



Bestuurlijke rapportage ENSIA 2020



door
Nico Boom Strategisch Adviseur Informatie en Veiligheid



Begrippenlijst

Ensia: De Eenduidige Normatiek Single Information Audit heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus.

Collegeverklaring: Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen hebben voldaan aan de voor de ENSIA verantwoording geselecteerde normen en indien aan de orde welke onderdelen daarvan zijn uitgezonderd.

Assurance rapport: De bevindingen naar aanleiding van de controlewerkzaamheden van een accountant vinden hun weerslag in het door de accountant af te geven assurance-rapport.

SUWI: Wet Structuur Uitvoeringsorganisatie Werk en Inkomen

Suwinet: De Gemeenschappelijke elektronische Voorziening Suwi (GeVS - ook wel Suwinet genoemd) is een elektronische infrastructuur t.b.v. de Suwi ketenpartijen (UWV, SVB en gemeenten) om gegevens met elkaar te kunnen uitwisselen voor de uitoefening van onze wettelijke taak.

DigiD: Digitale Identiteit: een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening.

TPM: Third Party Mededeling is een verklaring die afgegeven wordt door een onafhankelijk audit partij over de kwaliteit van een ICT-dienstverlening en – beheersing van een organisatie

BIO: Baseline Informatieveiligheid Overheid. Vervanger- per 1-1-2020- van de Base Informatieveiligheid Gemeenten (BIG) volgens de ISO 27001. (internationale informatiebeveiligingstandaard)

IOAZ: de Wet Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen

IOAW: de Wet Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers

AVG: Algemene verordening gegevensverwerking. EU richtlijn met betrekking tot de bescherming van persoonsgegevens.

Deze bestuurlijke rapportage is een samenvatting opgesteld op basis van de uitkomsten van de ENSIA 2020 en geeft een beknopte samenvatting van de collegeverklaring DigiD en Suwinet en de uitgevoerde zelfevaluaties op het gebied van informatiebeveiliging door de gemeente Sluis.

VERANTWOORDING AAN HET RIJK UIT ENSIA

- Getoetste collegeverklaring ENSIA – DigiD (audit)
- Getoetste collegeverklaring ENSIA – Suwinet (audit)
- Status Basisregistratie Personen (BRP) en Reisdocumenten (zelfevaluatie)
- Status GEO basisregistraties (BAG, BGT, BRO) (zelfevaluatie)

STATUS INFORMATIEBEVEILIGING (BIO) (zelfevaluatie)

Getoetste Collegeverklaring ENSIA - DigiD

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor DigiD worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder Logius/BZK.

Aansluiting 1 - 97027 DigiD1 Website gemeente Sluis	Geen bijzonderheden	 voldaan
Aansluiting 2 - 1002547 DigiD2 Centric Suwinet	Een (1) bijzonderheid uit 20 controls	 Niet voldaan
Aansluiting 3 - Suwinet voor SUWI-taken	Geen bijzonderheden	 voldaan
Aansluiting 4 - Suwinet voor niet SUWI-taken	Geen bijzonderheden	 voldaan

Toelichting aansluiting 2:

Naar aanleiding van de toetsing aansluiting 2 van de Collegeverklaring Ensia 2020 en de uitgevoerde audit door Ernst & Young Accountants LLP (TPM – Third Party Mededeling) is op één van de 20 controls een afwijking geconstateerd. Bij afwijking van een van de controls krijgt de gehele set de beoordeling “voldoet niet”. De leverancier Centric is er niet in geslaagd op tijd dit punt op te lossen. De control waaraan niet wordt voldaan (U/PW.03) heeft betrekking op het inrichten van de webserver van Suwinet conform een bepaalde configuratie baseline. Het betreft een norm hoe de webserver configuratie dient te worden vorm gegeven. Dit had in 2020 uitgevoerd dienen te zijn (BIO). De nieuwe oplostermijn welke door Centric is toegezegd, is 1-11-2021. Daarmee is geborgd dat dit punt in de ENSIA 2021 geen herhaling kent.

Getoetste collegeverklaring ENSIA - Suwinet

De door de gemeente Sluis uitgevoerde ENSIA-zelfevaluatie wordt jaarlijks op 2 hoofdzaken geaudit door een externe IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor Suwinet worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder BKWI/SZW.

Binnen Suwinet worden alleen gegevens uitgewisseld waarvoor een wettelijke grondslag is. De gemeente Sluis gebruikt Suwinet voor de uitvoering van de Participatiewet, de uitvoering van de IOAZ en IOAW en het raadplegen van adresgegevens bij Burgerzaken.

Participatiewet/IOAZ/IOAW

-Suwinet Inkijk

Audit inkijk binnen de gemeente.

 voldaan

-Suwinet Inlezen

Scope: team Porthos – Externe dienstverlening

-DKD Inlezen (koppelingen)

Burgerzaken

Audit inkijk binnen de gemeente.

 voldaan

Scope: team Burgerzaken – Externe dienstverlening

Algemene toelichting:

Zoals in de collegeverklaring vermeld, voldoet de gemeente Sluis aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2020 in opzet en bestaan aan de gecontroleerde controls.

Status GEO-basisregistraties

Wij verantwoorden ons met betrekking tot de ENSIA aan het ministerie van BZK/Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) over drie basisregistraties in het geografische domein. De rapportages zijn tot stand gekomen op basis van door ons uitgevoerde zelfevaluaties. De zelfevaluaties betreffen de kwaliteit van de registraties (geen informatiebeveiliging).

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen:

- BAG 75 %
- BGT 75 %
- BRO 60 %

Basisregistratie Adressen en Gebouwen (BAG)	De zelfevaluatie BAG over het jaar 2020 is afgerond met een score van 160 van maximaal 205 zijnde 78 %	 voldaan
Basisregistratie Grootschalige Topografie (BGT)	De zelfevaluatie BGT over het jaar 2020 is afgerond met een score van 140 van maximaal 150 zijnde 93 %	 voldaan
Basisregistratie Ondergrond (BRO)	De zelfevaluatie BGT over het jaar 2020 is afgerond met een score van 105 van maximaal 120 zijnde 88 %	 voldaan

Algemene toelichting:

Met de BAG en BGT zelfevaluatie heeft de gemeente een score die boven de norm blijft. Deze zijn vergelijkbaar met de ENSIA 2019. Op het gebied van de BRO is vanuit de verbeterplannen een significante verbetering in de zelfevaluatie opgetekend ten opzicht van de score in de ENSIA 2019 zelfevaluatie (16,7%).

Status Basisregistratie Personen en Reisdocumenten

Van onze zelfevaluatie ENSIA wordt de verantwoording over de Basisregistratie Personen (BRP) en de wet - en regelgeving voor de Reisdocumenten (paspoorten en ID-kaarten) afgeleid. De uitkomsten worden verzonden aan de Rijksdienst voor de Identiteitsgegevens (RvIG). De zelfevaluatie voor informatiebeveiliging vindt via de ENSIA systematiek plaats. De verantwoording over de kwaliteit van de registraties komt voort uit de zelfevaluatie in de Kwaliteitsmonitor.

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. De volgende scores zijn behaald.

Basisregistratie Personen (BRP):	De zelfevaluatie BRP over het jaar 2020 is afgerond met een score 100 %	 voldaan
Wet- en regelgeving voor Reisdocumenten:	De zelfevaluatie Reisdocumenten over het jaar 2020 is afgerond met een score van 100 %	 voldaan

Algemene toelichting :

Met de BRP en Reisdocumenten zelfevaluatie heeft de gemeente een score die ten opzichte van de ENSIA 2019 ruim is verbeterd. (respectievelijk 15,2 % en 11%).

Resultaten zelfevaluatie informatiebeveiliging BIO

BESTUURLIJKE UITGANGSPUNTEN

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van de gemeente Sluis:

- Volgt het integrale Informatie beveiliging- en Privacy beleid 2020-22 (afgeleid van het IB-Beleid VNG-IBD)
- Zorgt ervoor dat de juiste informatiebeveiliging door de gemeentelijke organisatie wordt uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

Toetsing uitgevoerd op basis van gemeentelijke zelfevaluatie ENSIA 2020 door de diverse betrokken afdelingen/teams, CISO en Privacy-Officer.



1. BELEID EN ORGANISATIE

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving



2. PERSONEEL EN TOEGANG

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens



3. CONTINUÏTEIT EN INCIDENTEN

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten



4. INFORMATIESYSTEMEN

Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers



5. DATABESCHERMING

Veilige omgang met data in onze software

