan de BIO en ook met een ander object van onderzoek. DigiD richt zich op de webomgeving van de DigiD-aansluiting met een geheel eigen set van normen. Daarnaast moet een gemeente de DigiD-audit laten uitvoeren per aansluiting. Daarnaast is een deel van de DigiD-norm soms van toepassing op de gemeente en soms op een leverancier en soms op beiden. Om die reden zijn de DigiD-vragen losgeweekt van de ENSIA-vragenlijst. Matching met BIO-normen is daarom niet meer van toepassing.

Nr	Beschrijving van de beveiligingsrichtlijn
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.

Nr	Beschrijving van de beveiligingsrichtlijn
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

In de zelfevaluatie is het DigiD-normenkader 2.0 verwerkt. Vanuit de zelfevaluatie wordt aan Logius in een voor hen verwerkbaar format per DigiD aansluiting informatie door de gemeente verstrekt (de documenten moeten in PDF/A-formaat aangeleverd worden, per document moet er één PDF/A-bestand worden aangeleverd). De in samenwerking met NOREA uitgewerkte guidance DigiD is uitgangspunt voor het uitvoeren van werkzaamheden door de gemeenten en de auditors.

Suwinet Verantwoordingsrichtlijn GeVS 2020
Als tweede is er de Suwinetverantwoordingsrichtlijn. Deze richt zich net zoals de BIO (generiek) op de bedrijfsvoering, met als focus de sociale keten binnen de gemeente. De verantwoording is gematcht met de BIO-controls, en zijn de Suwinet-vragen in de ENSIA-vragenlijst verweven met de BIO-controls en maatregelen.

Versie BIO:					
Hoofdstuk	**Nummer control**	**Toelichting control**	**Nummer maatregel**	**Toelichting maatregel**	**BBN**
5. Informatiebeveiligingsbeleid	5.1.1.	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de	1

Versie BIO:					
Hoofdstuk	**Nummer control**	**Toelichting control**	**Nummer maatregel**	**Toelichting maatregel**	**BBN**
				informatiebeveiligings functie, waaronder verantwoordelijkhede n, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkhede n voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseis en en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligings beleid wordt geëvalueerd; f) de bevordering van het beveiligings-bewustzijn.	
5. Informatiebeveiligings-beleid	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	5.1.2.1	Het informatiebeveiligings beleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheids verdeling, beoordeeld en zo nodig bijgesteld.	1
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkhede n en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	1
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.3	De rol en verantwoordelijkhede n van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	1
6. Organiseren van informatiebeveiliging	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	1

Versie BIO:					
Hoofdstuk	**Nummer control**	**Toelichting control**	**Nummer maatregel**	**Toelichting maatregel**	**BBN**
7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	1
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentifica-ties.	1
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	1
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverlening sprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	1
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverlening sprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	1
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	1
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	2
9. Toegangsbeveiliging	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij	9.2.6.1	Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering van	2

Versie BIO:					
Hoofdstuk	**Nummer control**	**Toelichting control**	**Nummer maatregel**	**Toelichting maatregel**	**BBN**
		beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.		functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.	
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) wanneer cryptografie ingezet wordt; (b) wie verantwoordelijk is voor de implementatie; (c) wie verantwoordelijk is voor het sleutelbeheer; (d) welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast; (e) de wijze waarop het beschermingsniveau vastgesteld wordt; (f) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.	2
12. Beveiliging bedrijfsvoering	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	12.1.1.1	Er zijn bedieningsprocedures voor alle gebruikers.	1
12. Beveiliging bedrijfsvoering	12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	1

Versie BIO:					
Hoofdstuk	**Nummer control**	**Toelichting control**	**Nummer maatregel**	**Toelichting maatregel**	**BBN**
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	1
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en –procedures binnen haar verantwoordelijkheids gebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	2

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente <naam gemeente>

Gemeentelijk kenmerk collegeverklaring:	

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente <naam gemeente>

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate de gemeente <naam gemeente> voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[1] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2020.

De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen [eventuele afwijkingen] en waar deze belegd zijn, is opgenomen in de bijlagen:

bijlage 1 DigiD met kenmerk [kenmerk]

bijlage 2 Suwinet met kenmerk [kenmerk]

Verklaring college

[[Indien volledig wordt voldaan aan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2020 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD en Suwinet.]]

[[Bij uitzonderingen: [Het college verklaart dat voor [DigiD] [en] [Suwinet] niet aan alle normen wordt voldaan. Wij hebben [een] verbeterplan[nen] opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.]]

[1] ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD (1)	[Ja] [Nee]	[Ja] [Nee]
DigiD (2)	[Ja] [Nee]	[Ja] [Nee]
DigiD (3)	[Ja] [Nee]	[Ja] [Nee]
DigiD (4)	[Ja] [Nee]	[Ja] [Nee]
DigiD (5)	[Ja] [Nee]	[Ja] [Nee]
DigiD (6)	[Ja] [Nee]	[Ja] [Nee]
DigiD (7)	[Ja] [Nee]	[Ja] [Nee]
DigiD (8)	[Ja] [Nee]	[Ja] [Nee]
DigiD (9)	[Ja] [Nee]	[Ja] [Nee]
Suwinet voor SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]
Suwinet voor niet-SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]

[Plaatsnaam], [datum]

College van B en W gemeente <naam gemeente>

[naam/namen en functie('s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

Collegeverklaring informatiebeveiliging DigiD

Gemeente <naam gemeente>

Gemeentelijk kenmerk collegeverklaring:	

Collegeverklaring informatiebeveiliging DigiD

Gemeente <naam gemeente>

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate de gemeente <naam gemeente> voldoet aan de informatiebeveiligingsnormen voor DigiD.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[2] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouder van DigiD, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD op 31 december 2020.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD. Het overzicht van normen [eventuele afwijkingen] en waar deze belegd zijn, is opgenomen in de bijlagen:

bijlage 1 DigiD met kenmerk [kenmerk]

Verklaring college

[[Indien volledig wordt voldaan aan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2020 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD.]]

[[Bij uitzonderingen: [Het college verklaart dat voor DigiD niet aan alle normen wordt voldaan. Wij hebben een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.]]

[2] ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD (1)	[Ja] [Nee]	[Ja] [Nee]
DigiD (2)	[Ja] [Nee]	[Ja] [Nee]
DigiD (3)	[Ja] [Nee]	[Ja] [Nee]
DigiD (4)	[Ja] [Nee]	[Ja] [Nee]
DigiD (5)	[Ja] [Nee]	[Ja] [Nee]
DigiD (6)	[Ja] [Nee]	[Ja] [Nee]
DigiD (7)	[Ja] [Nee]	[Ja] [Nee]
DigiD (8)	[Ja] [Nee]	[Ja] [Nee]
DigiD (9)	[Ja] [Nee]	[Ja] [Nee]

[Plaatsnaam], [datum]

College van B en W gemeente <naam gemeente>

[naam/namen en functie('s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

Collegeverklaring informatiebeveiliging Suwinet

Gemeente <naam gemeente>

Gemeentelijk kenmerk collegeverklaring ENSIA:	

Collegeverklaring informatiebeveiliging Suwinet

Gemeente <naam gemeente>

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate de gemeente <naam gemeente> voldoet aan de informatiebeveiligingsnormen voor Suwinet.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[3] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouder Suwinet, te weten het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor Suwinet op 31 december 2020.

De beheersingsmaatregelen inzake Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake Suwinet af. Het overzicht van normen [eventuele afwijkingen] en waar deze belegd zijn, is opgenomen in de bijlagen:

bijlage 1 Suwinet met kenmerk [kenmerk]

Verklaring college

[[Indien volledig wordt voldaan aan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2020 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake Suwinet.]]

[[Bij uitzonderingen: [Het college verklaart dat voor Suwinet niet aan alle normen wordt voldaan. Wij hebben [een] verbeterplan[nen] opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.]]

[3] ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
Suwinet voor SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]
Suwinet voor niet-SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]

[Plaatsnaam], [datum]

College van B en W gemeente <naam gemeente>

[naam/namen en functie('s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

Bijlage 3. De invulling van verantwoordelijkheden in samenwerkingsverbanden

Wat is de aanleiding?
Eind 2013 is in de BALV de resolutie 'Informatieveiligheid randvoorwaarde voor een professionele gemeente aangenomen. In de resolutie hebben gemeenten afgesproken de BIG (Baseline Informatie veiligheid Gemeenten) te hanteren als gezamenlijk normenkader. Gemeenten zullen zich in het jaarverslag gaan verantwoorden over informatieveiligheid aan de eigen toezichthouder (horizontale verantwoording). Gemeenten hebben gevraagd aan Min BZK om de bestaande verantwoordingen op het vlak van informatiebeveiliging te stroomlijnen. In de huidige situatie hebben gemeenten te maken met minimaal vijf verantwoordingen op het vlak informatiebeveiliging. Deze verschillen qua diepgang, timing en gevraagde assurance, terwijl zij steeds hetzelfde thema belichten.

Min BZK heeft in samenwerking met betrokken departementen en VNG het project ENSIA gestart en (Eenduidige Normatiek Single Information Audit) heeft tot doel om het horizontale verantwoordingsproces rond informatiebeveiliging bij gemeenten in te richten op basis van een zelfevaluatie (met als basis de BIG). De betrokken departementen vervolgens krijgen vanuit dit proces de voor hen relevante informatie. De zelfevaluatie leidt tot een gemeentelijke collegeverklaring informatiebeveiliging die door een IT-auditor wordt onderzocht. De departementen 'steunen' als het ware op de resultaten van dit verantwoordingsproces.

Kern van het geheel is de eigen verantwoordelijkheid van het gemeentebestuur voor de inrichting van deze informatiebeveiliging. Die verantwoordelijkheid is eenduidig zolang de diverse relevante processen zich binnen de gemeentelijke organisatie afspelen. De praktijk is echter dat gemeenten voor een aantal taken de samenwerking opzoekt. En natuurlijk geldt ook in die situatie dat uiteindelijk de gemeentelijk bestuurder verantwoordelijkheid kent voor de processen die in die samenwerking worden afgehandeld. De vraag ligt voor hoe aan die verantwoordelijkheid invulling te geven en hoe dat vervolgens moet landen in de ENSIA-verantwoording.

De WGR en informatiebeveiliging
(Inter) gemeentelijke samenwerkingen zijn geënt op Wet Gemeenschappelijke regelingen (WGR). De wet beschrijft een aantal mogelijke juridische mogelijkheden om samenwerkingen vorm te geven. En beschrijft daarbij op de hoofdlijn de wijze waarop per construct verantwoording moet/kan worden afgelegd. De wet gaat bij geen enkele beschreven samenwerking in op het thema informatiebeveiliging en laat de invulling daarvan over aan de samenwerkende partijen die daarover al dan niet afspraken (wensen te) maken. De wijze waarop die verantwoording vorm krijgt, is ook afhankelijk van de specifieke juridische constructie van het samenwerkingsverband. Een openbaar lichaam (als zelfstandig rechtspersoon) heeft daartoe andere mogelijkheden dan bijvoorbeeld een BV of stichting. Een centrumgemeenteconstructie kent ook weer zijn eigen beperkingen in het afleggen van verantwoording. De wet geeft verder weinig kapstokken om aan die verantwoordelijkheid invulling te geven.

Handreiking Informatieveiligheid en intergemeentelijke samenwerking
In deze handreiking is al het volgende opgenomen:

- *Een portefeuillehouder binnen het college van B en W is verantwoordelijk voor de (prioritering van) beveiliging van informatie binnen de bedrijfs(werk)processen. Deze verantwoordelijkheid wijzigt niet op het moment dat de gemeente besluit om een bepaalde dienst of taak uit te besteden of samen met andere gemeenten (intergemeentelijk) uit te voeren. De gemeente blijft als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan de portefeuillehouder om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken. In de handreiking informatieveiligheid en intergemeentelijke samenwerking worden aanzetten gegeven hoe die verantwoording invulling te geven. https://vng.nl/files/vng/publicaties/2015/20150731_informatieveiligheid-en-intergemeentelijke.pdf. In dit rapport wordt ingegaan op publiekrechtelijke samenwerkingsvormen (openbaar lichaam, centrumgemeente), privaatrechtelijke samenwerkingsvormen en ketens. In het rapport wordt het volgende al behandeld: afspraken over de BIG, aanvullende afspraken tov de BIG, afleggen van verantwoording en audits. Er is dus al het een en ander verwoord als het gaat over de gemeentelijke verantwoordelijkheid bij samenwerking.*

Om invulling te geven aan de specifieke verantwoordelijkheid rond (intergemeentelijke) informatiebeveiliging suggereren de bij ENSIA betrokken auditors de volgende aanvulling op deze handreiking:

- *Bij publiekrechtelijke en privaatrechtelijke samenwerkingsvormen is het uitgangspunt dat de gemeente voor de bij de samenwerkingsvorm ondergebrachte activiteiten verantwoordelijk blijft voor het aantoonbaar voldoen aan de BIG (c.q. de beveiligingsafspraken). De verantwoording van de gemeente over het voldoen aan de BIG omvat derhalve ook de activiteiten van de samenwerkingsvormen voor de gemeente. De gemeente laat zich door de samenwerkingsvorm informeren over het voldoen van de ondergebrachte activiteiten aan de BIG (c.q. beveiligingsafspraken) en de gemeente stelt de juistheid en volledigheid van de ontvangen verantwoording van de samenwerkingsvorm vast. De gemeente kan dit zelf doen of de samenwerkingsvorm vragen hiervoor een auditor in te schakelen.*

Kern van deze aanvulling is dat de gemeenten binnen het samenwerkingsverband afspreken hoe zij zich wil laten informeren over de gerealiseerde informatiebeveiliging en op welke wijze deze informatie landt in de zelfevaluatie. De ontwikkelde tool biedt daarvoor beperkte functionaliteit. Als met het samenwerkingsverband een vorm van gebruik van TPM's is ingericht, kunnen gemeenten daar (desgewenst) uiteraard op steunen.

- *Bij ketens heeft iedere deelnemer een zelfstandige verantwoordelijkheid. Iedere deelnemer van de keten legt verantwoording af over het voldoen aan de BIG en laat deze verantwoording **desgewenst** van zekerheid voorzien door een auditor. De ketenpartners/ ketenregisseur stelt vast dat er niets tussen de wal en het schip valt en dat de verantwoordingen de gehele keten afdekken.*

Kern van deze aanvulling is dat aanvullend op de reguliere verantwoording van een ketenpartner wordt bewaakt dat alle in de keten betrokken partijen voldoen aan de gemaakte afspraken. Concreet betekent dit dat binnen de keten in ieder geval de afspraak moet bestaan dat voldaan wordt aan BIG (of vergelijkbare baseline). Inmiddels is de BIG vervangen door de BIO.

Binnen ENSIA is vooralsnog de afspraak dat minimaal BRP, wet- en regelgeving reisdocumenten, SUWI en DigiD in de zelfevaluatie betrokken zijn. De evaluatie betreft het voldoen aan de volle breedte van de BIO op dit vlak. De audit in 2021 over 2020 spitst zich toe op een beperkt aantal normen.

De verantwoordelijkheid van gemeenten betreft uiteraard alle vormen van samenwerking. Voorstelbaar is dat de focus voor gemeenten allereerst ligt bij die samenwerkingsverbanden die binnen de scope van ENSIA vallen.

Bijlage 4. Handreiking Paragraaf Informatiebeveiliging in het jaarverslag van gemeenten / separate Rapportage Informatiebeveiliging

Met de VNG-resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ van november 2013 hebben gemeenten afgesproken om de informatiebeveiliging op orde te krijgen en te houden. In deze resolutie is onder meer afgesproken dat de gemeente in het jaarverslag een aparte paragraaf opneemt over informatiebeveiliging. Met deze paragraaf verantwoordt een college van B en W zich aan de gemeenteraad over informatiebeveiliging in brede zin (‘horizontale verantwoording’). Dit betreft onder meer gemeentelijke doelstellingen en afspraken over informatiebeveiliging. Daaronder zijn de afspraken die gemaakt zijn voor de ENSIA-verantwoording informatiebeveiliging (‘verticale verantwoording’). Over (het nakomen van) de ENSIA-afspraken doet de gemeente ook een specifieke uitspraak in de ‘Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet)’[0]. De IT-auditor doet een uitspraak over de juistheid en volledigheid van de Collegeverklaring ENSIA.

De (sub-)paragraaf Informatiebeveiliging wordt opgenomen in de paragraaf Bedrijfsvoering van het jaarverslag (als onderdeel van de jaarstukken, naast de jaarrekening). Om gemeenten te faciliteren de paragraaf Informatiebeveiliging op eenduidige wijze op te stellen, volgt hierna een format met de ingrediënten daarvan.

Voor grotere aandacht voor het onderwerp informatiebeveiliging in de Raad, kiezen gemeenten er in toenemende mate voor om een separate Rapportage Informatiebeveiliging aan de Raad te verstrekken. Deze rapportage omvat zowel de informatie over informatiebeveiliging in brede zin als de strekking van de Collegeverklaring ENSIA. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

[0] Over het verantwoordingsjaar 2019 richt de IT-audit zich op de DigiD-normen en een selectie van Suwinet-normen (zie bijlage 1). Hierbij is een groeipad voorzien.

Paragraaf Informatiebeveiliging in het jaarverslag óf separate Rapportage Informatiebeveiliging

IB-beleid, doelstellingen en afspraken Bestuurlijke beschrijving van de belangrijkste gemeentelijke doelstellingen van het informatiebeveiligingsbeleid, waaronder onder meer: “zorgvuldig omgaan met informatie”, “betrouwbare en continue dienstverlening”, “voldoen aan wet- en regelgeving (privacy)” en “beheersen van risico’s” (Governance, Risk en Compliance). Beschrijf hier ook specifieke doelstellingen zoals: • De ambities om te voldoen aan de BIO als basisnormenkader voor de IB maatregelen. • Het nakomen van de afspraken over de ‘ENSIA verantwoording’.
Algemeen beeld en resultaten afgelopen periode Beschrijving van de (belangrijkste) activiteiten / resultaten die in het afgelopen jaar hebben bijgedragen aan het behalen van de doelstellingen. “In 2020 heeft de gemeente ..”
“Disclaimer” Wellicht verstandig om iets op te nemen over de illusie van 100% veiligheid.
Beheersmaatregelen IB Geef een overzicht van de belangrijkste maatregelen die bijdragen aan het realiseren van de IB-doelstellingen: • Organisatie en TBV’s, awareness • Organisatorische en technische maatregelen • Information Security Management System (ISMS) / PDCA
Realisatie doelstelling IB Beleid (effectiviteit beheersmaatregelen en risico’s) Geef aan in welke mate de afgesproken doelstellingen voor 2019 zijn gerealiseerd (in hoeverre beheersmaatregelen effectief zijn in relatie tot realiseren van het IB Beleid en welke (*specifieke) doelstellingen en risico’s nog aandacht behoeven (en waarvoor nog maatregelen getroffen moeten worden). Let wel, hier wel omzichtig zijn met wat naar buiten gebracht wordt. Geef aan hoe dit is getoetst. Onder meer met de (‘brede’) Zelfevaluatie Informatiebeveiliging en eventueel andere instrumenten (ISMS). Geef ook aan wat de reikwijdte is van de Zelfevaluatie Informatiebeveiliging. **Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet** Bij zowel een paragraaf Informatiebeveiliging in het Jaarverslag als een separate Rapportage Informatiebeveiliging wordt hier de strekking van de Collegeverklaring ENSIA opgenomen.
Incidenten Rapportage (privacy) incidenten / datalekken en de afhandeling daarvan.
Meerjarenperspectief Beschrijving van aandachtspunten, doelstellingen en resultaatafspraken (planning) volgende periode. De stappen en het tijdspad voor het implementeren van de BIO. Beschrijf per stap de reikwijdte (systemen en ICT-beheerprocessen[0]).

[0] Bijvoorbeeld Logische Toegangsbeveiliging (LTB).