Handreiking

Plan van aanpak 2022

**VNG Realisatie**

Nassaulaan 12

2514 JS Den Haag

Juli 2022

Inhoud

[1. Doel van het format Plan van Aanpak 3](#_Toc109897627)

[1.1. Waarom dit Plan van Aanpak (PvA)? 3](#_Toc109897628)

[1.2. Toelichting op het gebruik van verschillende lettertypes 3](#_Toc109897629)

[1.3. Advies besluitvorming PvA 3](#_Toc109897630)

[2. Indeling en achtergrond 4](#_Toc109897631)

[2.1. Waarom ENSIA? 4](#_Toc109897632)

[2.2. Wat is ENSIA? 4](#_Toc109897633)

[2.3. Tijdpad ENSIA 5](#_Toc109897634)

[2.4. Nieuw in het verantwoordingsjaar 2022 5](#_Toc109897635)

[2.5. Overige aandachtspunten voor het verantwoordingsjaar 2022 5](#_Toc109897636)

[3. Inleiding 7](#_Toc109897637)

[3.1. Doelstelling 7](#_Toc109897638)

[3.2. Uitgangspunten 7](#_Toc109897639)

[3.3. Aanpak en methodiek 7](#_Toc109897640)

[3.4. Resultaat 8](#_Toc109897641)

[3.5. Wat doe de verantwoording ENSIA niet? 8](#_Toc109897642)

[3.6. Relaties met andere projecten en activiteiten 9](#_Toc109897643)

[4. Planning 10](#_Toc109897644)

[4.1. Hoofdlijnen 10](#_Toc109897645)

[4.2. Planning en fasering 10](#_Toc109897646)

[4.3. Activiteitenplanning 12](#_Toc109897647)

[5. Organisatie 16](#_Toc109897648)

[5.1. Opdrachtgeversoverleg ENSIA 16](#_Toc109897649)

[5.2. Werkgroep ENSIA 16](#_Toc109897650)

[5.3. Overlegstructuur 18](#_Toc109897651)

[5.4. Interne stakeholders 18](#_Toc109897652)

[5.5. Externe stakeholders 19](#_Toc109897653)

[5.6. Samenwerkingsverbanden 20](#_Toc109897654)

[5.7. Begroting 20](#_Toc109897655)

[A. Bijlage: Rol- en taakbeschrijvingen interne stakeholders 21](#_Toc109897656)

[College van B&W 21](#_Toc109897657)

[Portefeuillehouder informatiebeveiliging 22](#_Toc109897658)

[Gemeenteraad 22](#_Toc109897659)

[Griffier 22](#_Toc109897660)

[Gemeentesecretaris 23](#_Toc109897661)

[ENSIA - coördinator 23](#_Toc109897662)

[CIO of informatiemanager 24](#_Toc109897663)

[CISO 24](#_Toc109897664)

[Controller 25](#_Toc109897665)

[Lijnmanagers 25](#_Toc109897666)

[Domeindeskundigen 26](#_Toc109897667)

## Doel van het format Plan van Aanpak

### Waarom dit Plan van Aanpak (PvA)?

Dit format Plan van Aanpak ENSIA 2022 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 2022. 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 relevante 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 een toelichting op het in de paragraaf beschreven onderwerp.
* Standaard geschreven teksten zijn teksten die u kunt overnemen in uw eigen plan van aanpak.
* [Geel gearceerd] zijn teksten waar de eigen gemeentenaam of naam van de medewerker kan worden ingevuld.

### 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 creëren 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 van de gemeente.

## Indeling en achtergrond

### Waarom ENSIA?

Burgers verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informa-tie(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 (al gerealiseerde) thema’s en projecten zoals de resultaten van de zelfevaluatie 2021 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’[[1]](#footnote-2) aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid. Sinds 2020 is de Baseline Informatiebeveiliging Overheid (BIO) het verplichte gemeentelijk normenkader 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 en de WOZ ligt hierop de nadruk.

Met ENSIA sluit de verantwoording over informatieveiligheid en datakwaliteit/data-integriteit aan op de planning en control-cyclus 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 Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) en een gedeelte van de Wet Onroerende Zaken (WOZ).

### Tijdpad ENSIA

Op 1 juli 2022 start het zesde jaar van verantwoording met ENSIA. De zelfevaluatie moet vóór 31 december 2022 zijn ingeleverd. In het voorjaar van 2023 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 2022

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.

In het verantwoordingsjaar 2022 zijn de volgende vernieuwingen geïntroduceerd:

* De BIO-vragenlijst is uitgebreid met controls waarvoor geen verplichte overheidsmaatregelen gelden. Daarmee kan nu over de gehele BIO verantwoord worden. Er zijn aanvullende maatregelen opgenomen in de tool, waarvoor moet worden ingevuld welke maatregel de organisatie heeft gedefinieerd. Het is ook mogelijk om gemeentebreed controls en/of maatregelen ‘niet-van-toepassing’ te verklaren. Dit kan niet voor de vragen die voor de verantwoording aan het rijk worden gesteld (BKWI, RvIG). Ook is een aantal vragen in de BIO-vragenlijst tekstueel aangepast (vraagstelling, toelichting en verwijzing naar wet- en regelgeving).
* In de Bijlage 2 Suwinet van de collegeverklaring is de tabel met Suwi-taken uitgebreid voor Wgs (Wet gemeentelijke schuldhulpverlening).
* De vragen voor de BAG, BGT en BRO zijn op enkele punten aangepast. Ook is de rappor-tage verbeterd door een betere toelichting op de behaalde percentages en het overnemen van maatregelen uit de vragenlijst in de rapportage.
* In de WOZ-vragenlijst zijn vragen vervangen en inhoudelijk verbeterd.
* De DigiD-vragenlijst is eenduidiger gemaakt door een meer heldere vraagstelling en het la-ten vervallen van irrelevante vragen.
* Aan de VDW-rapportage is een maatregel toegevoegd bij “Beheer bedrijfsmiddelen” en zijn twee nieuwe maatregelen beschrijven in een nieuw hoofdstuk “Netwerken”.
* Rapportages kunnen voortaan vanaf 1 juli worden vervaardigd. Gedurende de zelfevaluatiefase bevatten ze het kenmerk “Concept”. Dit kenmerk verdwijnt vanaf 1 januari 2023 op het moment dat de verantwoordingsfase start.

### Overige aandachtspunten voor het verantwoordingsjaar 2022

* De collegeverklaring over Suwinet en DigiD wordt vastgesteld door het college van B & W. De collegeverklaring heeft niet langer de raad als doelgroep opgenomen en is vanaf dit verantwoordingsjaar alleen bestemd voor het college en de toezichthouders voor Suwinet (BKWI) en DigiD (Logius). De tekst van de collegeverklaring is hierop aangepast. U dient echter wel de raad te informeren over de status van informatiebeveiliging en de uitkomsten van de IT-audit (interne verantwoording over de BIO). Hier wordt een (vormvrij) sjabloon voor ter beschikking gesteld.
* Suwinet volgt de Verantwoordingsrichtlijn 2022. Deze is volledig op basis van de BIO opgesteld en in te zien via de site van [BKWI](https://www.bkwi.nl/).
* Voor Suwinet geldt de [carve-out methodiek](https://vng.nl/media/48296). 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.
* In de BIO-zelfevaluatie worden specifieke vragen over de Suwinet-bevragingen voor Burgerzaken, RMC en voor de heffingen door de gemeentelijk gerechtsdeurwaarders (belastingsamenwerking) gesteld. Zonder input vanuit de TPM’s voor Suwinet (zie ook vorig punt) kunnen we de zelfevaluatie ENSIA niet voor 31 december afsluiten. Sturing op tijdige aanlevering van deze TPM’s is belangrijk.
* De wettelijke inlevertermijn voor de uittreksels BRP en Reisdocumenten is voortaan ook 30 april.

## Inleiding

### Doelstelling

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 en WOZ op te leveren aan de toezichthouders van het Rijk.

### Uitgangspunten

*Beschrijf hier welke uitgangspunten de gemeente hanteert bij de verdere uitwerking van de aanpak. Denk hierbij aan:*

* *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 2021 n.a.v. uitgevoerde zelfevaluatie;*
* *Interne communicatie via bestaande kanalen (welke?).*

De gemeente gaat bij de uitwerking van de ENSIA-verantwoording 2022 uit van de volgende uitgangspunten:

* …

### Aanpak en methodiek

*Hoe wilt u de organisatie van de verantwoording aanpakken? Wat zijn de ervaringen met het verantwoordingsjaar 2021 (intern en extern). Elementen die in de aanpak kunnen worden opgenomen zijn bijvoorbeeld:*

* *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 vragen bij domeinen).*
* *Proces om te komen tot een definitief antwoord.*
* *Aandacht voor informatievoorziening aan alle medewerkers.*

De gemeente gaat bij de aanpak van de ENSIA-verantwoording 2022 uit van de volgende uitgangspunten:

* …

### 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;
* Het college heeft de rapportages uit ENSIA m.b.t de WOZ vastgesteld;
* De relevante informatie voor de verantwoording aan het rijk wordt in de ENSIA-tool tijdig ingeleverd (voor 1 mei 2023).

### Wat doe de verantwoording 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 informatieveiligheidsvragen over de BRP en de Reisdocumenten binnen ENSIA gesteld voor uitvoering van de zelfevaluatie en verantwoording. De antwoorden op de ENSIA-vragen voor BRP en Reisdocumenten moeten uiterlijk 31 december 2022 in het ENSIA-platform worden ingeleverd. In de fase verantwoorden, vanaf 1 januari 2023, moeten de verantwoordingsrapportages (na vaststelling door het college) worden geüpload via de Kwaliteitsmonitor. De verantwoording over BRP en de Reisdocumenten loopt hiermee mee in het proces van de Kwaliteitsmonitor en maakt daarom niet voor het gehele proces deel uit van het verantwoordingsproces met ENSIA. De verantwoording BRP en Reisdocumenten moet uiterlijk 30 april 2023 zijn aangeleverd bij RvIG.*

De volgende aspecten m.b.t. verantwoording vallen niet onder de scope van ENSIA:

* …

### 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 2021;*
* *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).*

De volgende projecten/activiteiten hebben een raakvlak met de uitvoering van de ENSIA-verantwoording 2022:

* …

## Planning

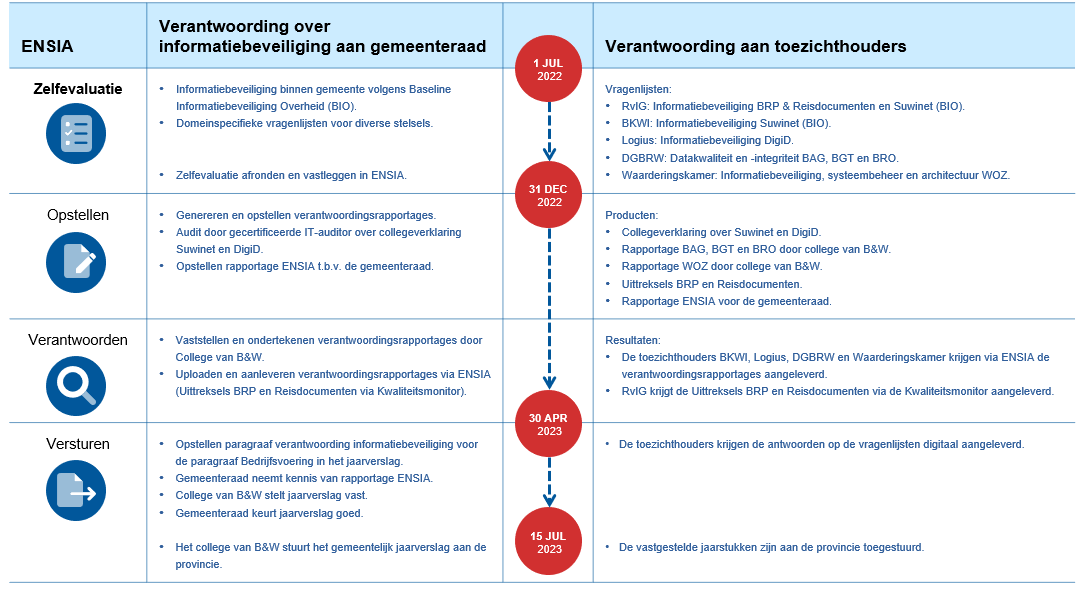
Dit hoofdstuk gaat in op de activiteiten die in dit project moeten worden uitgevoerd: de fasering van het project, de activiteiten, de randvoorwaarden en de externe afhankelijkheden.

### Hoofdlijnen

De hoofdlijnen van de planning zien er als volgt uit.

Afbeelding met tekst

Automatisch gegenereerde beschrijving



### Planning en fasering

|  |  |  |
| --- | --- | --- |
| Fase | Van | Tot en met |
| Voorbereiding | 01-06-2022 | 30-06-2022 |
| Zelfevaluatie | 01-07-2022 | 31-12-2022 |
| Opstellen | 01-01-2023 | 30-04-2023 |
| Verantwoorden | 01-01-2023 | 30-04-2023 |
| Versturen | 01-01-2023 | 14-07-2023 |
| Evaluatie | 01-05-2023 | 31-05-2023 |

In de fase Voorbereiding treft de ENSIA-coördinator de voorbereidingen voor het nieuwe verantwoordingsjaar. Zoals bijvoorbeeld het opstellen van dit plan van aanpak en het formeren van een team dat de ENSIA-verantwoording gaat doen. De ervaringen van het afgelopen verantwoordingsjaar worden hierin meegenomen.

In de fase Zelfevaluatie verantwoordt de gemeente zich over informatiebeveiliging over de Baseline Informatiebeveiliging Overheid en over andere stelsels waarvoor domeinspecifieke vragenlijsten bestaan. Voor BRP en Reisdocumenten en Suwinet gebruiken we de hiervoor de BIO-vragenlijst. Voor DigiD, BAG, BGT, BRO en de WOZ) zijn domeinspecifieke vragenlijsten.

In de fase Opstellen worden de verantwoordingsrapportages gedownload en door de verantwoordelijke personen aangevuld. Voor DigiD en Suwinet wordt een collegeverklaring opgesteld die door een auditor getoetst wordt. Het resultaat van deze fase is een collegeverklaring voor DigiD en Suwinet, een rapportage over de BAG, BGT en BRO, een rapportage over de WOZ, de Uittreksels BRP en Reisdocumenten en een rapportage over ENSIA aan de gemeenteraad. De collegeverklaringen en de verantwoordingsrapportages worden aan het college aangeboden.

De fase Verantwoorden start op het moment dat de collegeverklaringen en de verantwoordingsrapportages door het College van B&W worden behandeld. Dit moet voor 30 april 2023 gebeuren. Het College van B&W stelt de documenten vast en ondertekend ze. Daarna worden de rapportages in ENSIA geüpload. De rapportages voor BRP en Reisdocumenten worden echter via de Kwaliteitsmonitor van RvIG geüpload. Het resultaat van deze fase is dat de toezichthouders uiterlijk 30 april 2023 de gevraagde verantwoordingsrapportages ontvangen.

De fase Versturen heeft betrekking op het jaarverslag en de jaarrekening van de gemeente. Deze start op 1 mei 2023. Het college van B&W neemt in het jaarverslag in de paragraaf Bedrijfsvoering een aparte subparagraaf op over informatiebeveiliging. Hierin rapporteert het College aan de gemeenteraad over informatiebeveiliging. Nadat het College van B&W het jaarverslag heeft vastgesteld en de gemeenteraad het heeft goedgekeurd, worden de jaarstukken door het college aan de provincie verstuurd. Dit moet voor 15 juli.

In de fase Evaluatie evalueert de ENSIA-coördinator met zijn team het afgelopen jaar en stelt vast wat goed ging en wat beter kan. De evaluatie is weer input voor de fase Voorbereiding.

### Activiteitenplanning

#### Fase Voorbereiding

|  |  |
| --- | --- |
| Voorbereiding 1 juni – 1 juli 2022 | Wie |
| Benoemen ENSIA-coördinator | Gemeentesecretaris |
| Bestuderen achtergrondinformatie (scope 2022) | ENSIA-coördinator |
| Opstellen plan van aanpak | ENSIA-coördinator |
| Uitvoeren korte risicoanalyse m.b.t. succes ENSIA | … |
| Inventariseren en informeren intern en extern betrokkenen | ENSIA-coördinator |
| Toewijzen taken bevoegdheden en verantwoordelijkheden   * Verantwoordelijken domeinen (BRP/Reisdocumenten, BAG/BGT/BRO, SUWI, DIGID, WOZ) * Verantwoordelijken op afdelingen (IT, HRM, Facilitair, Inkoop, Juridisch, Belastingen) * Betrokkenen vanuit samenwerkingsverbanden   + SSC IT   + Regionale Sociale Dienst   + Regionale Belastingsamenwerking | ENSIA-coördinator |
| Inventariseren stakeholders   * ENSIA-collega’s in de regio * Auditor * Leveranciers * Portefeuillehouder(s) * FG * Controller * Raad * Communicatie | ENSIA-coördinator |
| Afstemming interne communicatie | … |
| Kick-off verantwoording ENSIA 2022 \*   * Scope ENSIA 2022 * Jaarcyclus ENSIA * Zelfevaluatie en wijzigingen t.o.v. 2021 * Planning en aanpak 2022 * Hoe werken we samen * Samenwerkingsverbanden & leveranciers * Afsluiting   \* Zie het Format Kick-off bijeenkomst ENSIA 2022.pptx. | ENSIA-coördinator |

Resultaat fase Voorbereiding:

1. De gemeente is klaar om op 1 juli 2022 te starten met het invullen van de zelfevaluatie.

#### Fase Zelfvaluatie

| Uitvoering zelfevaluatie 1 juli – 31 december 2022 | Wie |
| --- | --- |
| Opdracht auditor collegeverklaring 2022   * Bepaal scope afhankelijk van inzet TPM’s SUWI | … |
| Aanvraag TPM’s samenwerkingsverband(en) Suwinet   * Oplevering uiterlijk 15 oktober 2022 | … |
| Aanvraag TPM(‘s) DigiD leverancier(s)   * Oplevering uiterlijk 15 oktober 2022 | … |
| 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 leveranciers * TPM van samenwerkingsverbanden SUWI * Domeinspecifieke zelfevaluaties * Invullen ENSIA-zelfevaluatie 2022 (BIO) | ENSIA-coördinator |
| Inventariseren van in te zetten verbeteracties voor 31-12-2022 | ENSIA-coördinator |
| Akkoord op definitieve antwoorden | ENSIA-coördinator |
| Inleveren vragenlijsten voor 31 december 2022   * ENSIA-zelfevaluatie 2020 (BIO) * DigiD * BAG * BGT * BRO * BRP en Reisdocumenten * Waar staat je gemeente * WOZ | ENSIA-coördinator |
| Informeren stakeholders over afronding zelfevaluatie en start van verantwoordingsproces | ENSIA-coördinator |

Resultaat fase Zelfevaluatie:

1. Directe maatregelen zijn ingezet als de resultaten uit de zelfevaluatie hier aanleiding voor geven.
2. De gemeente heeft alle vragenlijsten beantwoord en ingeleverd voor 31 december 2022.

#### Fase Opstellen

| Afronding interne verantwoording 1 januari – 30 april 2023 | Wie |
| --- | --- |
| Analyse uitkomsten zelfevaluatie | ENSIA-coördinator + … |
| Opstellen rapportage informatiebeveiliging (BIO) | ENSIA-coördinator + … |
| Aanvullen uittreksels BRP en Reisdocumenten | ENSIA-coördinator + … |
| Opstellen verbeterplan (indien nodig 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 control  ENSIA-coördinator  CISO |
| Inplannen behandeling College B&W   * Interne verantwoording informatiebeveiliging (BIO) * Collegeverklaring DigiD en Suwinet * Ondertekening uittreksels BRP en Reisdocumenten * Vaststelling rapportages BAG, BGT & BRO en WOZ | ENSIA-coördinator + bestuurssecretariaat |

Resultaat Fase Opstellen:

1. Rapportages voor B&W zijn opgesteld.
2. Collegeverklaring met bijlagen DigiD en Suwinet is opgesteld.
3. Verbeterplan is opgesteld

#### Fase Verantwoorden

| Afronding interne verantwoording 1 januari – 30 april 2023 | Wie |
| --- | --- |
| Behandeling College B&W   * Vaststelling interne verantwoording informatiebeveiliging (BIO) * Ondertekening collegeverklaring Suwinet en DigiD * Ondertekening uittreksels BRP en Reisdocumenten * Vaststelling rapportages BAG/BGT/BRO en WOZ | Collegeverklaring door GS en College van B&W  BRP door GS en Burgemeester  Reisdocumenten door Burgemeester |
| Afronding auditproces   * Waarmerken individuele documenten * Opnemen in PDF/A | Auditor |
| Uploaden documenten verticale verantwoording in ENSIA uiterlijk 30 april 2023 | ENSIA-coördinator |
| Informeren van de raad via separate rapportage over status informatiebeveiliging (niet openbaar)   * Beleid, doelstellingen en ambities * Samenvatting gemeente brede beeld en resultaten zelfevaluatie ENSIA 2022 * Belangrijkste maatregelen * Realisatie van doelstellingen/verbeteringen * Incidenten * Meerjarenperspectief | College van B&W (opstellen door ENSIA-coördinator en/of CISO) |

Resultaat fase Verantwoorden:

1. De door het College, Burgemeester en Gemeentesecretaris vastgestelde stukken zijn aangeleverd bij de Stelselhouders.
2. De door de gemeenteraad vastgestelde jaarstukken zijn voor 15 juli 2023 toegestuurd aan de provincie.

#### Fase Versturen

| Versturen 1 mei – 15 juli 2023 | Wie |
| --- | --- |
| Versturen vastgestelde jaarstukken naar provincie | Controller |

Resultaat fase Versturen:

1. De door het College, Burgemeester en Gemeentesecretaris vastgestelde stukken zijn aangeleverd bij de Stelselhouders.
2. De door de gemeenteraad vastgestelde jaarstukken zijn voor 15 juli 2023 toegestuurd aan de provincie.

#### Fase Evaluatie

| Evaluatie 1 mei – 1 juni 2023 | 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 | * 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. |

**Tabel: Samenstelling opdrachtgeversoverleg ENSIA**

### 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.*

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-ciso-functieprofiel/>. |
| Functionaris Gegevensbescherming (FG) / Adviseur Privacy | […] | * 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 vragen m.b.t. Suwinet binnen de gemeente. * Agenderen van ENSIA in werkoverleg(en) indien van toepassing:   + P-Wet/IOAZ/IOAW   + RMC   + Burgerzaken   + Gemeentelijk Gerechtsdeurwaarders |
| 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. |
| Domeindeskundige WOZ (mogelijk extern i.v.m. belastingsamenwerking) |  | * Bijdrage aan invullen WOZ-vragenlijst. * Agenderen van ENSIA in werkoverleg van eigen afdeling/organisatie. |
| 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 / Adviseur Privacy) | […] | * Mede invullen vragen gerelateerd aan privacy. * Agenderen van ENSIA in werkoverleg van eigen afdeling . |
| Communicatiemedewerker | […] | * Aanpassen webberichten. * Plaatsen webberichten. * Redigeren eindrapportages. |
| Aanspreekpunt Samenwerkingsverband IT/SSC/GR | […] | * Bijdrage aan invullen IT-vragen BIO-vragenlijst. |
| Aanspreekpunt Belastingsamenwerking | […] | * Bijdrage aan invullen Suwinet-vragen BIO vragenlijst m.b.t. gebruik Suwinet voor Gemeenten Gerechtsdeurwaarders. |
| Aanspreekpunt ISD | […] | * Bijdrage aan invullen Suwinet vragen BIO vragenlijst m.b.t. gebruik Sociale Dienst (uitvoering P-wet/IOAZ/IOAW). * Coördinatie uitvoering SUWI-audit (afgestemd met deelnemende gemeenten in de samenwerking). |

**Tabel: Samenstelling ENSIA-werkgroep**

*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. |

**Tabel: Overlegstructuur ENSIA**

### 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. * Vaststellen rapportage WOZ. |
| Burgemeester | [Naam] | * Ondertekenen rapportage BRP en Reisdocumenten. |
| Portefeuillehouder | [Naam] | * Uitnodigen voor kick-off. |
| Gemeentesecretaris | [Naam] | * Borging benodigde capaciteit voor uitvoering taken. * Informeren resultaten zelfevaluatie. * Ondertekenen rapportage BRP. |
| Directeur/Manager 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] | * … |

**Tabel: Interne stakeholders**

### 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 2022). * 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 | * Zie <https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten/>. |
| Auditor | [Bedrijf en naam contactpersoon] | * Uitvoeren audit | * Opdrachtverlening – uiterlijk oktober 2022. * Zie format opdracht auditor. |
| … |  |  |  |

**Tabel: Externe stakeholders**

### 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?*

### Begroting

*Voor de verantwoording ENSIA 2022 is mogelijk budget benodigd geweest. Op basis van deze ervaringen kunt u de begroting opstellen voor 2023. 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.*

## A. Bijlage: Rol- en taakbeschrijvingen 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, Suwinet, BAG, BGT en BRO, BRP en Reisdocumenten, WOZ. * 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 Suwinet en antwoorden die nodig zijn voor volledige zelfevaluatie (vóór 31 december 2022). * 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 werkgroep-overleggen 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 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 informatiebeveiligingplannen. * 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, DigiD en WOZ).

| **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. |  |

1. De uitgangspunten van deze resolutie zijn herbevestigd in de nieuwe resolutie Digitale Veiligheid die op 12 februari 2021 unaniem is aangenomen in de Bijzondere Algemene Ledenvergadering van de VNG. [↑](#footnote-ref-2)