Plan van aanpak 2025

**Format**

Juli 2025

Thema of datum

**VNG Realisatie**

Nassaulaan 12

2514 JS Den Haag

070 373 80 08

realisatie@vng.nl

Juli 2025

Inhoud

[Doel van het format Plan van Aanpak 4](#_Toc203658946)

[Toelichting op het gebruik van verschillende lettertypes 4](#_Toc203658947)

[Advies besluitvorming PvA 4](#_Toc203658948)

[1. Inleiding en achtergrond 5](#_Toc203658949)

[1.1. Waarom? 5](#_Toc203658950)

[1.2. Wat is ENSIA? 5](#_Toc203658951)

[1.3. Tijdpad ENSIA 5](#_Toc203658952)

[2. Nieuw in het verantwoordingsjaar 2025 6](#_Toc203658953)

[2.1. Overige aandachtspunten 6](#_Toc203658954)

[3. Definitie 7](#_Toc203658955)

[3.1. Doelstellingen 7](#_Toc203658956)

[3.2. Uitgangspunten 7](#_Toc203658957)

[3.3. Aanpak en methodiek 7](#_Toc203658958)

[3.4. Resultaat 8](#_Toc203658959)

[3.5. Wat doet de verantwoording met ENSIA niet? 8](#_Toc203658960)

[3.6. Relaties met andere projecten en activiteiten 8](#_Toc203658961)

[4. Activiteiten en planning 9](#_Toc203658962)

[4.1. Planning/fasering 9](#_Toc203658963)

[5. Organisatie 14](#_Toc203658964)

[5.1. Opdrachtgeversoverleg ENSIA 14](#_Toc203658965)

[5.2. Werkgroep ENSIA 14](#_Toc203658966)

[5.3. Overlegstructuur 16](#_Toc203658967)

[6. Stakeholders 17](#_Toc203658968)

[6.1. Interne stakeholders 17](#_Toc203658969)

[6.2. Samenwerkingsverbanden 17](#_Toc203658970)

[6.3. Externe stakeholders 18](#_Toc203658971)

[7. Begroting 19](#_Toc203658972)

[Bijlage - Rol- en taakbeschrijving interne stakeholders 20](#_Toc203658973)

[College van B&W 20](#_Toc203658974)

[Portefeuillehouder informatiebeveiliging 21](#_Toc203658975)

[Gemeenteraad 21](#_Toc203658976)

[Griffier 21](#_Toc203658977)

[Gemeentesecretaris 22](#_Toc203658978)

[ENSIA – coördinator 22](#_Toc203658979)

[CIO of informatiemanager 23](#_Toc203658980)

[CISO 23](#_Toc203658981)

[Controller 24](#_Toc203658982)

[Lijnmanagers 24](#_Toc203658983)

[Domeindeskundigen 25](#_Toc203658984)

## Doel van het format Plan van Aanpak

Dit format Plan van Aanpak (PvA) ENSIA 2025 is gemaakt om ENSIA-coördinatoren te ondersteunen bij het organiseren van de ENSIA-verantwoording. In het format is uitgegaan van de specifieke kenmerken van het verantwoordingsjaar 2026. Het format is naar eigen inzicht toe/aan te passen.

Dit plan van aanpak helpt u om de benodigde activiteiten te omschrijven om de ENSIA-verantwoording uit te voeren. Het plan heeft tot doel om uitvoering van ENSIA in goede banen te leiden en de rollen en taken te organiseren. In dit plan komen de volgende voor de uitvoering rele-vante onderwerpen aan bod:

* Activiteiten
* Planning
* Communicatie
* Organisatiestructuur
* Begroting.

In het format zijn basisteksten, suggesties en vragen opgenomen die helpen om de aanpak te formuleren die het beste bij uw organisatie past.

### Toelichting op het gebruik van verschillende lettertypes

In dit format zijn verschillende lettertypes gebruikt:

* Cursieve tekst betreft beschreven instructies die u helpen bij het opstellen van de teksten. Deze cursieve tekst dient u altijd te verwijderen.
* Standaard geschreven teksten zijn teksten die u kunt overnemen in uw eigen plan van aanpak. U kunt ze vrij aanpassen en desgewenst ook weghalen.
* [Geel gearceerd] zijn teksten waar de eigen gemeentenaam of naam van de medewerker kan worden ingevuld. De gele arcering haalt u na het invullen weg.

### Advies besluitvorming PvA

Het organiseren van de ENSIA-verantwoording raakt verschillende afdelingen van de gemeente en vraagt de inzet van mensen op operationeel, tactisch en strategisch niveau. Om draagvlak te cre-eren voor de aanpak, goedkeuring te krijgen voor inzet van mensen en eventueel middelen, wordt aangeraden om het plan van aanpak te laten accorderen door het managementteam (MT) van de gemeente.

De bovenstaande tekst is een instructie en kunt u na gebruik verwijderen. plek. Haal deze tekst weg en vervang het door je eigen tekst. De tussenkop is niet verplicht.

## Inleiding en achtergrond

### Waarom?

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.

Ga in deze paragraaf in op andere onderwerpen die rondom informatiebeveiliging spelen in uw gemeente. Geef ook de context weer en de raakvlakken met andere (reeds gerealiseerde) thema’s en projecten zoals de resultaten van de zelfevaluatie 2025 en de afspraken voor doorontwikkeling die gemaakt zijn.

### Wat is ENSIA?

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de Baseline Informatiebeveiliging Overheid (BIO) als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Gemeenten riepen in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. ENSIA is in 2017 ontstaan op initiatief van gemeenten en de ministeries van BZK en SZW. ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. De focus ligt hierbij op de interne verantwoording: binnen de gemeente, met een belangrijke rol voor de gemeenteraad. 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.

Met ENSIA sluit de verantwoording over informatieveiligheid en datakwaliteit/data-integriteit aan op de planning en controlcyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van de gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad. ENSIA structureert ook de verantwoording richting de rijksoverheid, over de Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

### Tijdpad ENSIA

Op 1 juli 2025 start de verantwoording met ENSIA. De zelfevaluatie moet vóór 31 december 2025 zijn ingeleverd. In het voorjaar van 2026 vindt verantwoording aan de gemeenteraad en de toezichthouders van het rijk plaats. Alle verbeteracties die worden ingezet worden op basis van de controls en maatregelen van de BIO genomen.

## Nieuw in het verantwoordingsjaar 2025

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 informatieveiligheid : 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.

In het verantwoordingsjaar 2025 zijn de volgende vernieuwingen geïntroduceerd:

* De auditor kan gaan toetsen op het gebruik van Suwinet voor de Regeling opvang ontheemde Oekraïners. Hierover hoeven geen vragen in de BIO-vragenlijst beantwoord te worden maar hierover moet wel via de collegeverklaring verantwoord worden.
* In de vragenlijsten van BAG, BGT en BRO zijn vragen en/of antwoordmogelijkheden gewijzigd.

### Overige aandachtspunten

1. De collegeverklaring over Suwinet en DigiD wordt vastgesteld door het college van B&W. De collegeverklaring is alleen bestemd voor het college en de toezichthouders voor Suwinet (BKWI) en DigiD (Logius). U moet echter wel de raad informeren over de status van informatiebeveiliging en de uitkomsten van de IT-audit (interne verantwoording over de BIO). Hier zijn (vormvrije) sjablonen beschikbaar.
2. Suwinet volgt de Verantwoordingsrichtlijn GeVS 2025 Deze is volledig op basis van de BIO opgesteld en in te zien via de site van BKWI <https://bkwi.nl/standaarden/privacy-beveiliging/verantwoordings-richtlijn-gevs-2025-v10>.
3. Voor Suwinet geldt de carve-out methodiek. Dit betekent dat de auditor van de collegeverklaring steunt op de ontvangen TPM's van dienstenleveranciers Suwinet. Om de antwoorden tijdig te kunnen verwerken, adviseren wij om uiterlijk 15 oktober de TPM’s van onze op-drachtnemers/dienstenleveranciers/samenwerkingsverbanden te laten aanleveren. Sturing op tijdige aanlevering van deze TPM’s is belangrijk.

## Definitie

### Doelstellingen

De gemeente [naam gemeente] beoogt met de implementatie van ENSIA:

* Het verantwoordingsproces in de gemeente te organiseren;
* Met een brede betrokkenheid, informatieveiligheidsbewustzijn en bijdrage van medewerkers;
* Met een integraal overzicht van waaruit een verbeterplan kan worden opgesteld en zelfregulering kan worden ingericht, zodat college en raad integraal kunnen sturen;
* Dat het college verantwoording over informatiebeveiliging en datakwaliteit en -integriteit aan de raad kan afleggen;
* Tijdig en accuraat de verantwoording over DigiD, Suwinet, BAG, BGT, BRO, BRP en Reisdocumenten op te leveren aan de toezichthouders van het Rijk.

### Uitgangspunten

De gemeente [naam gemeente] hanteert bij de verdere uitwerking van de aanpak de volgende uitgangspunten:

* Streven naar een inrichting voor een structurele situatie waarbij horizontale samenwerking binnen uw gemeente voorop staat;
* Continu verbeteren van informatieveiligheid door middel van jaarlijkse planning en sturing;
* Breed draagvlak en bewustzijn binnen de gemeente over informatieveiligheid;
* Beschikbaarheid van resources als het gaat om aanspreekpunten bij burgerzaken (BRP/Reisdocumenten/DigiD), sociaal domein (Suwinet), geografische informatie (BAG/BGT/BRO), ICT (technische componenten), facilitaire zaken (fysieke beveiliging), HRM (personele beveiliging), inkoop, juridische zaken etc.;
* Referentie aan maximaal benodigd/gewenst/beschikbaar budget;
* Gebruikmakend van verbeterplannen ENSIA 2024 n.a.v. uitgevoerde zelfevaluatie;
* Interne communicatie via bestaande kanalen.
* …..

### Aanpak en methodiek

*Hoe wilt u de organisatie van de verantwoording aanpakken? Wat zijn de ervaringen met het verantwoordingsjaar 2025 (intern en extern).*

De gemeente [naam gemeente] heeft de volgende elementen in haar aanpak meegenomen:

* Coördinatie van het project ligt bij …
* Breed samengestelde werkgroep bestaat uit …
* Er wordt samengewerkt met de intergemeentelijke sociale dienst, shared services center, belastingsamenwerkingsverband, etc.
* De wijze van beantwoording van de zelfevaluatie in ENSIA (gezamenlijk/uitzetten van vra-gen bij domeinen).
* Proces om te komen tot een definitief antwoord.
* Aandacht voor informatievoorziening aan alle medewerkers.

### Resultaat

*Welke resultaten wilt u in uw gemeente bereiken met de zelfevaluatie en verantwoording met EN-SIA? In onderstaande opsomming zijn de minimale resultaten opgenomen, zoals die door gemeenten en de rijksoverheid zijn afgesproken. U kunt hier naar eigen inzicht extra resultaten aan toevoegen, die van belang zijn voor uw gemeente.*

Met het uitvoeren van de zelfevaluatie en het afleggen van verantwoording met ENSIA beoogt de gemeente een aantal effecten te realiseren:

Voor de verantwoording aan de raad gaat het om:

* Een goed functionerende werkgroep t.b.v. de uitvoering van het ENSIA-verantwoordingsproces;
* In het jaarverslag is verslag gedaan over de status van informatieveiligheid;
* In de raadsvergaderingen wordt het onderwerp informatieveiligheid besproken;
* Er worden verbeteracties geformuleerd en belegd;
* Borging van het interne verantwoordingsproces t.a.v. informatieveiligheid.

Voor de verantwoording aan de toezichthouders van het rijk gaat het om:

* De auditor heeft ‘assurance’ gegeven over de collegeverklaring over Suwinet en DigiD;
* Burgemeester en gemeentesecretaris hebben de uittreksels BRP en Reisdocumenten (relatie met kwaliteitsmonitor Burgerzaken) vastgesteld;
* Het college heeft de rapportages uit ENSIA m.b.t de BAG, BGT en BRO vastgesteld;
* De relevante informatie voor de verantwoording aan het rijk wordt in de ENSIA-tool tijdig ingeleverd (voor 1 mei 2026).

### Wat doet de verantwoording met ENSIA niet?

*Vul hier in welke aspecten die ook met verantwoording te maken hebben, maar die niet in dit project(plan) worden meegenomen omdat ze niet vallen onder de scope van ENSIA. Denk hierbij bijvoorbeeld aan:*

* *Mogelijke andere lokale projecten die met verantwoording te maken hebben;*
* *Kwaliteitsmonitor BRP en Reisdocumenten: Evenals de voorgaande jaren worden de vragen over informatiebeveiliging over de BRP en de Reisdocumenten binnen ENSIA gesteld. De antwoorden op de ENSIA-vragen voor BRP en Reisdocumenten moeten uiterlijk 31 december 2025 in het ENSIA-platform worden ingeleverd.*

### Relaties met andere projecten en activiteiten

Geef in deze paragraaf aan welke andere projecten er lopen die een raakvlak hebben met de uitvoering van de ENSIA-verantwoording.

* Met welke projecten moet afstemming of samenwerking worden gezocht? Denk hierbij bijvoorbeeld aan samenwerkingsverbanden, lokale ontwikkelingen of projecten zoals:
	+ Ontwikkelingen m.b.t. de uitvoering van verbeteringen die zijn opgesteld vanuit de zelfevaluatie 2024;
	+ Implementatie en/of gebruik van een ISMS;
	+ Agenda digitale veiligheid 2020-2024;
	+ Herijking afspraken met samenwerkingspartners, zoals gemeenschappelijke regelingen of serviceorganisaties en de onderliggende IT-leveranciers (SLA’s).

## Activiteiten en planning

Dit hoofdstuk gaat in op de activiteiten die in het project moeten worden uitgevoerd: de fasering van het project, de activiteiten, de randvoorwaarden en de externe afhankelijkheden. De hoofdlijnen van de planning zien er als volgt uit.





### Planning/fasering

Het project bestaat uit de volgende fasen:

|  |  |  |
| --- | --- | --- |
| Fase | Start | Einde |
| Voorbereiding | 1 juni 2025 | 30 juni 2025 |
| Zelfevaluatie | 1 juli 2025 | 31 december 2025 |
| Verantwoorden (intern en toezichthouders) | 1 januari 2026 | 30 april 2026 |
| Evaluatie | 1 mei 2026 | 1 juni 2026 |

**Activiteiten voorbereiding**

|  |  |
| --- | --- |
| Voorbereiding 1 juni – 1 juli 2025 | Wie |
| Benoeming ENSIA-coördinator | Gemeentesecretaris |
| Bestudering achtergrondinformatie* Scope 2025
 | ENSIA-coördinator |
| Opstellen plan van aanpak  | ENSIA-coördinator |
| Uitvoeren korte risicoanalyse t.a.v. succes ENSIA |  |
| Inventariseren en informeren intern en extern betrokkenenToewijzen taken bevoegdheden en verantwoordelijkheden* Verantwoordelijken domeinen (BRP/Reisdocumenten, BAG/BGT/BRO, SUWI, DigiD)
* Verantwoordelijken op afdelingen (IT, HRM, Facilitair, Inkoop, Juridisch)
* Betrokkenen vanuit samenwerkingsverbanden
	+ SSC IT
	+ Regionale Sociale Dienst
	+ Regionale Belastingsamenwerking
* ENSIA-collega’s in de regio
* Auditor
* Leveranciers
* Portefeuillehouder(s)
* FG
* Controller
* Raad
* Communicatie
 | ENSIA-coördinator |
| Afstemming interne communicatie |  |
| Kick-off verantwoording ENSIA 2025* Scope 2025
	+ Scope
	+ Wijzigingen 2025 in ENSIA
* Planning en aanpak
* Hoe werken we samen
	+ Betrokkenen (rollen en taken)
	+ Werkafspraken
* Toelichting op gebruik ENSIA
	+ Rollen en autorisaties
	+ Antwoorden
* Samenwerkingsverbanden & leveranciers
	+ TPM’s
 | ENSIA-coördinator |

Resultaat voorbereiding:

1. De gemeente is klaar om op 1 juli 2025 te starten met het invullen van de zelfevaluatie.

**Activiteiten uitvoering zelfevaluatie**

| Uitvoering zelfevaluatie 1 juli – 31 december 2025 | Wie |
| --- | --- |
| Opdracht auditor collegeverklaring 2025* Bepaal scope afhankelijk van inzet TPM’s SUWI
 | ? |
| Aanvraag TPM’s samenwerkingsverband(en) Suwinet* Oplevering uiterlijk 15 oktober 2025
 | ? |
| Aanvraag TPM(‘s) DigiD leverancier(s) * Oplevering uiterlijk 15 oktober 2025
 | ? |
| Opdracht (laten) geven voor uitvoeren PEN-test | ? |
| Autoriseren betrokkenen ENSIA | ENSIA-coördinator |
| Uitzetten van vragenlijsten bij betrokkenen | ENSIA-coördinator |
| Afstemming (terugkerend)  | ENSIA-coördinator |
| Presentatie aan de raad (in afstemming met portefeuillehouder) | ? |
| Bewaken voortgang (continue)* Aanlevering TPM’s van leveranciers
* TPM van samenwerkingsverbanden SUWI
* Domeinspecifieke zelfevaluaties
* Invullen ENSIA-zelfevaluatie 2025 (BIO)
 | ENSIA-coördinator |
| Inventariseren van in te zetten verbeteracties voor 31-12-2025 | ENSIA-coördinator |
| Akkoord op definitieve antwoorden | ENSIA-coördinator |
| Inleveren vragenlijsten voor 31 december 2025* ENSIA-zelfevaluatie (BIO)
* DigiD
* BAG
* BGT
* BRO
* Waar staat je gemeente
 | ENSIA-coördinator |
| Informeren stakeholders over afronding zelfevaluatie en start van verantwoordingsproces | ENSIA-coördinator |

Resultaat zelfevaluatie:

1. Directe maatregelen zijn ingezet als de resultaten uit de zelfevaluatie hier aanleiding voor geven.
2. De gemeente heeft alle vragenlijsten ingevuld en ingeleverd voor 31 december 2025.

**Activiteiten verantwoording (intern en externe toezichthouders)**

| Afronding interne verantwoording 1 januari – 15 juli 2026 | Wie |
| --- | --- |
| Analyse uitkomsten zelfevaluatie | ENSIA-coördinator + ? |
| Opstellen rapportage informatiebeveiliging (BIO)  | ENSIA-coördinator + ? |
| Aanvullen uittreksels BRP en Reisdocumenten | ENSIA-coördinator + ? |
| Opstellen verbeterplan (ten minimale voor Suwinet en DigiD) | ENSIA-coördinator + ? |
| Opstellen concept Collegeverklaring DigiD en Suwinet | ENSIA-coördinator |
| Plannen audit Collegeverklaring DigiD en Suwinet | ENSIA-coördinator |
| Voorbespreking uitkomsten audit met portefeuillehouder/opdrachtgever | ENSIA-coördinator |
| Voorbereiden audit Collegeverklaring DigiD en Suwinet | ENSIA-coördinator |
| Uitvoeren en faciliteren audit Collegeverklaring SUWI en DigiD | ENSIA-coördinator + ? |
| Aanlevering Assurancerapport | Auditor |
| Afstemming concern control over tekst in jaarverslag gemeente over informatiebeveiliging (binnen de paragraaf bedrijfsvoering) | Concern controlENSIA-coördinator |
| Inplannen behandeling College B&W* Interne verantwoording informatiebeveiliging (BIO)
* Collegeverklaring DigiD en Suwinet
* Vaststelling rapportages BAG, BGT & BRO
 | ENSIA-coördinator + bestuurssecretariaat |
| Behandeling College B&W* Vaststelling interne verantwoording informatiebeveiliging (BIO)
* Ondertekening collegeverklaring Suwinet en DigiD
* Vaststelling rapportages BAG, BGT & BRO
 | Collegeverklaring door GS en College van B&W |
| Afronding auditproces* Waarmerken individuele documenten
* Opnemen in PDF/A
 | Auditor |
| Uploaden documenten verticale verantwoording in ENSIA uiterlijk 30 april 2026 | ENSIA-coördinator |
| Informeren van de raad via separate rapportage over status informatiebeveiliging (niet openbaar)* Beleid, doelstellingen & ambities
* Samenvatting gemeente brede beeld en resultaten zelfevaluatie ENSIA 2025
* Belangrijkste maatregelen
* Realisatie van doelstellingen/verbeteringen
* Incidenten
* Meerjarenperspectief
 | College van B&W (opstellen door ENSIA-coördinator en/of CISO)  |

Resultaat verantwoording:

1. Het college van B&W heeft de rapportages vastgesteld.
2. De gemeente heeft de verantwoording aan de toezichthouders van het rijk op basis van de vastgestelde rapportages afgerond.
3. De raad is geïnformeerd op hoofdlijnen via het openbaar jaarverslag van de gemeente.
4. De raad is via een separate (niet-openbare) rapportage geïnformeerd over de status van informatieveiligheid.

**Activiteiten evaluatie**

| Evaluatie 1 mei – 1 juni 2026 | Wie |
| --- | --- |
| Gezamenlijke evaluatie aanpak | Werkgroep ENSIA |
| Borgen van resultaten evaluatie (lessons learned) t.b.v. verantwoording op basis van de BIO | ENSIA-coördinator |

Resultaat:

1. De gemeente heeft inzicht in het functioneren van haar aanpak. Ook is bekend wat de volgende verantwoordingscyclus anders/beter kan worden gedaan.

## Organisatie

De organisatie en is als geheel verantwoordelijk voor de informatiebeveiliging en datakwaliteit/-integriteit. Omdat het ENSIA-verantwoordingsjaar vaste deadlines heeft, is het verstandig om de activiteiten projectmatig op te pakken. Hieronder staat omschreven hoe de organisatie rond ENSIA eruitziet.

### Opdrachtgeversoverleg ENSIA

*Met het opdrachtgeversoverleg kan de coördinator verbinding houden met de opdrachtgever(s). Zorg dat helder is wie binnen de gemeente de ambtelijk en bestuurlijk opdrachtgever voor de EN-SIA-verantwoording is. Leg ook vast hoe vaak overleg met de opdrachtgevers wordt gevoerd (zie overlegstructuur). Zorg als coördinator voor achtervang en leg dit met de opdrachtgevers vast.*

*Het opdrachtgeversoverleg hoeft geen separaat overleg te zijn, het kan onderdeel zijn van een bestaand overleg.*

|  |  |  |
| --- | --- | --- |
| Rol | Naam | Taken/verantwoordelijkheden |
| Opdrachtgever  | Portefeuillehouder [Naam portefeuillehouder] | * Bestuurlijk eindverantwoordelijk voor het project
* Zorgt voor eventuele financiële middelen voor de uitvoering van het project
* Bewaakt de voortgang van het project op strategisch niveau
 |
| Gedelegeerd opdrachtgever  | Gemeentesecretaris, Afdelingshoofd, lid MT?  | * Is ambtelijk verantwoordelijk voor de uitvoering van ENSIA
* Stuurt coördinator aan
 |
| Opdrachtnemer, coördinator/vervangend coördinator | [Naam coördinator][Naam achtervang]  | * Zorgt voor de dagelijkse uitvoering van het project.
 |

### Werkgroep ENSIA

*In de tabel is een overzicht opgenomen van de verschillende deskundigheden die betrokken zijn bij de zelfevaluatie. In de tweede kolom kan de naam van de medewerkers die deelnemen aan de werkgroep worden ingevuld.*

*Om de zelfevaluatie te kunnen uitvoeren is de inzet gewenst van de volgende rollen c.q. personen. Afhankelijk van de gemeentegrootte is het mogelijk dat één persoon meerdere rollen vervult.*

|  |  |  |
| --- | --- | --- |
| Rol | Naam | Taken/verantwoordelijkheden |
| Coördinator  | […] | * Is primair verantwoordelijk voor het project
* Rapporteert aan de portefeuillehouder
* Overlegt regelmatig met opdrachtgever
* Is het aanspreekpunt voor vragen
 |
| Projectondersteuner (*afhankelijk van gemeentegrootte)* | […] | * Zorgt voor de projectondersteuning
* Zorgt voor de interne coördinatie, planning, voortgangsbewaking en rapportage
 |
| CISO / adviseur informatieveiligheid  | […] | * Betrokkenheid vanuit informatieveiligheid
* Zie profiel CISO op <https://www.informatiebeveiligingsdienst.nl/product/handreiking-functieprofielen-informatiebeveiliging/>
 |
| Functionaris Gegevensbescherming (FG) | […] | * Betrokkenheid vanuit privacy
* Zie <https://www.informatiebeveiligingsdienst.nl/product/handreiking-positionering-en-taken-van-de-fg/>
 |
| Domeindeskundige BRP | […] | * Bijdrage aan beantwoorden van vragen
* Agenderen van ENSIA in werkoverleg van eigen afdeling
* Afstemmen met contactpersoon zelfevaluatie BRP en Reisdocumenten (deze persoon is aanspreekpunt voor RvIG voor het invullen van de Kwaliteitsmonitor BRP en Reisdocumenten)
 |
| Domeindeskundige Reisdocumenten | […] | * Afstemmen met contactpersoon zelfevaluatie BRP en Reisdocumenten (deze persoon is aanspreekpunt voor RvIG voor het invullen van de Kwaliteitsmonitor BRP/Reisdocumenten)
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Domeindeskundige(n) Suwinet | […] | * Mede invullen van bijlage 2 Suwinet binnen de gemeente
* Agenderen van ENSIA in werkoverleg(en)
 |
| Domeindeskundige DigiD | […] | * Bijdrage aan invullen DigiD-vragenlijst
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Domeindeskundige BAG |  | * Bijdrage aan invullen BAG-vragenlijst
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Domeindeskundige BGT |  | * Bijdrage aan invullen BGT-vragenlijst
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Domeindeskundige BRO |  | * Bijdrage aan invullen BRO-vragenlijst
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Medewerker HR/Financiën/Middelen/Control/Inkoop | […] | * Mede invullen vragen gerelateerd aan de eigen domeinen
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Functionaris Gegevensbescherming (FG) | […] | * Mede invullen vragen gerelateerd aan privacy
* Agenderen van ENSIA in werkoverleg van eigen afdeling
 |
| Communicatiemedewerker | […] | * Aanpassen intranetberichten
* Plaatsen intranetberichten
* Redigeren eindrapportages
 |
| Aanspreekpunt Samenwerkingsverband IT/SSC/GR | […] | * Bijdrage aan invullen IT-vragen BIO-vragenlijst
 |
| Aanspreekpunt Belastingsamenwerking  | […] | * Bijdrage aan invullen bijlage 2 Suwinet m.b.t. gebruik Suwinet voor Gemeenten Gerechtsdeurwaarders
 |
| Aanspreekpunt ISD | […] | * Bijdrage aan invullen bijlage 2 Suwinet m.b.t. gebruik Sociale Dienst (uitvoering P-wet/IOAZ/IOAW)
* Coördinatie uitvoering SUWI-audit (afgestemd met deelnemende gemeenten in de samenwerking)
 |

*In deze paragraaf kunt u ook nog aangeven hoe de werkgroep zich verhoudt tot andere overleggen die mogelijk binnen de gemeenten raakvlakken hebben met informatieveiligheid en/of verantwoording.*

### Overlegstructuur

*Bedenk met wie het van belang is om gedurende het project te overleggen, met welke frequentie en met welk doel. De hieronder genoemde overleggen zijn minimaal van belang.*

*Onderstaande tabel kunt u gebruiken om de situatie in uw eigen gemeente verder uit te werken.*

|  |  |  |  |
| --- | --- | --- | --- |
| Overleg | Deelnemer | Frequentie | Doel |
| Opdrachtgever – opdrachtnemer overleg | * Opdrachtgever
* Gedelegeerd opdrachtgever
* Opdrachtnemer/ coördinator
 | Eens per twee à drie maanden | * Informeren opdrachtgever over voortgang
 |
| Werkgroepoverleg | * Coördinator
* Leden werkgroep
 | Maandelijks  | * Afstemmen over verschillen tussen domeinen
* Afstemmen over het invullen vragenlijst
* Bespreken voortgang
* Inventariseren van benodigde verbeteracties
 |
| Regionaal overleg | * Coördinatoren
* Auditor (op aanvraag)
* Verantwoordelijken bij samenwerkingsverbanden
 | Maandelijks | * Afstemmen over opdrachtgeverschap naar samenwerkingsverbanden
* Afstemmen over scope (welke vragen ENSIA) en auditwerkzaamheden (TPM’s) samenwerkingsverbanden
* Afstemmen over aanleveren antwoorden vragenlijst
 |

## Stakeholders

### Interne stakeholders

*Wie zijn de stakeholders die u in het project wilt betrekken en die geen onderdeel uitmaken van de werkgroep? Denk hierbij bijvoorbeeld aan:*

* *College van B&W;*
* *Afdelingshoofden sociale zaken, burgerzaken, publiekszaken, financiën, HR;*
* *Collega’s van andere afdelingen;*
* *Raadsleden.*

*Bedenk voor elk van deze interne stakeholders waarvoor u hen zou willen betrekken en hoe u dat doet. In de bijlage geven we een overzicht van gangbare taken, bevoegdheden en verantwoordelijkheden van stakeholders. Het kan praktisch zijn om deze bijlage aan het aan uw situatie aangepaste plan van aanpak toe te voegen. U kunt de bijlage aanpassen aan uw specifieke situatie.*

|  |  |  |
| --- | --- | --- |
| Stakeholder | Naam | Doel |
| College van B&W | [Naam] | * Vaststellen paragraaf informatieveiligheid
* Vaststellen collegeverklaring
* Vaststellen rapportage BAG, BGT en BRO
 |
| Burgemeester | [Naam] | * Ondertekenen collegeverklaring
 |
| Portefeuillehouder | [Naam] | * Uitnodigen voor kick-off
 |
| Gemeentesecretaris | [Naam] | * Borging benodigde capaciteit voor uitvoering taken
* Informeren resultaten zelfevaluatie
 |
| Directeur Bedrijfsvoering | [Naam] | * Informeren resultaten zelfevaluatie
 |
| Concern control | [Naam] | * Input jaarrekening over informatieveiligheid
 |
| Lijnmanagement: Manager burgerzaken | [Naam] | * Verbeteracties binnen burgerzaken berspreken
* Agenderen van ENSIA in werkoverleg
 |
| .. | [Naam] | * …
 |

### Samenwerkingsverbanden

*Denk bij het uitwerken van de organisatiestructuur ook aan samenwerkingsverbanden. De gemeente is verantwoordelijk voor de informatieveiligheid, ook als werk is uitbesteed aan samenwerkingsverbanden. De gemeente blijft verantwoording over informatieveiligheid afleggen aan gemeenteraad over informatiebeveiliging (BIO) en aan de toezichthouders van het Rijk. Het is dus van belang dat u contact onderhoudt met het samenwerkingsverband.*

*Onderwerpen waarover met het samenwerkingsverband mogelijk afspraken kunnen worden gemaakt:*

* *Gezamenlijke projectorganisatie;*
* *Het delen van de vragenlijst die voor meerdere gemeenten identiek wordt ingevuld;*
* *Gezamenlijke inkoop van de auditor, als de samenwerking gaat over Suwinet;*
* *Is verantwoording over informatieveiligheid in gezamenlijke afspraken opgenomen?*

### Externe stakeholders

*Er zijn ook partijen buiten de gemeente nodig om van de implementatie van ENSIA een succes te maken. Denk hierbij aan:*

* *De auditor;*
* *De uitvoerder van de pentest;*
* *Softwareleveranciers t.b.v. TPM.*

*Bedenk voor elke stakeholder waarvoor u deze wilt betrekken, op welke wijze en welke deadlines er zijn.*

|  |  |  |  |
| --- | --- | --- | --- |
| Stakeholder | Naam | Doel | Wijze van contact |
| Softwareleverancier(s) | [Naam bedrijf] | * TPM t.bv……
 | * Via opdrachtverlening
* Opdrachtverlening (zomer 2025)
* Gewenste opleverdatum – uiterlijk 15 oktober (geen vaste datum, maar wel een datum die ruimte biedt voor het afwikkelen van de besluitvorming)
 |
| Onafhankelijke pentester | [Naam bedrijf] | * Uitvoeren pentest
 | * Via opdrachtverlening
 |
| Auditor | [Bedrijf en naam contactpersoon] | * Uitvoeren audit
 | * Opdrachtverlening – uiterlijk oktober 2025
* Zie format opdracht auditor
 |
| … |  |  |  |

## Begroting

*Voor de verantwoording ENSIA 2024 is mogelijk budget benodigd geweest. Op basis van deze ervaringen kunt u de begroting opstellen voor 2025. Bij de opstelling van de begroting kunt u denken aan kosten voor:*

* *Inhuur uitvoering pentest;*
* *Inhuur auditor;*
* *Inhuur van vervangers van mensen die activiteiten voor het project ENSIA doen;*
* *Bij een samenwerkingsverband zijn er wellicht kosten verbonden aan het betrekken van een medewerker van het samenwerkingsverband;*
* *Kosten voor de uitvoering van verbeterplannen;*
* *Kosten die gemaakt worden voor overleg, zoals een vergaderlocatie.*

## Bijlage - Rol- en taakbeschrijving interne stakeholders

Deze bijlage bevat een kort overzicht van alle relevante gemeentelijke stakeholders. Daarbij is aangegeven wat er van hen verwacht wordt voor een succesvolle uitvoering van het ENSIA-verantwoordingsproces.

### College van B&W

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Vaststellen/benoemen coördinator.
* Laten uitvoeren van zelfevaluatie informatiebeveiliging en zelfevaluatie DigiD, BAG, BGT en BRO, BRP en Reisdocumenten.
* Maken van afspraken binnen de samenwerkingsverbanden over de omgang met informatiebeveiliging en ENSIA.
* Het geven van opdracht aan RE-Auditor om Assurance te geven over de juistheid en volledigheid van de collegeverklaring.
* Afgeven collegeverklaring informatiebeveiliging (DigiD en Suwinet) en hiermee aangeven in hoeverre de beheermaatregelen aan de beveiligingsnormen voldoen.
* Hierbij ook aangeven - mits aan de orde - welke onderdelen daarvan zijn uitgezonderd.
* Opstellen paragraaf informatieveiligheid t.b.v. interne verantwoording in de jaarrekening.
* Vaststellen van maatregelen voor het verbeteren van informatieveiligheid.
* Het afleggen van verantwoording aan de raad over informatieveiligheid.
 | * Adequate en tijdige rapportage aan de gemeenteraad over informatiebeveiliging en datakwaliteit/-integriteit in een separate rapportage.
* Bij samenwerkingsverbanden als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie.
* Adequate en tijdige rapportage aan de gemeenteraad over informatiebeveiliging en datakwaliteit/-integriteit in de paragraaf bedrijfsvoering van de jaarrekening.
* Eindverantwoordelijk voor interne verantwoording met betrekking tot informatiebeveiliging.
 | * Benoemen van de coördinator.
* Keuze van verbetermaatregelen en de prioritering hiervan.
* De gemeenteraad informeren over informatieveiligheid en voortgang over ENSIA.
 |

### Portefeuillehouder informatiebeveiliging

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Opdracht geven aan gemeentesecretaris voor aanwijzen van coördinator.
* Gemeenteraad systematisch informeren over de ENSIA- voortgang en hun rol daarin. College van B&W systematisch informeren over de voortgang van ENSIA.
* Namens het college van B&W rol vervullen van bestuurlijk opdrachtgever voor de uitvoering van ENSIA.
 | * Binnen het college van B&W verantwoordelijk voor de (prioritering van) beveiliging van informatie binnen de bedrijfs(werk)processen.
* Als bestuurlijk opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie.
* Verantwoordelijk voor het maken van afspraken met samenwerkingsverband(en) over informatiebeveiliging.
 | * Bepalen inhoud en frequentie van de voorlichtings-informatie richting de gemeenteraad.
 |

### Gemeenteraad

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Stellen van vragen over informatieveiligheid (BIO en ENSIA).
* Beoordelen paragraaf informatieveiligheid en collegeverklaring.
* Beoordelen van voorgenomen maatregelen voor het verbeteren van informatieveiligheid.
 | * Het college van B&W controleren op de invoering
* Opstellen paragraaf Bedrijfsvoering, incl. paragraaf informatieveiligheid, voor het jaarverslag. Aangevuld met separate rapportage informatieveiligheid.
 | * Stellen van vragen over implementatie BIO en uitvoering ENSIA.
* Onderzoek instellen naar stand van zaken informatieveiligheid.
* Bepalen van beleidskeuzes.
 |

### Griffier

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Regelmatig agenderen van voortgang implementatie BIO en verantwoording ENSIA bij de gemeenteraad.
* Als onderdeel van jaarverslag: opstellen annotatie bij jaarverslag - aandacht voor informatieveiligheid.
* Als er sprake is van een separate verantwoording: uitgebreide annotatie over ENSIA-verantwoording.
* Agenderen jaarverslag dan wel stukken verantwoording informatiebeveiliging ter informatie:
	+ Paragraaf informatieveiligheid
	+ Collegeverklaring
	+ Assurance rapport
 | * Tijdige agendering. Ontvangen, verzamelen en distribueren van Collegeverklaring, paragraaf Informatieveiligheid en separate Rapportage informatiebeveiliging.
 | * Verslaglegging, verantwoording en adviseren van de gemeenteraad over verantwoording ENSIA.
 |

### Gemeentesecretaris

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Namens de portefeuillehouder: vervullen van de rol van gedelegeerd opdrachtgever voor de operationele sturing van ENSIA-uitvoering.
* Benoemen van de coördinator.
* Sturing van de uitvoering van ENSIA-verantwoording
* Beschikbaar stellen van benodigde middelen en resources voor de uitvoering van ENSIA.
* Faciliteren van coördinator ENSIA bij besluitvorming.
 | * Is eindverantwoordelijk voor tijdige uitvoering van ENSIA met bijbehorende tijd, geld en kwaliteitsaspecten.
 | * Aanstelling ENSIA-coördinator en vervanger.
 |

### ENSIA – coördinator

| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| --- | --- | --- |
| * Schrijven plan van aanpak voor uitvoering ENSIA.
* Opzetten projectorganisatie.
* Plannen en uitvoeren Kick-Off.
* Organiseren ENSIA-verantwoordingsproces.
* Intern uitzetten vragenlijsten inleveren antwoorden die nodig zijn voor zelfevaluatie DigiD en antwoorden die nodig zijn voor volledige zelfevaluatie (vóór 31 december 2025).
* Uploaden verantwoordings-documenten (Collegeverklaring en bijlagen, TPM’s en verantwoordingsrapportages).
* Opstellen van de collegeverklaring Informatiebeveiliging.
* Organiseren opdrachtverlening voor IT-audit.
* Organiseren opdracht voor pentesten per DigiD-aansluiting.
* Faciliteren werkzaamheden van RE-Auditor en bewaken tijdige oplevering Assurance Rapport.
* ENSIA-proces en stappen afstemmen met de RE-auditor.
* Verzamelen TPM’s van derde partijen en controleren op compleetheid.
* Inventariseren en toewijzen van verbeterpunten.
* Ondersteunen van domeindeskundigen bij de verantwoording en bij invullen zelfevaluatievragenlijsten.
* Organiseren werkgroepoverleggen en -bijeenkomsten.
* Coördineren/faciliteren van alle activiteiten die leiden tot paragraaf Informatiebeveiliging in jaarverslag en separate Rapportage informatieveiligheid.
* Interne communicatie t.b.v. domeindeskundigen, management, maar ook niet- direct betrokkenen.
* Externe communicatie en afstemming met ondersteunende organisaties, zoals VNG Realisatie.
 | * Projectleiding.
* Zorgdragen voor brede betrokkenheid en draagvlak binnen de organisatie.
* Borgen van tijdige inlevering van antwoorden en het volledig uploaden van documenten.
* Voortgang en scope bewaken van het project.
* Tijdige afsluiting van implementatie van ENSIA, binnen met de opdrachtgever overeengekomen afspraken over tijd, geld en kwaliteit.
* Nauw overleg met CISO m.b.t. afstemmen procedures, maatregelen en controles die wel/niet worden uitgevoerd.
 | * Het nemen van operationele beslissingen binnen het raamwerk van het (met de opdrachtgever overeengekomen en goedgekeurde) plan van aanpak met vastgestelde tijd, geld en kwaliteitsafspraken.
 |

### CIO of informatiemanager

Als de CIO door de gemeentesecretaris is aangewezen als coördinator, dan heeft hij/zij dezelfde taken en verantwoordelijkheden als deze coördinator (Zie de vorige tabel). Als de CIO niet fungeert als ENSIA-coördinator, dan zijn de taken, verantwoordelijkheden en bevoegdheden in relatie tot ENSIA als volgt:

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Ondersteunen van coördinator bij definiëren van taken en toewijzen aan bijv. proceseigenaren.
* Afstemming met CISO over informatiebeveiligingsbeleid en de uitvoering daarvan. Bepaling van consequenties na implementatiefase ENSIA. Aanpassen begroting t.b.v. verantwoording informatieveiligheid.
* Borgen van archivering van ENSIA- verantwoordingsdocumentatie
 | * Opstellen Informatiebeveiligingsbeleid en –plan.
* Aansturen op de invoering van procedures, maatregelen en controles.
* Afspraken met leveranciers over het treffen en verantwoorden van informatiebeveiligings-maatregelen.
 | * Uitbreiden van middelen in termen van manuren of geld.
* Escaleren waar nodig.
 |

### CISO

Als de CISO door de gemeentesecretaris wordt aangewezen als coördinator ENSIA, dan heeft hij/zij dezelfde taken en verantwoordelijkheden als deze coördinator (zie paragraaf ENSIA-coördinator). Indien de CISO niet fungeert als ENSIA-coördinator, dan zijn de taken, verantwoordelijkheden en bevoegdheden in relatie tot ENSIA als volgt:

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Ondersteunen van de ENSIA-coördinator als expert op het terrein van informatiebeveiliging.
* Opstellen, bijstellen, vernieuwen en herzien van het Informatiebeveiligingsbeleid en de daaruit voortvloeiende Informatiebeveiligingsplannen.
* Opnemen van verbeterpunten vanuit evaluatie ENSIA in de informatiebeveiligingsplannen.
* Ondersteunen van lijnmanagement bij verbeteracties.
* Adviseren van het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheids-gebieden. Daarnaast adviseren bij de implementatie van deze plannen.
* Afstemmen van ENSIA met overige lopende projecten in de organisatie.
 | * Verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het Informatiebeveiligingsbeleid en de daaruit voortvloeiende Informatiebeveiligings-plannen (inclusief verbeteracties).
* Projecten leiden die als doel hebben beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en waar nodig te verbeteren.
* Prioriteren van maatregelen die ingevoerd worden om de effectiviteit van informatieveiligheid te vergroten.
 | * De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen doen en zo nodig zaken af te dwingen.
* Bij (grote) beveiligingsincidenten/- risico’s heeft de CISO de bevoegdheid direct in te grijpen (met verantwoording achteraf richting het management).
* Gevraagd en ongevraagd rapporteren aan het college van B&W of de Raad.
 |

### Controller

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Afstemmen met ENSIA-coördinator over P&C-cyclus.
* Input leveren aan passende tekst voor paragraaf bedrijfsvoering voor jaarverslag.
* Rapporteren van de uitkomsten van interne audits, beveiligingsincidenten (i.s.m. CISO) en misstanden aan college of B&W.
 | * Nauw overleg met CISO voor de uitvoering van interne audits, of specifieke plekken waar procedures, maatregelen en controles (lees: verantwoording) getoetst worden.
* Rapporten van interne audits overeenkomen met college B&W.
 | * Toetsen of procedures worden gehandhaafd, maatregelen worden toegepast, en controles worden uitgevoerd. De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen doen en zo nodig zaken af te dwingen. Gevraagd en ongevraagd rapporteren aan het college van B&W of de raad.
 |

### Lijnmanagers

Zoals de managers Burgerzaken/Publiekszaken, Sociaal domein, Ruimtelijke ordening, ICT, HR, Facilitair.

|  |  |  |
| --- | --- | --- |
| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| * Maken van resource afspraken met coördinator.
* Tijdige levering van medewerkers, met juiste expertise, aan het ENSIA-project.
* Tijdige realisatie van verbeteracties voortvloeiend uit het ENSIA-project.
 | * Is primair verantwoordelijk voor de domein/materie specifieke kennis en ervaring van opgeleverde resources.
* Kwaliteit bewaken van informatiebeveiliging van die domeinen waarvoor zijn/haar afdeling verantwoordelijk is.
* Opnemen van verbeteracties in informatiebeveiligingsplan en zorgen voor de tijdige realisatie.
* Realiseren van constante aandacht voor informatieveiligheid in eigen domein, inclusief verbeteringen.
 | * Bepalen welke medewerkers uit de afdeling in de rol van domeindeskundigen bijdragen aan de uitvoering van ENSIA.
* Bepalen wie als gegevensbeheerders fungeren, die een rol hebben in de waarborging van informatieveiligheid.
 |

### Domeindeskundigen

Domeindeskundigen zijn medewerkers afkomstig van de afdelingen of samenwerkingsverbanden zoals: zoals Burgerzaken/Publiekszaken, Sociaal domein, Ruimtelijke ordening, ICT, HR, Facilitair of Belastingen. Ze worden door hun lijnmanager in overleg met een coördinator aan het project beschikbaar gesteld. Elke domeindeskundige heeft specifieke kennis van het eigen domein en al dan niet kennis van informatiebeveiliging en/of datakwaliteit en -integriteit op dit domein (BRP, Reisdocumenten, Suwinet, BAG, BGT en BRO en DigiD).

| **Taken** | **Verantwoordelijkheden** | **Bevoegdheden** |
| --- | --- | --- |
| * Deelname aan kick-off ENSIA.
* Met coördinator vaststellen welke zelfevaluatievragen hij/zij oppakt.
* Beantwoorden van ENSIA- zelfevaluatie binnen (met de coördinator overeengekomen) tijds- en kwaliteitsafspraken.
* Legt hiaten of uitzonderingen vast in de ENSIA-vragenlijst en doet voorstellen voor verbeteracties.
* Rapporteren over voortgang van de taken aan de ENSIA-coördinator.
* Deelname aan werkgroep- bijeenkomsten voor afstemming over de zelfevaluatievragen.
* Informeert collega’s binnen het domein over ENSIA-verantwoordingsproces en informatieveiligheid.
* Verbindt van kennis van domein met informatiebeveiliging.
* Pakt indien nodig in overleg met CISO, coördinator en lijnmanager verbeteracties op.
 | * Inzicht verwerven in informatieveiligheidsaspecten van het eigen domein.
* Is, met anderen, verantwoordelijk voor tijdige beantwoording van ENSIA-zelfevaluatie vragen, waarover met de ENSIA-coördinator afspraken zijn gemaakt.
* Fungeert als gegevensbeheerder die een rol heeft in de waarborging van informatieveiligheid.
 |  |