Informatiebeveiligings-rapportage 2019

Gemeente Het Hogeland

09-06-2020

Kenmerk:	Z.HHL.012986
Versie:	V1.0
Versiedatum:	09-06-2020
Gemaakt door:	G. Groot
Portefeuillehouder	Dhr. H.J. Bolding
Goedgekeurd door:	
Classificatie:	Openbaar

Versiebeheer

Versie	Datum	Auteur	Opmerkingen
0.5C	8-4-2020	Guido Groot	Opzet rapportage informatiebeveiliging 2019
0.6C	30-4-2020	Guido Groot	Reviewen rapportage teamcoach Gegevenshuis, coördinator en beveiligingsbeheerder Burgerzaken, FG, BAG-, BGT, BRO- beheerders.
0.7C	25-5-2020	Guido Groot	Aanvulling status BIO en datalekken (FG)
0.7C	3-6-2020	Guido Groot	Review rapportage concerncontroller
0.8C	4-6-2020	Guido Groot	Terugkoppeling concerncontroller verwerkt in rapportage.
V1.0	8-6-2020	Guido Groot	Rapportage besproken met de burgemeester en gemeentesecretaris.

Inhoudsopgave

1. Inleiding

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeenten om hun processen uit te voeren. Gemeenten beschikken over een schat aan vertrouwelijke informatie, over zowel burgers als bedrijven. Daarnaast is de gemeente verantwoordelijk voor een betrouwbare en continue dienstverlening. Het is daarom belangrijk dat gemeente Het Hogeland op passende wijze de informatie beveiligen.
Het begrip 'informatiebeveiliging' heeft betrekking op beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid van gegevens. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Gemeenten dienen bij hun informatiebeveiliging te voldoen aan wet- en regelgeving, zoals bijvoorbeeld voor de privacywetgeving.

Dit rapport geeft de uitkomsten weer van de gemeentebrede (horizontaal) uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2019. Deze zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten[1] (BIG)
In welke mate we voldoen aan deze Baseline is getoetst door middel van een zelfevaluatie die is uitgevoerd in de periode van 6 augustus 2019 tot 16 december 2019. Gemeente Het Hogeland rapporteert op één moment in het jaar over de status van onze informatieveiligheid. De methodiek heet ENSIA[2] en staat voor Eenduidig Normatiek Single Information Audit.

De verantwoording informatieveiligheidsvragen aan de stelselhouders over de Basisregistratie Personen (BRP), de wetgeving voor Reisdocumenten (PUN/PNIK) en Suwinet wordt afgeleid vanuit deze BIG-zelfevaluatie.

Voor de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergrond (BRO) en DigiD zijn separate evaluaties in ENSIA uitgevoerd.

Voor het verantwoordingsjaar 2019 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en BZK) wordt verantwoord door middel van een collegeverklaring. De collegeverklaring is opgesteld op basis van de bevindingen uit de zelfevaluaties en wordt getoetst door een IT-auditor. Deze neemt de bevindingen op in een Assurance rapport. Met het aanleveren van de vastgestelde collegeverklaring en het Assurance rapport voldoet gemeente Het Hogeland aan de verantwoordingsplicht voor Suwinet en DigiD.

Verder wordt in dit rapport ingegaan op de status van de Baseline Informatiebeveiliging Overheid. De Baseline Informatiebeveiliging Gemeenten is per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). 2019 werd dan ook gezien als een overgangsjaar van BIG naar BIO.

In deze rapportage gaat het college verder in op:

- Uitkomsten zelfevaluatie informatieveiligheid.
- Uitkomsten toetsing collegeverklaring DigiD en Suwinet.
- Uitkomsten zelfevaluatie BRP en PNIK.
- Uitkomsten zelfevaluatie BAG, BGT en BRO.

---

[1] De BIG/ BIO is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke informatie(systemen) bevordert. Het is een richtlijn die een totaalpakket aan informatiebeveiligingscontrols en -maatregelen omvat die voor iedere gemeente noodzakelijk is om te implementeren.

[2] ENSIA is *de single information audit*. Dit betekent dat u maar één keer per jaar deze zelfevaluatielijsten hoeft in te vullen. De informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting departementen.

- Status Baseline Informatiebeveiliging Overheid.
- Datalekken 2019
- Meerjarenperspectief informatieveiligheid.

2. Resultaten zelfevaluatie 2019

2.1 Informatieveiligheid

Informatiebeveiliging is van belang voor meer dan alleen de specifieke registraties en systemen die onderworpen worden aan een zelfevaluatie en of audit zoals de BAG, BGT, BRO, BRP, PNIK, Suwinet en DigiD. Dit geldt ook voor andere processen in de gemeente, vandaar dat binnen ENSIA ook gemeentebreed met een zelfevaluatie getoetst wordt of de gemeente voldoet aan de normen uit de het normenkader BIG.

De uitkomsten van de zelfevaluatie informatieveiligheid laat zien dat gemeente Het Hogeland informatiebeveiliging niet volledig beheerst en dat er ruimte is voor verbetering. Ook laat de zelfevaluatie zien dat de betrokkenheid van medewerkers hoog is en het belang van informatieveiligheid wordt ingezien.

Op de volgende gebieden heeft de gemeente wel maatregelen getroffen maar is een hoger volwassenheidsniveau nodig om te komen tot een voldoende basisniveau van informatieveiligheid:

- Kennis, houding en gedrag ten aanzien van informatiebeveiliging
- Borging van beveiliging door middel van het Plan-Do-Check-Act cyclus
- Wijzigingsbeheer[3] op IT-gebied
- Incidentenmanagement
- Autorisatiemanagement
- Contractmanagement
- Bedrijfscontinuïteitmanagement

De verbeterpunten uit de zelfevaluatie zijn opgenomen in het informatiebeveiligingsplan 2020-2021.

2.2 Digitale identiteit (DigiD)

DigiD is het authenticatiemiddel voor onze online dienstverlening. Het object van onderzoek zijn de webomgeving(en) van de bestaande DigiD aansluiting in *tabel I*. Ook de DigiD zelfevaluatie is getoetst door een RE-gecertificeerde IT-auditor. Geconcludeerd is dat Gemeente Het Hogeland voldoet aan alle geselecteerde normen voor DigiD in opzet en bestaan.
Naast het feit dat gemeente Het Hogeland voldoet aan de normen voor DigiD heeft de IT-auditor aanbevelingen beschreven in de Assuranceverklaring[4]. De aanbevelingen zijn uitgezet bij team Burgerzaken.

Het college dient over de DigiD audit formeel een collegeverklaring af te leggen aan de gemeenteraad en toezichthouder Logius. Daarom is de Assuranceverklaring opgenomen (zie bijlage I) en de collegeverklaring integraal opgenomen (zie bijlage II).

---

[3] Wijzigingsbeheer zorgt voor het efficiënt en snel doorvoeren van wijzigingen binnen de IT-infrastructuur.

[4] Een Assuranceverklaring is een rapport van een onafhankelijke externe auditor, die een betrouwbaarheidsoordeel over de cijfers of processen van een leverancier of haar diensten geeft.

Functionaliteit	Aansluitnaam	URL van website
Het genereren van aanvraag en of aangifteformulieren voor: • Aangifte geboorte • Huwelijk/Partnerschap • Aangifte verhuizing • Aangifte verhuizing (Buitenland) • Afschrift burgerlijke stand • Bewijs van in leven zijn • Bewijs van Nederlanderschap • Uittreksel BRP • Verstrekking beperking • Wijziging naamgebruik • Rijbewijzen • Reisdocumenten • Overlijden	iBurgerzaken	iburgerzaken.hethogeland.nl.

Tabel I. DigiD aansluiting Het Hogeland

2.3 Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet)

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. De focus ligt hier op de vertrouwelijkheid van persoonsgegevens. Gemeente Het Hogeland maakt gebruik van Suwinet voor uitvoering van de volgende taken:

- Uitvoering van de Participatiewet
- Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)
- Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)
- Landelijke adresonderzoek door Burgerzaken

De uitkomst uit de zelfevaluatie Suwinet is getoetst door een RE-gecertificeerde IT-auditor. Er is geconcludeerd dat Gemeente Het Hogeland voldoet aan alle geselecteerde normen voor de SUWI-taken in opzet en bestaan.
Ondanks dat Gemeente Het Hogeland voldoet aan de gestelde normen heeft de IT-auditor aanbevelingen beschreven in de Assuranceverklaring. De aanbevelingen zijn uitgezet bij team Werkspoor Werkplein Ability.

Het college dient over de Suwinet audit formeel een collegeverklaring af te leggen aan de gemeenteraad en de toezichthouder Bureau Keteninformatisering Werk & Inkomen. Daarom is deze collegeverklaring integraal opgenomen (zie bijlage I).

2.4 Basisregistraties Personen (BRP)

Bij de zelfevaluaties BRP wordt de eigen handelingsprotocollen getoetst, waar de focus ligt op de kwaliteitsaspecten integriteit (juistheid, volledigheid) en vertrouwelijkheid van informatie.

Voor de BRP is in 2019 de thema indeling net als in 2018 bepaald met een maximumaantal punten van 2000 voor 6 afzonderlijke thema's. De wettelijke vragen zijn verdeeld over de thema's 1 tot en met 5 met een totaalaantal van 1900 punten. De resterende 100 punten zijn aan de vragen in thema

6. Aanbeveling toegekend. De thema's 1, 2 en 3 zijn afkomstig uit de ENSIA-tool. De thema's 4, 5 en 6 zijn direct vanuit de Kwaliteitsmonitor in de rapportage verwerkt. Door middel van de uitgevoerde zelfevaluatie heeft gemeente Het Hogeland de volgende score behaald, zie *tabel II*:

BRP				
Thema		**Score Het Hogeland**	**Maximale score**	**Percentages**
1	Organisatie van de beveiliging	312	400	78,0 %
2	Toegangsbeveiliging	362	400	90,5 %
3	Naleving	354	400	88,5 %
4	Bijhouding van de BRP	242	400	60,5 %
5	Verstrekking van gegevens	72	300	24,0 %
6	Aanbeveling	44	100	44,0 %
Puntentotaal BRP		1386	2000	69,3 %

Tabel II. Score zelfevaluatie BRP

De scores van de zelfevaluatie over 2019 laten een daling zien van de kwaliteit van de BRP ten opzichte van de toetsing in 2018 van de 4 verschillende gemeenten voor de herindeling. De daling heeft deels te maken met ontbreken van bestaand beleid en vastgestelde procedures alsmede van het kennisniveau van medewerkers en de complexe toename van de zelfredzaamheid van de teams (frontoffice en backoffice) binnen de afdeling Burgerzaken. De scheiding tussen de teams Burgerzaken en Gegevenshuis vraagt eveneens om een betere afstemming en kennis(overdracht). Om de kwaliteit van de BRP te verbeteren heeft team Burgerzaken voor 2020 een verbeterplan opgesteld. Inmiddels zijn team Burgerzaken samen met team Gegevenshuis aan de slag gegaan om de kwaliteit van informatie en de dienstverlening naar een hoger niveau te tillen.

2.5 Paspoorten en Nederlandse identiteitskaarten (PNIK)

Bij de zelfevaluaties PNIK wordt eveneens de eigen handelingsprotocollen getoetst, waar de focus ligt op de kwaliteitsaspecten integriteit (juistheid, volledigheid) en vertrouwelijkheid van informatie

Voor de PNIK 2019 is de thema indeling net als in 2018 bepaald met een maximumaantal punten van 2000 punten voor 6 afzonderlijke thema's. De wettelijke vragen zijn verdeeld over de thema's 1 tot en met 5 met een totaalaantal van 1900 punten. De resterende 100 punten zijn aan de vragen in thema 6 aanbeveling toegekend. De thema's 1, 2 en 3 worden voor het deel dat onder de informatieveiligheidsvragen vallen in het uittreksel in de ENSIA-tool gegenereerd. De resultaten van de overige domeinvragen Reisdocumenten worden in de Kwaliteitsmonitor in de thema's 4 en 5 gegenereerd met de aanbevelingen als aanvulling. Beide uittreksels vormen samen de verantwoording zoals bedoeld in de zelfevaluatie. De score uit de zelfevaluatie staat hieronder weergegeven in *tabel III*.

PNIK				
Thema		**Score Het Hogeland**	**Maximale score**	**Percentages**
1	Organisatie van de beveiliging	370	400	92,5 %
2	Toegangsbeveiliging	352	400	88,0 %
3	Naleving	340	400	85,0 %
4	Aanvraag- en uitgifteproces reisdocumenten	340	400	85,0 %
5	Overige processen reisdocumenten	233	300	77,6 %
6	Aanbeveling	85	100	85,0 %
Puntentotaal Reisdocumenten		**1834**	**2000**	86,0 %

Tabel III. Score zelfevaluatie PNIK

De scores van het onderdeel waardedocumenten vallen eveneens lager uit dan in het voorgaande jaar waarbij de oorzaak mede is gelegen in het ontbreken van vastgestelde procedures, de bezettingscapaciteit, het werken op 4 locaties maar ook in attitude en het nemen van verantwoordelijkheid van de medewerkers. De aandachtspunten van de waardedocumenten vallen ook onder het verbeterplan die benoemd staat bij de BRP.

2.6 Basisregistraties adressen en gebouwen (BAG)

De BAG is onderdeel van het stelsel van basisregistraties in Nederland. Gemeenten zijn bronhouders van de BAG. Dat betekent dat de gemeente verantwoordelijk is voor het beheer en de kwaliteit van de gegevens van de adressen en gebouwen binnen de gemeentegrenzen. De focus ligt hier op de integriteit (juistheid, volledigheid en tijdigheid) van gegevens.

Gemeente Het Hogeland heeft met een zelfevaluatie de borging van de processen, tijdigheid, volledigheid en juistheid getoetst. De periode waar verantwoording over wordt afgelegd loopt van 01-07-2018 tot 01-07-2019. Vanuit het ministerie is de norm gesteld op 75% van de totaalscore. De score voor gemeente Het Hogeland staan weergegeven in *tabel IV*.

Onderdeel	Score Het Hogeland	Maximale score	Percentage
Borging Proces	80	80	100 %
Tijdigheid	0	45	0,0 %
Volledigheid	30	40	75 %
Juistheid	20	40	50 %
Puntentotaal BAG	130	205	63%

Tabel IV. Score zelfevaluatie BAG

De verklaring dat er bij de BAG onder de norm wordt gescoord, wordt met name veroorzaakt door de deelscore op tijdigheid. Deze veel te lage score is ontstaan door de zogenaamde BAG-freeze. Dit was de periode in de herindelingstransitie die nodig was om de BAG-data van de latende gemeenten samen te voegen naar de omgeving voor de nieuwe gemeente Het Hogeland. In de freeze-periode van 14-12-2018 tot en met 08-01-2019 zijn er daarom geen BAG-mutaties uitgevoerd, met als gevolg dat maximale verwerkingstermijnen zijn overschreden

De conclusie van de zelfevaluatie is dat de kwaliteit van de BAG-registratie van de gemeente Het Hogeland, op basis van de cijfers in het kwaliteitsdashboard niet voldoet aan de gestelde eisen van

het ministerie. Gelet op de onbetrouwbare gegevens in het kwaliteitsdashboard en kijkend naar de huidige aanpak zou 'voldoende' te rechtvaardigen zijn.
Bij de volgende verantwoording (2020) zal er een realistischer/betrouwbaarder beeld zijn. De gemeente Het Hogeland legt dan immers als bronhouder verantwoordelijkheid af over de hele periode. Voor de volledige verantwoordingsrapportage BAG 2019 zie bijlage III.

2.7 Basisregistratie grootschalige topografie (BGT)

Basisregistratie Grootschalige Topografie (BGT) is een gedetailleerde digitale kaart van heel Nederland. Daarin staan onder andere gebouwen, wegen, water, spoorlijnen en groen. Door de gegevens in de BGT eenduidig op te slaan, zijn ze herbruikbaar voor alle overheidsorganisaties, alarmdiensten, marktpartijen, bouwbedrijven, ingenieursbureaus, burgers en alle andere geïnteresseerden die deze gegevens nodig hebben. Gemeenten zijn bronhouder van deze basisregistratie en moeten er dus voor zorgen dat de gegevens van de BGT kloppen. Ook hier ligt de focus dus op de integriteit (juistheid, volledigheid en tijdigheid) van gegevens.

Ook voor de BGT heeft de gemeente Het Hogeland een zelfevaluatie uitgevoerd op het gebied van borging van processen, tijdigheid, volledigheid en juistheid.

Vanuit het ministerie is de norm gesteld op 75% van de totaalscore. De score voor gemeente Het Hogeland staat weergegeven in *tabel V*.

Onderdeel	Score Het Hogeland	Maximale score	Percentage
Borging Proces	45	70	64,3%
Tijdigheid	15	20	75,0%
Volledigheid	25	30	83,3%
Juistheid	30	30	100 %
Puntentotaal BGT	115	150	77,0 %

Tabel V. Score zelfevaluatie BGT

Uit de zelfevaluatie is gebleken dat de kwaliteit van de BGT van gemeente Het Hogeland voldoet aan de gestelde norm. Voor de BGT geldt dat de kwaliteit, in samenwerking met het team infra, verder zal worden verbeterd zodat de kaartgegevens nog beter overeenkomen met de werkelijke situatie. Daarnaast zal steeds meer detailinformatie worden toegevoegd, waardoor er een goede basis ontstaat voor het beheer van de openbare ruimte (BOR) en de uitvoering van de nieuwe omgevingswet[5]. Voor de volledige verantwoordingsrapportage BGT 2019 zie bijlage IV.

2.8 Basisregistratie ondergrond (BRO)

De Basisregistratie Ondergrond (BRO) bevat gegevens over geologische en bodemkundige opbouw en, voor zover van belang voor het benutten van natuurlijke hulpbronnen in de ondergrond, ondergrondse constructies en gebruiksrechten. Het gebruik van geologische en bodemkundige gegevens vindt veelal plaats in de vorm van kaarten en profielen gebaseerd op geologische en bodemkundige modellen.

[5] De Omgevingswet is een aangenomen maar nog niet ingegane Nederlandse wet die een verregaande vereenvoudiging van het stelsel van wetgeving voor de ontwikkeling en het beheer van de leefomgeving (omgevingsrecht) beoogt, door tientallen wetten en honderden regels te bundelen in één nieuwe wet.

Ook voor de BRO heeft de gemeente Het Hogeland een zelfevaluatie uitgevoerd op het gebied van borging van processen, tijdigheid, volledigheid en juistheid.
Vanuit het ministerie is de norm gesteld op 60% van de totaalscore. De score is weergegeven in *tabel VI*.

Onderdeel	Score Het Hogeland	Maximale score	Percentage
Borging Proces	55	70	78,6 %
Tijdigheid	10	20	50,0 %
Volledigheid	10	20	50,0 %
Juistheid	10	10	100 %
Puntentotaal BRO	85	120	70,8 %

Tabel VI. Score zelfevaluatie BRO

Uit de zelfevaluatie is gebleken dat de kwaliteit van de BRO van gemeente Het Hogeland voldoet aan de gestelde norm. De score is laag uitgevallen omdat de BRO een nieuwe basisregistratie is die qua beheer nog verder geïmplementeerd moet worden. De beheertaak is inmiddels belegd in het Gegevenshuis. Voor specialistische taken wordt samengewerkt met de Gemeente Groningen.
Voor de volledige verantwoordingsrapportage BRO 2019 zie bijlage V.

2.9 Conclusie zelfevaluaties

De gemeente Het Hogeland heeft een hectisch jaar achter de rug. Een herindeling eist veel van een organisatie zo ook voor de kwaliteit van informatieveiligheid. Het bouwen van een nieuwe organisatie kost tijd. Voor informatieveiligheid geldt eveneens dat gemeente Het Hogeland moet bouwen naar het gewenste niveau van informatiebeveiliging. Een zelforganiserende organisatie vraagt een andere manier van werken. Voor informatieveiligheid betekent dit verantwoordelijkheid voor eigenaarschap van processen, applicaties en gegevens laag in de organisatie liggen. Uit onderzoeken is gebleken dat de periode van harmonisatie in de regel één tot vijf jaar kost. Op basis van dit uitgangspunt is het informatiebeveiligingsbeleid opgesteld. Het doel is dan ook om in 2023 alle beheersmaatregelen vanuit de BIO te hebben gedocumenteerd, de beheersmaatregelen op een juiste wijze worden uitgevoerd en dat de uitvoering van de beheersmaatregelen aantoonbaar zijn.

Wanneer we de resultaten van de zelfevaluaties beoordelen kan worden gesteld dat de informatieveiligheid niet op alle onderdelen op het gewenste kwaliteitsniveau zit.
Kijkend naar de ontwikkeling van Het Hogeland kunnen we concluderen dat de uitkomsten van de zelfevaluatie gelijk oplopen met een organisatie in opbouw.

3. Status Baseline Informatiebeveiliging Overheid

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen[6] in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen te waarborgen en incidenten te beperken.

De BIO is van toepassing op de overheid en daarmee op de volgende bestuursorganen: de Rijksdienst, Provincies, Waterschappen en Gemeenten. De BIO bestaat uit 14 beveiligingscategorieën, 35 normen, 112 controls en 141 (verplichte) overheidsmaatregelen.

Gemeente Het Hogeland heeft op 1 januari 2019 de veiligheidscommissie samengesteld, die zich richten op de implementatie van de BIO. Op basis van informatiebeveiligingsrisico's is het informatiebeveiligingsplan 2019-2020 opgesteld. De beheersmaatregelen en overheidsmaatregelen uit de BIO zorgen ervoor dat risico's, afhankelijk van de risicostrategie, worden beheerst, vermeden of overgedragen. Indien de kosten disproportioneel zijn ten opzichte van de beheers- en of overheidsmaatregel kan besloten worden het risico te accepteren. Zo'n soort besluit zal ten alle tijden worden genomen door het directieteam.

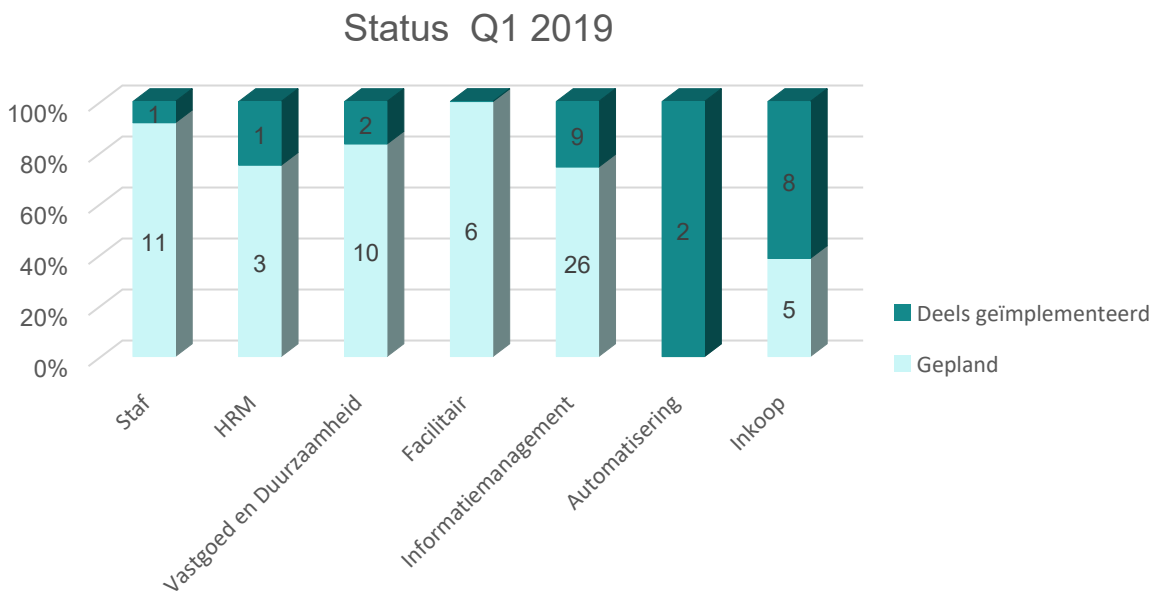
Het informatiebeveiligingsplan is in Q1 2019 opgemaakt met de teams Automatisering, Informatisering, Staf, Inkoop, HRM, Facilitair en Vastgoed en Duurzaamheid. In *figuur 1* is de status van de maatregelen per team weergegeven, zoals in Q1 2019. Een maatregel is geïmplementeerd indien deze één keer getoetst is aan opzet, bestaan en werking[7]. Standaard wordt jaarlijks de opzet en bestaan getoetst door middel van de ENSIA, de zelfevaluatie en IT-audit informatieveiligheid. In het kader van de PDCA-cyclus wordt jaarlijks de opzet, bestaan en werking getoetst

[6] Een informatiesysteem is het geheel van mensen, middelen, procedures en regels dat de informatievoorziening verzorgt.

[7] **Opzet:** is de norm gedefinieerd, is er beleid, procesbeschrijvingen en/of procedures.

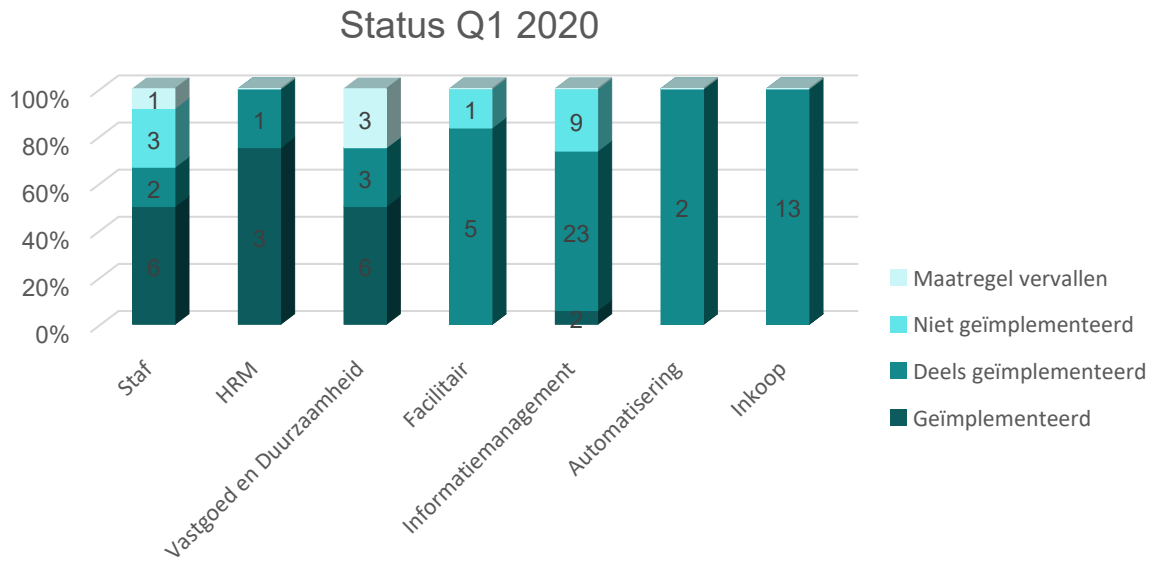
Bestaan: bestaat de (beheers)maatregel en kan deze aan de norm getoetst worden.

Werking: kan aangetoond worden dat het proces gedurende een periode werkt volgens de norm.



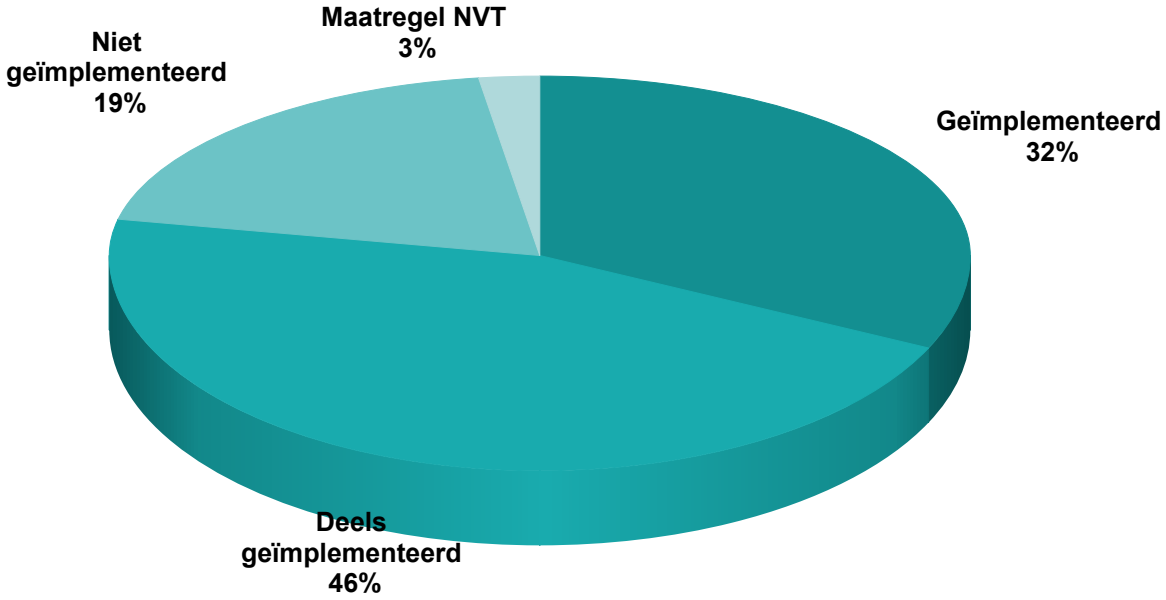
Figuur 1. Status informatiebeveiligingsplan Q1 2019

In *figuur 2* is de status weergegeven van het informatiebeveiligingsplan in Q1 2020. Wat hier opvalt is dat veel maatregelen deels geïmplementeerd zijn. Dit heeft voor een groot deel te maken met het missen van beleidsstukken, uitvoeringsdocumentatie, een juiste inrichting van de maatregel en/of de controle op werking van de beheersmaatregelen.



Figuur 2. Status informatiebeveiligingsplan Q1 2020

In *figuur 3* is de status van de BIO weergegeven zoals in Q1 2020. De status, zoals hieronder weergegeven, houdt niet automatisch in dat alle informatiesystemen dezelfde status hebben. Elk informatiesysteem dient afzonderlijk te voldoen aan de BIO.



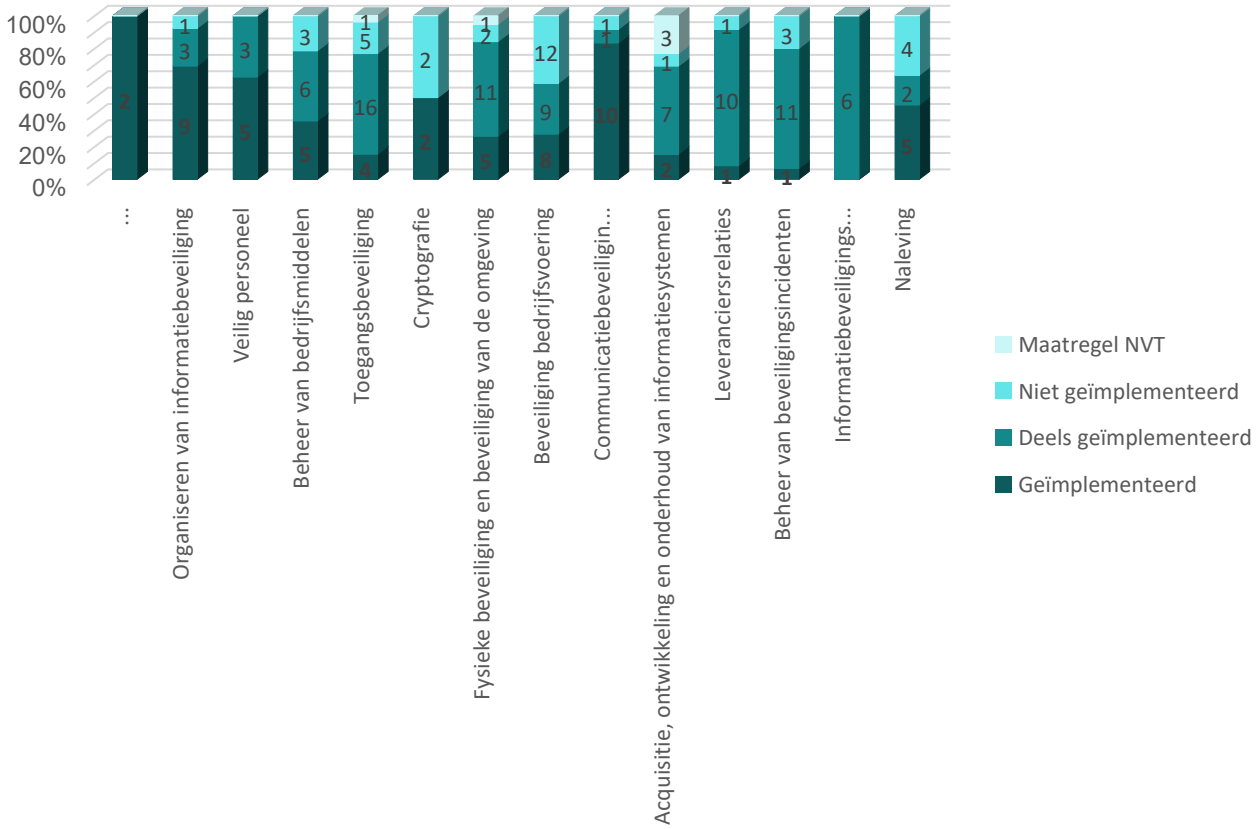
Figuur 3. Status implementatie BIO Q1 2020

Hier zoomen we verder in op de status per beveiligingscategorie. In *figuur 4* staat per categorie het aantal maatregelen weergegeven en de status hiervan.

De 14 beveiligingscategorieën bestaan uit:

- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie[8]
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van beveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

[8] Cryptografie is het versleutelen van data om het vertrouwelijke karakter van berichten en gegevens te handhaven.



Figuur 4. Status per beveiligingscategorie Q1 2020

Desondanks het hectische jaar en de strakke planning is er veel werk verzet door de leden van de veiligheidscommissie. Wanneer we kijken naar het doel, benoemd in het informatiebeveiligingsbeleid, dan is er nog veel werk te verzetten wil de organisatie alle structurele processen op volwassenheidsniveau 3 laten opereren. In augustus wordt het informatiebeveiligingsplan 2020 – 2021 voorgelegd aan het directieteam.

4. Datalekken 2019

Er is sprake van een datalek wanneer onbevoegden kennis kunnen nemen van persoonsgegevens waar zij niet toe zijn geautoriseerd. In 2019 zijn er 21 datalekken geconstateerd, dit is een lichte toename ten opzichte van 2018 waarin 17 datalekken zijn geregistreerd. Deze datalekken zijn conform de geldende procedure meldplicht datalekken gemeld bij de Functionaris Gegevensbescherming en vervolgens afgehandeld en geregistreerd op het interne datalekregister.

Als zich een datalek voordoet dient er conform de procedure een afweging gemaakt te worden of het nodig is het datalek te melden aan de Autoriteit Persoonsgegevens. In sommige gevallen kan het namelijk zo zijn dat dit niet nodig is. Dit is bijvoorbeeld het geval wanneer er voor de betrokkenen geen aanmerkelijke kans is dat zich schade zal voordoen. Vervolgens dient de afweging gemaakt te worden is of ook de betrokkenen geïnformeerd dienen te worden, hiervoor geldt ook dat dit niet altijd noodzakelijk is wanneer het probleem al is opgelost of wanneer dit een onredelijke inspanning vergt van de organisatie. Deze afweging is aan de Functionaris Gegevensbescherming.

Nagenoeg alle datalekken hebben als oorzaak dat er fouten worden gemaakt in de verzending. Zo vindt er regelmatig, door verscheidene teams, een verwisseling plaats. Er wordt bijvoorbeeld een verkeerde bijlage bij een brief gedaan of een brief/e-mail wordt verkeerd geadresseerd. Enerzijds heeft dit als oorzaak dat er onzorgvuldig gewerkt wordt en anderzijds is soms de werkdruk te hoog waardoor er te spoedig gewerkt moet worden. Daarnaast worden waar mensen werken fouten gemaakt en het feit dat deze datalekken gemeld worden en dat er sprake is van een lichte toename is in het kader van de verplichte transparantie uit de AVG een positieve ontwikkeling.

In het oog springende datalekken uit 2019 waren:

In het begin van 2019 was de werkdruk bij team Burgerzaken behoorlijk hoog. De reguliere werkwijze voor het versturen van een uittreksel BRP was dat men deze uitprint en meteen in een envelop stopt. Door de hoge werkdruk werden er meerdere uittreksel tegelijk geprint waardoor risico ontstaat dat hier een verwisseling optreedt. Dit was dus ook het geval. Zowel de betrokkenen en de Autoriteit Persoonsgegevens is op de hoogte gesteld van het datalek. Eerder was bij hetzelfde team ook al een datalek gemeld waarbij een verkeerd adres boven een verzonden persoonslijst is terechtgekomen, dit had te maken met het systeem dat door de samenvoeging nog niet optimaal werkte. Adressen moesten destijds handmatig worden ingevoerd. Ook dit datalek is zowel bij de betrokkene als bij de Autoriteit Persoonsgegevens gemeld.

Bij de Servicedesk kan bij uitzondering een laptop geleend worden. Op een uitgeleende laptop stonden twee documenten met daarin bijzondere persoonsgegevens (gegevens over de gezondheid). In één van de twee gevallen gaat het om een jeugdige. Van de andere is de leeftijd niet vast te stellen. De laptop is door Automatisering gewist. Dit datalek is gemeld bij de Autoriteit Persoonsgegevens. Door degene die het document aantrof en door de Functionaris Gegevensbescherming kon niet achterhaald worden om wie het gaat omdat er enkel voornamen bij de documenten werden gebruikt. Voor de opsteller van het document en meerdere personen uit de omgeving van de betrokkene was hoogstwaarschijnlijk wel af te leiden om wie het gaat, er is hier dus wel sprake van herleidbare persoonsgegevens en ook nog eens bijzondere persoonsgegevens, in dit geval gegevens over de gezondheid van de betrokkene.

5. Meerjarenperspectief informatieveiligheid

De gemeente Het Hogeland richt zich de komende jaren op het verbeteren en borgen van de informatieveiligheid door BIO-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA) in te richten, te ondersteunen en te bewaken. Op basis van risico, (lopende) projecten en beschikbare tijd en middelen wordt jaarlijks maatregelen uitgewerkt in een jaarplan. De informatiebeveiligingsmaatregelen in het jaarplan worden aan het einde van het jaar één keer getoetst is aan opzet, bestaan en werking. Hierna wordt in het kader van de Plan, Do, Check, Act cyclus jaarlijks de opzet, bestaan en werking getoetst.

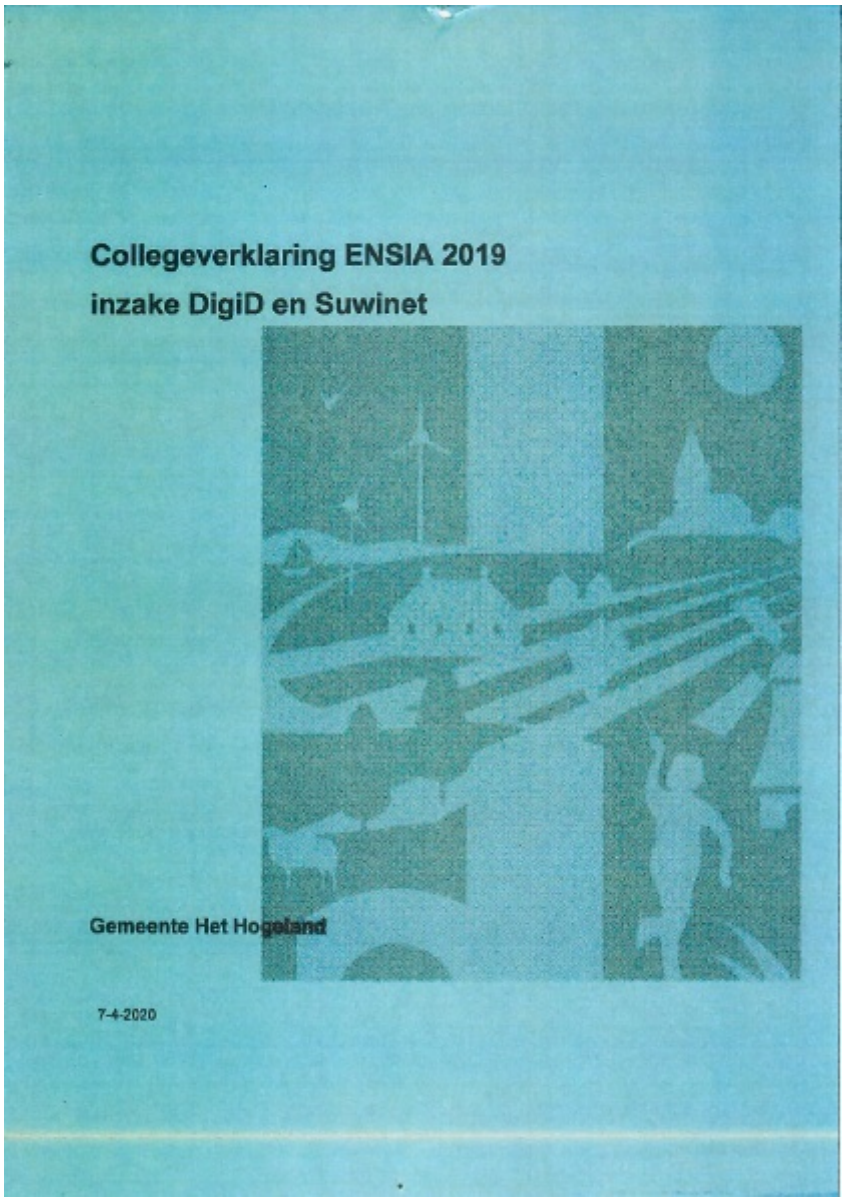
6. Tot slot

Bij informatie is het van belang dat deze op een passende wijze wordt beveiligd. Zoals in de inleiding gesteld: hoe waardevoller en gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. 100% beveiliging bestaat echter niet en dient ook niet nagestreefd te worden. De kosten van beveiliging moeten in verhouding zijn tot de risico's. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is wel van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico's.

Bijlage I Assuranceverklaring ENSIA 2019 DigiD en Suwinet

Deze bijlage bevat het Assurance rapport DigiD en Suwinet voor het verantwoordingsjaar 2019. De bijlage bevat niet de aangegeven bijlage A1, A2 en A3. Dit omdat de inhoud hiervan technische aanbevelingen betreft voor de verbetering van informatiebeveiliging.

Bijlage II Collegeverklaring DigiD en Suwinet



Collegeverklaring ENSIA 2019 inzake DigiD en Suwinet

Gemeentelijk kenmerk collegeverklaring ENSIA:	Z.HHL.012996

Gemeente Het Hogeland

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Het Hogeland voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

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

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte en diepgang verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Het Hogeland betreft dit in 2019 DigiD en Suwinet.

De verklaring houdt in dat de gemeente op 31 december 2019 voldoet aan de opzet en bestaan van de geselecteerde beheersmaatregelen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2019.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk Z.HHL. 016833) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener worden uitgevoerd, wordt door de dienstverlener verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersingsmaatregelen van de gemeente.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk Z.HHL. 016833) en Suwinet (bijlage 2 Suwinet met kenmerk Z.HHL. 016834) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk Z.HHL. 016833) en voor Suwinet (bijlage 2 Suwinet met kenmerk Z.HHL. 016834) geïnformeerd over de afwijkingen van de normen.

p. 2/8

BK BO
BKBO bv 22/4/20
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37
drs. M.B.H. IJpelaar RE CEH

Verklaring college

Het college verklaart dat bij gemeente Het Hogeland op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1002949	Ja	Neen
Suwinet voor SUWI-taken	Ja	Neen
Suwinet voor niet-SUWI-taken	Ja	Neen

Winsum, 07-04-2020

College van B en W gemeente Het Hogeland

H.J. Bolding
Burgemeester

Naam auditfirma:	BKBO bv.
Naam auditor:	drs. M.B.H. IJpelaar RE CEH CISA
Datum: 22 april 2020	Handtekening of paraaf auditor: drs. M.B.H. IJpelaar RE CEH

BKBO bv 22/4/20
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37 drs. M.B.H. IJpelaar RE CEH

p. 3/8

Bijlage III Verantwoordingsrapportage BAG 2019

Deze bijlage bevat de verantwoordingsrapportage BAG 2019 en is voorzien van de bestuurlijke verantwoordingsrapportage. Dit rapport is op 25 mei ’20 ingediend bij de landelijke toezichthouder van Binnenlandse Zaken en Koninkrijksrelaties.

Bijlage IV Verantwoordingsrapportage BGT 2019

Deze bijlage bevat de verantwoordingsrapportage BGT 2019 en is voorzien van de bestuurlijke verantwoordingsrapportage. Dit rapport is op 25 mei ’20 ingediend bij de landelijke toezichthouder van Binnenlandse Zaken en Koninkrijksrelaties.

Bijlage V Verantwoordingsrapportage BRO 2019

Deze bijlage bevat de verantwoordingsrapportage BRO 2019 en is voorzien van de bestuurlijke verantwoordingsrapportage. Dit rapport is op 25 mei ’20 ingediend bij de landelijke toezichthouder van Binnenlandse Zaken en Koninkrijksrelaties.