

ENSIA

Notitie Verantwoordingsstelsel Verantwoordingsjaar 2024

Versie 1.0 – 7 december 2023

Inhoudsopgave

Doel van de Notitie Verantwoordingsstelsel ENSIA.....	2
WAT IS ENSIA.....	2
UITGANGSPUNTEN VAN ENSIA	2
STURING OP ENSIA	4
REIKWIJDTE VAN ENSIA IN VERANTWOORDINGSJAAR 2024.....	4
Wijze van verantwoorden	5
MIJLPALEN EN DEADLINES IN HET VERANTWOORDINGSJAAR 2024	5
FASES IN HET VERANTWOORDINGSJAAR	6
WIJZE VAN VERANTWOORDEN VOOR NIET-GEMEENTEN	7
INFORMATIEVERSTREKKING AAN HET RIJK MET BEHULP VAN HET ENSIA-PLATFORM	7
Nieuw in het verantwoordingsjaar 2024	9
Bijlage 1 - De invulling van verantwoordelijkheden in samenwerkingsverbanden.....	10
AANLEIDING VOOR HET ONTSTAAN VAN ENSIA	10
DE WGR EN INFORMATIEBEVEILIGING	10
INFORMATIEVEILIGHEID EN INTERGEMEENTELIJKE SAMENWERKING	10
Bijlage 2 - Verantwoordingsnormen en richtlijnen 2024.....	12
HET DIGID-NORMKADER 3.0	12
SUWINET VERANTWOORDINGSRICHTLIJN GEVS 2022	13
Bijlage 3 - Format Collegeverklaring ENSIA en bijlagen DigiD en Suwinet.....	19
Bijlage 4 - Bouwstenen oplegnotitie separate rapportage Informatiebeveiliging aan gemeenteraad/publicatie in het jaarverslag van gemeenten	36
Bijlage 5 - Informatieverstrekking aan toezicht- en stelselhouders	37

Doel van de Notitie Verantwoordingsstelsel ENSIA

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. Het document wordt tenminste eenmaal per jaar bijgesteld en vastgesteld op basis van de nieuwe ontwikkelingen in het verantwoordingsjaar.

Wat is ENSIA

Burgers verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). Dat zorgt niet alleen voor betrouwbaarheid, maar ook voor een goede kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen.

ENSIA is in 2017 ontstaan op initiatief van gemeenten en de ministeries van BZK en SZW en is in het leven geroepen om een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te bieden. Inmiddels gebruiken ook provincies, waterschappen en enkele onderdelen binnen de rijksoverheid ENSIA om zich te verantwoorden over de staat van informatiebeveiliging op basis van de BIO (Baseline Informatiebeveiliging Overheid).

ENSIA is eveneens geschikt gebleken voor het afleggen van verantwoording op het gebied van datakwaliteit/data-integriteit. Voor de verantwoording ten aanzien van de geobasisregistraties ligt hierop de nadruk.

Aangezien gemeenten de meest intensieve gebruikers zijn van ENSIA, is op de omschrijvingen in deze notitie vooral de gemeentelijke terminologie toegepast. De onderliggende uitgangspunten, normen en processtappen zijn echter op alle deelnemende organisaties van toepassing.

Uitgangspunten van ENSIA

Inzet van ENSIA is dat de verantwoording over informatiebeveiliging op grond van de BIO onderdeel is van de jaarlijkse verantwoordingscyclus bij de deelnemende organisaties. De periode waarover verantwoording wordt afgelegd is het kalenderjaar.



De organisatie legt intern verantwoording af aan haar bestuur. De eigen verantwoordelijkheid is leidend: Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de jaarlijkse verantwoording. Aan de gemeenteraad legt het college van B&W verantwoording af in hoeverre zij in generieke zin in control is voor wat betreft de informatiebeveiliging op basis van de BIO. Bij deze verantwoording worden ook de verantwoording over de Basisregistratie Personen (BRP), wet- en regelgeving Reisdocumenten, DigiD en Suwinet betrokken. Daarnaast wordt intern verantwoording afgelegd over de datakwaliteit en -integriteit van BAG, BGT en BRO. Hierbij kan een gemeente een groepspad toepassen.

Gemeenten leggen verantwoording af aan (de toezichhouders van) het rijk verantwoording over de DigiD-aansluitingen, de Suwinet-services, de Basisregistratie Personen, de Reisdocumenten en de geobasis-registraties (BAG, BGT en BRO).

Kern van de verantwoording 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 dat ook in de situatie waarin taken zijn gemandateerd of gedelegeerd aan externe partijen uiteindelijk de gemeentelijk bestuurder verantwoordelijk is voor de ketenprocessen die in gehele samenwerkingsketen worden uitgevoerd (dus inclusief de onderaannemers waarvan deze externe partijen zich bedienen, zoals IT-serviceproviders).

Bij samenwerkingsverbanden blijft het college van B&W als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan het college van B&W om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken (zie nadere informatie in bijlage 1).

De 'ENSIA-verantwoording informatiebeveiliging' gaat uit van het principe van Single Information & Single Audit (SISA). Dit betekent éénmalige informatieverstrekking en éénmalige IT-audit. Dit betekent onder andere dat:

- De verantwoording aan het rijk plaatsvindt op basis van de interne verantwoording.
- Vanaf 2020 is de BIO binnen de overheid verplicht.

De verantwoording over informatiebeveiliging in ENSIA is gebaseerd op een BIO-vragenlijst. Gemeenten gebruiken deze vragenlijst om een zelfevaluatie uit te voeren op informatiebeveiliging. In deze vragenlijst zijn ook de beveiligingsnormen van de BRP, Reisdocumenten, en Suwinet betrokken.

Voor de beveiliging van Suwinet geldt dat de BIO, met een bijbehorend Basisbeveiligingsniveau 2, het vereiste gemeenschappelijke beveiligingsniveau is. De verantwoording over Suwinet is gericht op de naleving van een selectie van in de BIO geformuleerde normen en maatregelen. De DigiD-norm kent een andere scope dan de BIO en ook een andere scope van onderzoek. DigiD richt zich op de webomgeving van de DigiD-aansluiting met een geheel eigen set van normen. Om die reden bevat ENSIA een specifieke vragenlijst voor DigiD.

Het college van B&W stelt een Collegeverklaring ENSIA op over een aantal vooraf geselecteerde beveiligingsnormen. Een IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. Het college van B&W rapporteert vervolgens onder geheimhouding aan de gemeenteraad over de informatiebeveiliging. Naast deze vragenlijsten bevat ENSIA ook vragenlijsten voor de geobasisregistraties (BAG, BGT en BRO). Hierin ligt het accent op datakwaliteit en -integriteit.

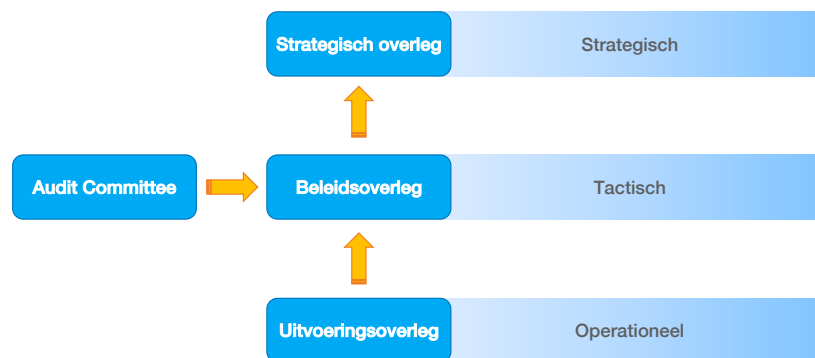
- De ENSIA-platform ondersteunt zowel het uitvoeren van de zelfevaluatie als het beschikbaar stellen van relevante verantwoordingsinformatie aan de betrokken partijen met een toezichhoudende verantwoordelijkheid.
- Voor de verantwoording rond de Algemene Verordening Gegevensbescherming (AVG) bestaan separate procedures waarvoor de Functionaris Gegevensbescherming verantwoordelijk is. Door het voldoen aan de BIO-maatregelen wordt voor persoonsgegevens voor een deel invulling gegeven aan de vereiste uit de AVG om passende organisatorische en technische maatregelen te nemen. De functionaris Gegevensbescherming kan hiervoor eventueel verwijzen naar/putten uit de zelfevaluatie ENSIA.
- Stelselhouders zetten in op het in lijn brengen van de bestaande wettelijke termijnen met de jaarplanning van de ENSIA-verantwoording.
- Via de website Waarstaatjegemeente.nl kunnen Nederlandse gemeenten aan de hand van thema's op gemeenteniveau aangeven hoe ze op verschillende gemeentelijke onderwerpen, waaronder Informatiebeveiliging, 'presteren'. Gemeenten kunnen hun eigen scores vergelijken

met die van andere gemeenten. De informatie is openbaar toegankelijk en het ENSIA-platform ondersteunt gemeenten met het beschikbaar stellen van gegevens over informatiebeveiliging aan 'Waar staat je gemeente'.

Het ENSIA-platform 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.

Sturing op ENSIA

De deelnemers aan ENSIA hebben verschillende verantwoordelijkheden en belangen. Om een evenwichtige sturing op ENSIA te waarborgen, is bij de start van ENSIA ook de besturing van ENSIA vastgelegd. De invulling van de besturing is beschreven in de Notitie Governance en Financiering ENSIA¹. Het hoogste orgaan in deze besturing is het Strategisch overleg, waar besluiten worden genomen op stelselniveau. In het Strategisch overleg hebben vertegenwoordigers op strategisch niveau van de stelselverantwoordelijke, de stelselhouders, gemeenten, de Audit Dienst Rijk (ADR) en de VNG zitting. Op tactisch niveau bestaat het Beleidsoverleg waarin de besluitvorming voor het Strategisch overleg wordt voorbereid. Op uitvoerend niveau bestaat het Uitvoeringsoverleg waarin operationele zaken worden besproken en waarin wijzigingsvoorstellen worden beoordeeld en, bij goedkeuring, aan het Beleidsoverleg worden voorgelegd. Daarnaast bestaat het Audit Committee waarin audittechnische zaken worden besproken. Het Audit Committee is adviserend aan het Beleidsoverleg.



Reikwijdte van ENSIA in verantwoordingsjaar 2024

Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in het Strategisch overleg ENSIA afspraken over de inhoud van de ENSIA-verantwoording voor het komende verantwoordingsjaar. Het betreft afspraken over te selecteren scope, normenkaders, vragen en over opzet/bestaan/werking, rapportageperiode, rapportagemoment en de IT-audit.

Een overzicht van de vigerende normen(kaders) en richtlijnen weergegeven voor het verantwoordingsjaar 2024 wordt gegeven in bijlage 2.

Net als in voorgaande jaren vindt in het verantwoordingsjaar 2024 de verantwoording plaats over *opzet en bestaan* van controls (*werking* zal op een later moment worden toegevoegd).

Ten aanzien van de domeinen DigID en Suwinet is het verplicht om een bij de NOREA geregistreeerde IT-auditor de Collegeverklaring te laten controleren. Deze stelt een Assurancerapport op dat wordt meegestuurd met de verantwoordingsstukken. Het staat gemeenten vrij om ook andere onderdelen van ENSIA-verantwoording te laten onderzoeken door een IT-auditor; hiertoe is geen verplichting.












¹ Notitie Governance en financiering ENSIA 2021 versie 1.2 van 2 december 2021.

Wijze van verantwoorden

De onderstaande plaat geeft een overzicht van de mijlpalen en fases in het ENSIA-verantwoordingsjaar. Hieronder worden de diverse onderdelen toegelicht.

Mijlpalen en deadlines in het verantwoordingsjaar 2024

De mijlpalen en deadlines voor het verantwoordingsjaar 2024 zijn in de onderstaande afbeelding opgenomen:



ENSIA	Verantwoording over informatiebeveiliging aan gemeenteraad		Verantwoording aan toezichthouders
Zelfevaluatie 	<ul style="list-style-type: none"> Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO). Domeinspecifieke vragenlijsten voor diverse stelsels. Zelfevaluatie afronden en vastleggen in ENSIA. 	  	Vragenlijsten: <ul style="list-style-type: none"> RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). BKWI: Informatiebeveiliging Suwinet (BIO). Logius: Informatiebeveiliging DigiD. DGBRW: Datakwaliteit en -integriteit BAG, BGT en BRO.
Opstellen 	<ul style="list-style-type: none"> Genereren en opstellen verantwoordingsrapportages. Audit door gecertificeerde RE-auditor over collegeverklaring Suwinet en DigiD. Opstellen rapportage ENSIA t.b.v. de gemeenteraad. 	 	Producten: <ul style="list-style-type: none"> Collegeverklaring over Suwinet en DigiD. Rapportage BAG, BGT en BRO door college van B&W. Uittreksels BRP en Reisdocumenten. Rapportage ENSIA voor de gemeenteraad.
Verantwoorden 	<ul style="list-style-type: none"> Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W. Uploaden en aanleveren verantwoordingsrapportages via ENSIA (Uittreksels BRP en Reisdocumenten verwerken in de rapportages uit de Kwaliteitsmonitor en daar uploaden). 	 	Resultaten: <ul style="list-style-type: none"> BKWI en de toezichthouders Logius en DGBRW krijgen via ENSIA de verantwoordingsrapportages aangeleverd. RvIG krijgt de informatie uit de Uittreksels BRP en Reisdocumenten via de Kwaliteitsmonitor aangeleverd.
Versturen 	<ul style="list-style-type: none"> Opstellen paragraaf verantwoording informatiebeveiliging voor de paragraaf Bedrijfsvoering in het jaarverslag. Gemeenteraad neemt kennis van rapportage ENSIA. College van B&W stelt jaarverslag vast. Gemeenteraad keurt jaarverslag goed. Het college van B&W stuurt het gemeentelijk jaarverslag aan de provincie. 		<ul style="list-style-type: none"> De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd. De vastgestelde jaarstukken zijn aan de provincie toegestuurd.

Het ENSIA-jaar kent de volgende deadlines:



1 juli 2024	Het ENSIA-platform wordt opengesteld voor het uitvoeren van de zelfevaluatie. De vragenlijsten worden beschikbaar gesteld. Door het uitvoeren van de zelfevaluatie geeft de ENSIA-coördinator namens de gemeente aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen.
31 december 2024	De deadline voor de zelfevaluatie: dit is de laatste dag waarop de zelfevaluatie binnen het ENSIA-platform kan worden ingeleverd. Hierna kunnen de ingeleverde vragenlijsten niet meer worden aangepast. De ingevulde informatie is de basis voor het genereren van rapporten ten behoeve van de verantwoordingfase. De verantwoording wordt vastgesteld door het College van B&W.
30 april 2025	De deadline voor het inleveren van de verantwoordingen DigiD en Suwinet (inclusief de collegeverklaring met bijlagen, het Assurance rapport en eventuele TPM's) en de verantwoordingsrapportages BAG, BGT en BRO binnen ENSIA. Ook is dit de deadline voor het inleveren van de verantwoording BRP en Reisdocumenten via de Kwaliteitsmonitor ² . De ondertekende rapportages BRP en Reisdocumenten uit de Kwaliteitsmonitor en de resultaten over BRP en Reisdocumenten uit ENSIA worden gecombineerd aangeleverd aan de toezichthouder via de Kwaliteitsmonitor.
15 juli 2025	De deadline voor het toesturen van de goedgekeurde jaarstukken aan de provincie door het college van B&W.

² De Kwaliteitsmonitor is een separate verantwoordingsomgeving ten behoeve van de BRP en de Reisdocumenten die in de meeste gevallen wordt beheerd door de afdeling Burgerzaken.

Fases in het verantwoordingsjaar

<p>Zelfevaluatie</p> 	<p>De gemeente vult tijdens de zelfevaluatie vragenlijsten in met betrekking tot de volgende onderwerpen:</p> <ul style="list-style-type: none"> • Informatiebeveiliging binnen de gemeente volgens de BIO. Waar de normen van BRP en wet- en regelgeving reisdocumenten, en Suwinet aansluiten op de BIO-normen zijn in de BIO-vragenlijst eveneens vragen opgenomen voor deze onderwerpen. • DigiD • BAG, BGT en BRO • Waarstaatjegemeente. <p>Met de ingevulde zelfevaluatievragenlijst geeft het college van B&W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen.</p>
<p>Opstellen</p> 	<p>Het college van B&W stelt aan de hand van de zelfevaluatie een Collegeverklaring ENSIA op over een aantal vooraf geselecteerde beveiligingsnormen. Met deze verklaring geeft het college van B&W aan in hoeverre bij de gemeente de beheersmaatregelen hebben voldaan aan de voor de ENSIA-verantwoording geselecteerde normen en als aan de orde welke afwijkingen aan de orde zijn. Ook wordt melding gemaakt van eventuele verbetermaatregelen die de gemeente gaat treffen. Zie bijlage 3 voor de uitwerking van de Collegeverklaring ENSIA en de bijlagen bij de Collegeverklaring voor DigiD en Suwinet.</p> <p>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-auditors aangeboden via de website van NOREA. Als uit de controlewerkzaamheden van de IT-auditor blijkt dat de zelfevaluatie niet geheel correct was dan wordt dat in de Collegeverklaring en/of in het assurancerapport toegelicht’.</p> <p>Daarnaast worden met behulp van het ENSIA-platform verantwoordingsrapportages gegenereerd voor BAG, BGT en BRO, BRP en Reisdocumenten. Deze rapportages worden door het college van B&W geaccordeerd.</p> <p>Het college van B&W rapporteert vervolgens onder geheimhouding³ aan de gemeenteraad over de informatiebeveiliging, waarbij het College van B&W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt. Hierbij rapporteert het college dus niet alleen aan de hand van de verantwoording op basis van de BIO, maar ook over de andere onderdelen van ENSIA. Op deze manier krijgt het onderwerp meer aandacht bij de raadsbehandeling dan bij de behandeling ervan als onderdeel van de jaarstukken. In bijlage 4 is een handreiking opgenomen voor het opstellen van de oplegger voor een separate rapportage.</p>

³ De ENSIA-rapportage geeft inzicht in eventuele kwetsbaarheden. Rapporteren onder geheimhouding voorkomt dat deze informatie in handen komt van onbevoegden of kwaadwillenden.

<p>Verantwoorden</p> 	<p>De verantwoordingsdeadline en de toegepaste verantwoordingsprocedure voor BRP en Reisdocumenten wijken af van ENSIA. De samengestelde rapportages uit de Kwaliteitsmonitor en ENSIA dienen uiterlijk 30 april 2025 beschikbaar te worden gesteld via de Kwaliteitsmonitor. Voordien dienen ze bestuurlijk te zijn geaccordeerd.</p> <p>De Collegeverklaring ENSIA, het Assurancerapport en eventuele TPM's en de bestuurlijke rapportages met betrekking tot BAG, BGT en BRO dienen door het college behandeld te worden en uiterlijk 30 april beschikbaar te worden geüpload via het ENSIA-platform.</p> <p>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.</p>
<p>Versturen</p> 	<p>Het college van B&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.</p> <p>De verantwoordingsrapportages vormen de basis voor deze subparagraaf. In bijlage 4 is een handreiking opgenomen voor het opstellen van de oplegger voor een separate rapportage informatiebeveiliging voor de gemeenteraad, de daarin gehanteerde opzet is eveneens bruikbaar voor het opstellen van een rapportage over informatiebeveiliging als onderdeel van de paragraaf Bedrijfsvoering in het jaarverslag.</p> <p>De door de gemeenteraad vastgestelde jaarstukken moeten voor 15 juli 2025 worden toegestuurd aan de provincie.</p>

Wijze van verantwoorden voor niet-gemeenten

Naast gemeenten zijn ook niet-gemeenten verplicht om jaarlijks (voor BGT en BRO) uiterlijk 31 december de ENSIA-vragenlijst in te dienen via de ENSIA-tool en uiterlijk 30 april een verantwoordingsrapportage te uploaden middels hetzelfde kanaal. Het afleggen van verantwoording mag bij niet-gemeenten gemandateerd worden aan de betreffende vakafdeling. Het dagelijks bestuur van niet-gemeenten staat namelijk doorgaans verder af van de inhoud. De terugkoppeling vanuit BZK/DGBRW als toezichthouder vindt wel langs de bestuurlijke lijn plaats. De inhoudelijke ondersteuning van niet-gemeentelijke bronhouders voor ENSIA vindt plaats door BZK/DRBRW.

Informatieverstrekking aan het Rijk met behulp van het ENSIA-platform

Via het ENSIA-platform 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 GeVS (BKWI)⁴ 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.

Toezichthouders kunnen, indien nodig, nader onderzoek doen. Hiervoor zijn protocollen aanwezig bij de betrokken ministeries.

In 2025 verwerken volgende partijen namens de verantwoordelijke ministeries de verantwoordingsinformatie die via ENSIA wordt aangeleverd:

- Logius – DigiD.

⁴ GeVS staat voor 'Gezamenlijke elektronische Voorzieningen Suwi'. De aangeboden services zijn: Suwinet-inkijk, Suwinet-inlezen (BKWI) en DKD-inlezen (Inlichtingenbureau).

- Bureau Ketensamenwerking Werk en Inkomen (BKWI) – Suwinet.
- RvIG - BRP en Reisdocumenten.
- Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) - BAG, BGT en BRO.

In bijlage 5 is een overzicht gegeven welke informatie op welk moment aan deze partijen vanuit ENSIA beschikbaar wordt gesteld.

Nieuw in het verantwoordingsjaar 2024

ENSIA is voortdurend in ontwikkeling. In 2020 heeft BZK een evaluatie van de werking van ENSIA laten uitvoeren. De belangrijkste conclusie hiervan wordt vermeld in de kamerbrief van de staatssecretaris van BZK met betrekking tot de voortgang van de informatieveiligheid⁵: de implementatie van ENSIA heeft de bewustwording over het thema informatieveiligheid bij gemeenten vergroot, maar er is behoefte om het stelsel effectiever en efficiënter te kunnen toepassen. Een belangrijke stap in deze richting is de introductie van een nieuw verantwoordingsplatform dat in dit verantwoordingsjaar in gebruik wordt genomen.

De stelselverantwoordelijke heeft aangegeven dat in het vervolg met enige regelmaat zal 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). Daarnaast ontstaan verbetervoorstellen uit de dagelijkse praktijk van ENSIA en dienen zich nieuwe partijen aan die deelnemer willen worden van ENSIA.

Het Strategisch overleg toetst nieuwe ontwikkelingen aan de uitgangspunten voor doorontwikkeling die bij de start van het stelsel door de deelnemers zijn geformuleerd⁶. In de 'Notitie governance en financiering ENSIA' zijn de uitgangspunten voor de doorontwikkeling van ENSIA op de lange termijn vastgelegd.

In het verantwoordingsjaar 2024 worden de volgende inhoudelijke wijzigingen en vernieuwingen geïntroduceerd:

- a. Suwinet: geen inhoudelijke wijzigingen.
- b. DigiD: gemeenten worden door de auditor getoetst op werking van de normen U/TV.01, U/WA.02, C.07, C.08 en C.09. De werking moet over een periode van zes maanden worden aangetoond.
- c. BRP en Reisdocumenten: geen wijzigingen.
- d. BAG, BGT en BRO: beperkte aanpassing van de vragenlijsten.
- e. WaarStaatJeGemeente: geen wijzigingen.

⁵ Kamerbrief 'Voortgang informatieveiligheid bij de overheid', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 18 maart 2022.

⁶ De uitgangspunten voor doorontwikkeling zijn voor het eerst vastgelegd in het "Narratief ENSIA" (2018).

Bijlage 1 - De invulling van verantwoordelijkheden in samenwerkingsverbanden

Aanleiding voor het ontstaan van ENSIA

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 informatieveiligheid te stroomlijnen. In de toenmalige situatie hadden gemeenten te maken met minimaal vijf verantwoordingen op het vlak informatieveiligheid. 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 interne verantwoordingsproces rond informatieveiligheid 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 informatieveiligheid die door een IT-auditor wordt onderzocht. De departementen 'steunen' als het ware op de resultaten van dit verantwoordingsproces.

Kern van de verantwoording is de eigen verantwoordelijkheid van het gemeentebestuur voor de inrichting van deze informatieveiligheid. 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 informatieveiligheid

(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 constructie verantwoording moet/kan worden afgelegd. De wet gaat bij geen enkele beschreven samenwerking in op het thema informatieveiligheid 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.

Informatieveiligheid en intergemeentelijke samenwerking

In de handreiking Informatieveiligheid en intergemeentelijke samenwerking is het volgende opgenomen:

- *Een portefeuillehouder binnen het college van B&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. 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 t.o.v. 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 BIO (c.q. de beveiligingsafspraken). De verantwoording van de gemeente over het voldoen aan de BIO 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 BIO (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 BIO 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 BIO (of vergelijkbare baseline).

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 over 2024 spitst zich toe op een beperkt aantal normen.

De verantwoordelijkheid van gemeenten betreft uiteraard alle vormen van samenwerking met inbegrip van de IT-serviceproviders waarvan deze vormen van samenwerking zich bedienen. Voorstelbaar is dat de focus voor gemeenten allereerst ligt bij die samenwerkingsverbanden die binnen de scope van ENSIA vallen.

Bijlage 2 - Verantwoordingsnormen en richtlijnen 2024

In deze bijlage zijn de voor het verantwoordingsjaar 2024 gemaakte afspraken over de ENSIA-verantwoording nader beschreven. Deze afspraken zijn gemaakt in het Strategisch overleg van ENSIA. Het betreft afspraken over te selecteren scope, normen/vragen en over opzet en bestaan, rapportageperiode, rapportagemoment en de IT-audit.

Voor het verantwoordingsjaar 2024 zijn in de volgende documenten het verantwoordingskader/de van kracht zijnde normen geformuleerd voor de scope waarover verantwoording wordt afgelegd:

- BIO Versie 1.04;
- Suwinet Verantwoordingsrichtlijn GeVS 2022, versie 1.0
- DigiD Het DigiD normenkader 3.0
- 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

De Collegeverklaring ENSIA en de IT-audit hebben betrekking op opzet en bestaan van de beheersingsmaatregelen per 31 december 2024 voor de gearceerde normen (controls) en scope in de onderstaande tabellen

Het DigiD-normkader 3.0

De DigiD-norm heeft een andere scope dan de BIO. DigiD richt zich op de webomgeving van de DigiD-aansluiting met een geheel eigen set van normen. De gemeente moet een DigiD-audit laten uitvoeren per aansluiting. Soms is een deel van de DigiD-norm van toepassing op de gemeente en soms op een leverancier of op beiden. Om die reden zijn de DigiD-vragen losgekoppeld van de BIO-vragenlijst. Matching met BIO-normen is daarom niet van toepassing.

Nr.	Beschrijving van de beveiligingsrichtlijn
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.
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 privacy bevorderende en cryptografische technieken.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.

Nr.	Beschrijving van de beveiligingsrichtlijn
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.
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 assessments (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 3.0 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). Een door NOREA uitgewerkte guidance DigiD is uitgangspunt voor het uitvoeren van werkzaamheden door de gemeenten en de auditors.

Suwinet Verantwoordingsrichtlijn GeVS 2022

Voor de verantwoording over Suwinet bestaat de Suwinet Verantwoordingsrichtlijn GeVS 2022. SZW is stelselverantwoordelijke (stelselhouder) voor GeVS/Suwinet. Het vaststellen van de Verantwoordingsrichtlijn GeVS/Suwinet is belegd bij UWV, SVB en gemeenten. In overleg tussen SZW en UWV/SVB/gemeenten wordt vastgesteld welke normen voor ENSIA worden geselecteerd. Het corrigerend toezicht valt onder de verantwoordelijkheid van SZW.

De verantwoordingsrichtlijn Suwinet 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 BIO-vragenlijst verweven met de BIO-controls en maatregelen.

Versie BIO: 1.04

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 informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f) de bevordering van het beveiligingsbewustzijn.	1
5. Informatiebeveiligingsbeleid	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 informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, 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 verantwoordelijkheden 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 verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	1
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	1

Versie BIO: 1.04

Hoofdstuk	Nummer control	Toelichting control	Nummer maatregel	Toelichting maatregel	BBN
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
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
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.	7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	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 gebruikersidentificaties.	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 gebruikerstoegangsverleningsprocedure 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 gebruikerstoegangsverleningsprocedure 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

Versie BIO: 1.04

Hoofdstuk	Nummer control	Toelichting control	Nummer maatregel	Toelichting maatregel	BBN
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	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 beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	9.2.6.1	Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering van 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.	2
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
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	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

Versie BIO: 1.04

Hoofdstuk	Nummer control	Toelichting control	Nummer maatregel	Toelichting maatregel	BBN
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
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.	12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	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.	12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/ of SOC middels detectievoorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risicoinschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	1
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	1
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
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	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.	18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	2

Versie BIO: 1.04

Hoofdstuk	Nummer control	Toelichting control	Nummer maatregel	Toelichting maatregel	BBN
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 verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	2

Bijlage 3 - Format Collegeverklaring ENSIA en bijlagen DigiD en Suwinet

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente <organisatiernaam>



Collegeverklaring informatiebeveiliging DigiD en Suwinet 2024

Gemeente <organisatiennaam>

Doel en achtergrond verklaring

De voorzieningen die we als gemeente voor DigiD en Suwinet hebben, moeten beveiligd zijn tegen onrechtmatig gebruik. De gemeente treft (beheers)maatregelen om veilig gebruik te maken van deze voorzieningen.

Met deze verklaring geven wij, het College van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA⁷ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de door de toezichthouder geselecteerde eisen uit de Baseline Informatiebeveiliging Overheid voor Suwinet en het Normenkader 3.0 voor DigiD. De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor.

Deze verklaring is bestemd voor de toezichthouders van DigiD en Suwinet, te weten Logius en het Ministerie van Sociale Zaken en Werkgelegenheid via het Bureau Keteninformatie Werk en Inkomen (BKWI) alsmede de stelselhouders: het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toegang die we als gemeentelijke organisatie voor DigiD en Suwinet hebben, moet beveiligd zijn tegen onrechtmatig gebruik. Hiervoor stellen de stelselhouders een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet beheersmaatregelen treffen om te voldoen aan deze gestelde normen en gebruik te mogen (blijven) maken van deze voorzieningen.

De toetsing van de IT-auditor gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2024. Voor DigiD wordt het door Logius vastgestelde DigiD-normenkader 3.0 gehanteerd; voor Suwinet de Verantwoordingsrichtlijn GeVS 2022 (actuele versie) die ten behoeve van ENSIA nader is uitgewerkt in de ENSIA Suwinet-guidance.

De door de gemeente uitbestede beheersingsmaatregelen inzake DigiD en Suwinet zijn getoetst door een onafhankelijke IT-auditor van de externe dienstverlener. Hiervan hebben wij als gemeente een auditrapport ontvangen.

⁷ 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 Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Collegeverklaring en samenvattend beeld van de auditbevindingen

Verklaring / Conclusie

Het college van Burgemeester en Wethouders van de gemeente <naam> verklaart dat de gemeentelijke organisatie op 31 december 2024 [voldoet][niet voldoet] aan alle geselecteerde normen inzake DigiD en Suwinet.

Indien volledig wordt voldaan aan de normen:

[Het college verklaart dat bij gemeente <organisatiernaam> op 31 december 2024 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.]

Samenvattend beeld

Deze collegeverklaring en de verantwoording van de externe dienstverlener(s) dekken tezamen de beveiligingsnormen inzake DigiD en Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Bijlage 1 DigiD met kenmerk [nummer]
- Bijlage 2 Suwinet met kenmerk [nummer]

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD <tabel:digid.aansluitingen.aansluitnummer>	[Ja] [Nee]	[Ja] [Nee] [Niet van toepassing]
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]

College van B&W Gemeente <organisatiernaam>

[Plaats], [datum]

Auditor [naam]

[Plaats], [datum]

Dit document wordt door de auditor voorzien van een digitale handtekening. Verwijder deze tekst voordat het in het college wordt ingebracht.

Collegeverklaring informatiebeveiliging DigiD

Gemeente <organisatiennaam>



Collegeverklaring informatiebeveiliging DigiD 2024

Gemeente <naam>

Doel en achtergrond verklaring

De voorzieningen die we als gemeente voor DigiD hebben, moeten beveiligd zijn tegen onrechtmatig gebruik. De gemeente treft (beheers)maatregelen om veilig gebruik te maken van deze voorzieningen.

Met deze verklaring geven wij, het College van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA⁸ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de door de toezichthouder geselecteerde eisen uit de Baseline Informatiebeveiliging Overheid voor Suwinet en het Normenkader 3.0 voor DigiD. De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor.

Deze verklaring is bestemd voor de toezichthouder van DigiD, te weten Logius alsmede de stelselhouder: het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Reikwijdte en diepgang verklaring

De toegang die we als gemeentelijke organisatie voor DigiD hebben, moet beveiligd zijn tegen onrechtmatig gebruik. Hiervoor stelt de stelselhouder een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet beheersmaatregelen treffen om te voldoen aan deze gestelde normen en gebruik te mogen (blijven) maken van deze voorziening.

De toetsing van de IT-auditor gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD op 31 december 2024. Voor DigiD wordt het door Logius vastgestelde DigiD-normenkader 3.0 gehanteerd.

De door de gemeente uitbestede beheersingsmaatregelen inzake DigiD zijn getoetst door een onafhankelijke IT-auditor van de externe dienstverlener. Hiervan hebben wij als gemeente een auditrapport ontvangen.

Collegeverklaring en samenvattend beeld van de auditbevindingen

Verklaring / Conclusie

Het college van Burgemeester en Wethouders van de gemeente <naam> verklaart dat de gemeentelijke organisatie op 31 december 2024 [voldoet][niet voldoet] aan alle geselecteerde normen inzake DigiD.

Indien volledig wordt voldaan aan de normen:

[Het college verklaart dat bij gemeente <organisatienaam> op 31 december 2024 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD.]

⁸ 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 Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Gemeentelijk kenmerk collegeverklaring ENSIA over 2024	[zaaknummer]
--	--------------

Bij uitzonderingen:

[Het college verklaart dat voor DigiD 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.]

Samenvattend beeld

Deze collegeverklaring en de verantwoording van de externe dienstverlener(s) dekken tezamen de beveiligingsnormen inzake DigiD en Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Bijlage 1 DigiD met kenmerk [nummer]

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD <tabel:digid.aansluitingen.aansluitnummer>	[Ja] [Nee]	[Ja] [Nee] [Niet van toepassing]

College van B&W Gemeente <organisatienaam>

[Plaats], [datum]

Auditor [naam]

[Plaats], [datum]

Dit document wordt door de auditor voorzien van een digitale handtekening. Verwijder deze tekst voordat het in het college wordt ingebracht.

Collegeverklaring informatiebeveiliging Suwinet

Gemeente <organisatiennaam>



Collegeverklaring informatiebeveiliging Suwinet 2024

Gemeente <organisatiernaam>

Doel en achtergrond verklaring

De voorzieningen die we als gemeente voor Suwinet hebben, moeten beveiligd zijn tegen onrechtmatig gebruik. De gemeente treft (beheers)maatregelen om veilig gebruik te maken van deze voorzieningen.

Met deze verklaring geven wij, het College van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA⁹ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de door de toezichthouder geselecteerde eisen uit de Baseline Informatiebeveiliging Overheid voor Suwinet. De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor.

Deze verklaring is bestemd voor de toezichthouder van Suwinet, te weten het Ministerie van Sociale Zaken en Werkgelegenheid via het Bureau Keteninformatie Werk en Inkomen (BKWI) alsmede de stelselhouder: het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toegang die we als gemeentelijke organisatie voor Suwinet hebben, moet beveiligd zijn tegen onrechtmatig gebruik. Hiervoor stellen de stelselhouders een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet beheersmaatregelen treffen om te voldoen aan deze gestelde normen en gebruik te mogen (blijven) maken van deze voorzieningen.

De toetsing van de IT-auditor gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor Suwinet op 31 december 2024. Voor Suwinet wordt de Verantwoordingsrichtlijn GeVS 2022 (actuele versie) gehanteerd die ten behoeve van ENSIA nader is uitgewerkt in de ENSIA Suwinet-guidance.

De door de gemeente uitbestede beheersingsmaatregelen inzake Suwinet zijn getoetst door een onafhankelijke IT-auditor van de externe dienstverlener. Hiervan hebben wij als gemeente een auditrapport ontvangen.

Collegeverklaring en samenvattend beeld van de auditbevindingen

Verklaring / Conclusie

Het college van Burgemeester en Wethouders van de gemeente <naam> verklaart dat de gemeentelijke organisatie op 31 december 2024 [voldoet][niet voldoet] aan alle geselecteerde normen inzake Suwinet.

⁹ 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), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Gemeentelijk kenmerk collegeverklaring ENSIA over 2024	[zaaknummer]
--	--------------

Indien volledig wordt voldaan aan de normen:

[Het college verklaart dat bij gemeente <organisatiennaam> op 31 december 2024 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.]

Samenvattend beeld

Deze collegeverklaring en de verantwoording van de externe dienstverlener(s) dekken tezamen de beveiligingsnormen inzake Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Bijlage 2 Suwinet met kenmerk [nummer]

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]

College van B&W Gemeente <organisatiennaam>

[Plaats], [datum]

Auditor [naam]

[Plaats], [datum]

Dit document wordt door de auditor voorzien van een digitale handtekening. Verwijder deze tekst voordat het in het college wordt ingebracht.

Bijlage 1 DigiD - <digid.aansluitingen.aansluitingnaam> - <digid.aansluitingen.aansluitnummer>

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting <digid.aansluitingen.aansluitingnaam> met aansluitnummer <digid.aansluitingen.aansluitnummer>

<organisatiename> biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting <digid.aansluitingen.aansluitingnaam> voor authenticatie wordt gebruikt:

- Voeg hier (een opsomming) van de geboden functionaliteit toe bijvoorbeeld “Het genereren van aanvraagformulieren voor een uitkering bij de Snelbalie”.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Geef hier de naam van de applicatie op, bijvoorbeeld Snelbalie.

Deze applicatie betreft een [[maak een keuze uit [geheel maatwerk] [een combinatie van maatwerk en standaard software] [een geheel standaardpakket]] en wordt onderhouden door [naam gemeente en/of naam leverancier(s)].

Deze applicatie is extern benaderbaar via [de] [het] volgende internetadres(sen): [neem hier de extern benaderbare website(s) op].

DigiD aansluiting <Naam aansluiting> bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door [naam gemeente en/of naam leverancier[s]] in de vorm van [neem vorm op bijvoorbeeld, fysieke hosting, IAAS, PAAS, SAAS].

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting <naam aansluiting>. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de “Norm ICT-beveiligingsassessments DigiD” van Logius.

[[Alleen indien er een serviceorganisatie is, anders weglaten] <Naam gemeente> heeft een deel van de DigiD web-omgeving uitbesteed aan [naam leverancier[s]]. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier[s] van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM[’s] / assurance-rapportage[’s] van de leverancier[s]:

Leverancier 1	
Naam serviceorganisatie:	
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[Ja] [Nee]

Leverancier 2

Naam serviceorganisatie:	
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[Ja] [Nee]

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM[’s] / assurancerapportage[s] van onze serviceorganisatie[s] het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).]]

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk [kenmerk van het assurancerapport van onze auditor].

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm [[opnemen indien van toepassing [inclusief de normen die getoetst zijn bij leverancier[s]]].

DigiD-norm		Getoetst bij aanbesteding	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
B.05	Contractmanagement	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/TV.01	Identificatie en authenticatie	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA.02	Webapplicatiebeheerproces	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA.03	Automatische data-invoercontrole	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA.04	Normaliseren uitvoer	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA.05	Cryptografie/ Privacybevordering	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.02	Garanderen webprotocollen	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.03	Configureren webserver	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.05	Toegang tot beheermechanismen	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.07	Hardening van platformen	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing

DigiD-norm		Getoetst bij aansluitouder	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaaloordeel norm
U/NW.03	DMZ	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/NW.04	Protectie- en detectiemechanismen	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/NW.05	Scheiding beheer- en productieomgeving	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/NW.06	Hardening van netwerken	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.03	Vulnerability-assessments	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.04	Penetratietesten	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.06	Signaleringsfuncties	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.07	Monitoringfuncties	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.08	Wijzigingenbeheer	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.09	Patchmanagement	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing

De bovenstaande tabel is geautomatiseerd gevuld met de antwoorden uit de vragenlijst. Controleer iedere cel zorgvuldig. Verwijder deze instructietekst voordat u deze bijlage afdruckt.]

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2024 van <organisatie-naam>. Onderwerp van de verklaring is het gebruik van Suwinet. Deze verklaring heeft betrekking op de Verantwoordingsrichtlijn GeVS 2022 die is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO).

Suwinet-gegevens worden ten behoeve van de dienstverlening aan onze burgers [wel][niet] door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Alleen indien er een serviceorganisatie is, anders weglaten

[Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. <Organisatiename> heeft een deel van de [Suwinet taken] [en] [of] [niet-SUWI-taken] uitbesteed aan [naam serviceorganisatie(s)] [en] [of] [naam andere gemeente(n)]. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s] [en] [of] [[naam andere gemeente]]. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie(s) maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm.

De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie[s] valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling[en] (TPM[’s]) / assurancerapportage[s] (AR) van onze serviceorganisatie[s] [en] [of] [naam andere gemeente].

De volgende tabellen zijn optioneel en kunnen verwijderd worden indien niet van toepassing:

Leverancier 1	
Naam serviceorganisatie:	[Naam]
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[Ja] [Nee]

Leverancier 2	
Naam serviceorganisatie:	[Naam]
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[Ja] [Nee]

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]
Wet gemeentelijke schuldhulpverlening (Wgs)	[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	[Niet van toepassing] [Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	[Niet van toepassing] [Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]
Adresonderzoek door Burgerzaken	[Niet van toepassing] [Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee] [Ja] [Nee]

Naleving BIO-maatregelen

Indien geen afwijkingen van de maatregelen de volgende tekst opnemen:

[Zoals in de Collegeverklaring vermeld, voldoet <organisatiennaam> aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2024 in opzet en bestaan aan de geselecteerde controls.]]

Bij afwijkingen van de normen betreffende SUWI-taken de volgende tekst opnemen:

[Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2024 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2022:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Participatiewet (Pw)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]] [DKD-Inlezen met [naam inleesapplicatie]]
[[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]] [DKD-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]] [DKD-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Wet gemeentelijke schuldhulpverlening (Wgs)	[Maatregel]	[Wgs-Inkijk] [Wgs-Inlezen met [naam inleesapplicatie]]

]]

Bij afwijkingen van de normen betreffende niet-SUWI-taken de volgende tekst opnemen:

[Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de niet-SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

Organisatie	Niet-SUWI-taak	BIO-maatregel	Applicatie
[Niet van toepassing] [Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]]

Organisatie	Niet-SUWI-taak	BIO-maatregel	Applicatie
[Niet van toepassing] [Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]]
[Niet van toepassing] [Binnen de gemeente] [en] [of] [Naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [Andere gemeente]: [[naam andere gemeente]]	Adresonderzoek door Burgerzaken	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]]

]]

Bijlage 4 - Bouwstenen oplegnotitie separate rapportage Informatiebeveiliging aan gemeenteraad/publicatie in het jaarverslag van gemeenten

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&W zich aan de gemeenteraad over informatiebeveiliging in brede zin. Dit betreft onder meer gemeentelijke doelstellingen en afspraken over informatiebeveiliging. Daaronder zijn de afspraken die gemaakt zijn voor de ENSIA-verantwoording informatiebeveiliging aan het rijk. Over (het nakomen van) de ENSIA-afspraken doet de gemeente ook een specifieke uitspraak in de 'Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwlnet'. De IT-auditor doet een uitspraak over de juistheid en volledigheid van de Collegeverklaring ENSIA. Dit commitment is onlangs herbevestigd met de unanieme vaststelling van de nieuwe VNG-resolutie 'Digitale Veiligheid: een kerntaak van gemeenten' (februari 2021).

Het college van B&W rapporteert onder geheimhouding aan de gemeenteraad over de informatiebeveiliging, waarbij het College van B&W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt. Op deze manier krijgt het onderwerp meer aandacht bij de raadsbehandeling dan bij de behandeling ervan als onderdeel van de jaarstukken. Formats hiervoor zijn beschikbaar op de website van ENSIA (<https://www.vng.nl/projecten/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.



Bouwstenen oplegnotitie bestuurlijke verantwoording



Introductie

Inwoners en ondernemers verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Verwijs in de introductie naar het vastgestelde beleid, de missie en de visie van de organisatie op het terrein van informatiebeveiliging en -kwaliteit. Kijk of je deze kunt vertalen in risico's en kansen voor inwoners/ondernemers.



Focuspunten

Sommige gemeenten werken per jaar met specifieke aandachtsgebieden/ focuspunten die in dit verantwoordingsjaar de aandacht hadden. Benoem deze als dit het geval is.



Samenvatting resultaten

Bekijk of je de resultaten van dit jaar ten opzichte van het vorige jaar in één overzicht kunt weergeven. Zodat je in een oogopslag ziet op welke terreinen sprake is van een verbetering/verslechtering. Meld hier dat het college een verklaring heeft afgegeven op basis van een audit en wie deze heeft gecertificeerd.



Activiteiten in 2024

Beschrijf de belangrijkste inzet/activiteiten/beheersmaatregelen van afgelopen jaar en hoe die hebben bijgedragen aan de doelstellingen.



Resultaten in 2024

Beschrijf het gemeentebrede beeld uit de zelfevaluatie ENSIA. Beschrijf welke doelstellingen zijn gerealiseerd en welke nog aandacht nodig hebben. *Tip: Wees voorzichtig met details waar kwaadwillenden mogelijk misbruik van zouden kunnen maken. Deel in deze paragraaf ook de uitkomsten van de zelfevaluatie BIO (BRP, Reisdocumenten en Suwlnet), DigiD, BAG, BGT en BRO. Maak hierbij ook een duidelijke verwijzing naar de Collegeverklaring en het Assurancerapport. De bevindingen van de auditor op de specifieke onderdelen moeten herkenbaar terugkomen.*



Verbeterplan(nen)

Beschrijf de verbeterplannen (impact, eigenaar, doorlooptijd, budget/benodigde resources) en zorg voor de link met de bevindingen uit de zelfevaluatie ENSIA.

 **ENSIA**
Eén slimme verantwoording
voor informatiebeveiliging

 **VNG**
Realisatie

www.vng.nl/projecten/ensia

Bijlage 5 - Informatieverstrekking aan toezicht- en stelselhouders

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

Type	Organisatie	Type gegevens uit ENSIA-platform	Datum opleveren ruwe data*	Documenten uit ENSIA-platform	Datum opleveren documenten	Publicatie	Aan stelselhouder
BRP	RvIG	Ruwe data uit punten-rapport BIO zelfevaluatie	Na 15 januari 2025	Rapportage BRP*	1 jan - 1 mei 2025	Rapportage BRP door minister BZK.	BZK
Wet- en regelgeving reisdocumenten	RvIG	Ruwe data uit punten-rapport BIO zelfevaluatie	Na 15 januari 2025	Rapportage reisdocumenten*	1 jan - 1 mei 2025	Rapportage Reisdocumenten door minister BZK.	BZK
BAG	DGBRW	Ruwe data uit rapportage	Na 15 januari 2025	Bestuurlijke rapportage	1 jan - 1 mei 2025	Openbare publicatie van rapportages inclusief beoordelingsoverzicht.	BZK
BGT	DGBRW	Ruwe data uit rapportage	Na 15 januari 2025	Bestuurlijke rapportage	1 jan - 1 mei 2025	Openbare publicatie van rapportages inclusief beoordelingsoverzicht.	BZK
BRO	DGBRW	Ruwe data uit rapportage	Na 15 januari 2025	Bestuurlijke rapportage	1 jan - 1 mei 2025	Openbare publicatie van rapportages inclusief beoordelingsoverzicht.	BZK
Suwinet	BKWI	-	-	Collegeverklaring en bijlage Suwinet Assurancerapport	1 jan - 1 mei 2025	Totaaloverzicht beveiliging GeVS door minister SZW.	SZW
DigiD	Logius	-	-	Collegeverklaring en bijlage(n) DigiD en TPM's Assurancerapport	1 jan - 1 mei 2025	Niet van toepassing	BZK
WSJG	N.v.t.	Ruwe data uit vragenlijst	Na 15 januari 2025	-	-	Publicatie via www.wsjg.nl	-

* De in dit stadium verstrekte informatie kan – als gevolg van de uitgangspunten van ENSIA – uitsluitend worden gebruikt voor begeleidende activiteiten. Toetsing en handhaving vindt uitsluitend plaats op basis van de door het College van B&W goedgekeurde verantwoordingsrapportages (waaronder de Collegeverklaring) in combinatie met de Assurance rapporten en overige bewijslast.

** Resultaten uit ENSIA worden verwerkt in de rapportages uit de Kwaliteitsmonitor en geüpload via de Kwaliteitsmonitor.